Université catholique de Louvain
Faculté des Sciences Appliquées
LABORATOIRE DE TÉLÉCOMMUNICATIONS
ET
TÉLÉDÉTECTION

B - 1348 Louvain-la-Neuve Belgique

Digital Watermarking Algorithms Robust Against Loss of Synchronization

Damien Delannay

Thèse présentée en vue de l'obtention du grade de
Docteur en Sciences Appliquées

Examination Committee:

Benoît MACQ (UCL/TELE) - *Supervisor*
Luc VANDENDORPE (UCL/TELE)
Jean-Jacques QUISQUATER (UCL/DICE)
Inald LAGENDIJK (Delft University of Technology, The Netherlands)
Pierre MOULIN (University of Illinois at Urbana-Champaign, USA)
Jean-Didier LEGAT (UCL/DICE) - *President*

April 2004

Acknowledgements

I wish to thank my supervisor for creating this opportunity to study exciting and fascinating research fields in image processing. I am very thankful for the guidance, advices and encouragements he provided since the beginning, and for the research contacts and collaborations he made possible. I am also grateful for his support and his efforts in my struggle for combining research and teaching activities.

It was a pleasure, in the last 6 years, to share my office with many exceptional colleagues. I remember especially the stimulating discussions and the very nice times I had in the office, together with the long-term French visitors, my wonderful Columbian colleague and the quite pleasant and experimented system engineer. I also want to mention the valuable friendship that was build with many other researchers during these years. I am thankful to all present and past members of the Communication and Remote Sensing Laboratory for making it a stimulating and pleasant environment.

It is difficult to overstate how thankful I am for the many extraordinary friendships that have emerged from these last years spent on the University campus. I think especially to these very special people I have lived with in different places in Louvain-la-Neuve and a large number of wonderful people within and around the community of kot-à-projets.

I am very thankful to the irreplaceable long-lived friends from university, high school and elsewhere for their continuous and valuable encouragements. I think especially to those in Brussels and abroad, which, in spite of less frequent contact lately, will continue playing very important roles in my life.

Last and most importantly, I wish to thank my parents and family for their everlasting love and support.

Contents

Introduction

The organization of the present work is depicted in figure 1 and proceeds as follow.

Chapter one summarizes the young signal processing discipline, called digital watermarking, which constitutes the basis framework of this work.

Chapter two presents a challenging issue in the design of watermarking algorithms: the robustness against the specific set of distortions which causes loss of synchronization. Being able to cope with geometrical distortions is far from evident for a watermarking scheme. The limitations and weaknesses of the previously proposed solutions are discussed.

Subsequent chapters describe the new contributions that are brought about by this work to the resolution of this issue.

Chapter three addresses the design of periodical structures in watermarking schemes. A new scheme is proposed and its robustness and security features are analyzed.

Chapter four presents an image normalization method based on the signal characteristics observation. The robustness of the method and its exploitation to secure watermarking schemes relying on pilot registration are presented.

Finally, chapter five explores the issue of quantifying the perceptual nuisance caused by a geometrical distortion. We show that such a quality assessment is mandatory both to evaluate robustness and to design new watermarking schemes.

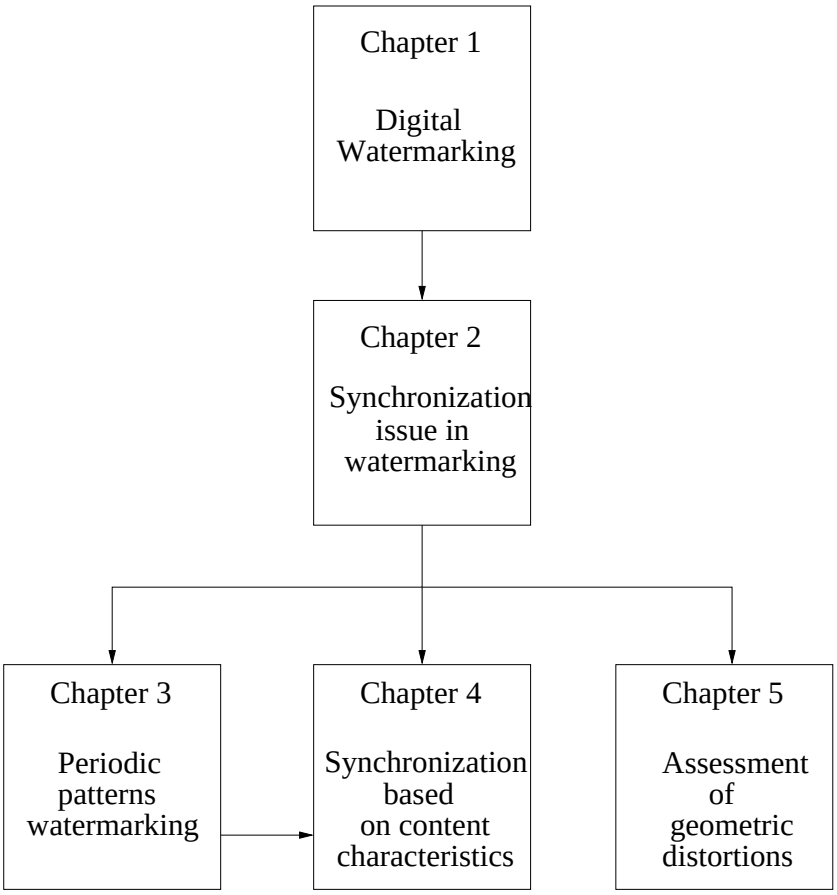


Figure 1: *Outline of the work.*

Chapter 1

Digital Watermarking

1.1 Introduction

During the last decade, digital technology expansion has established the advent of the digital era for information. This technology has introduced powerful means to every level of the information handling: production, reproduction, distribution, storage, processing, ... Almost all information media are now handled under digital form.

Only few traditional analogue media processes are still widely used. They are mainly limited to specific, still digitally unequaled, production and perception/prehension forms. In addition, one must deal with a large number of analogue devices still in consumers hands and extensively used in less developed regions. There is no doubt however that the evolution towards digital will go on at an accelerated rate in the coming years.

Not only digital technology has improved usual techniques, but it has also introduced new processing opportunities. Some of these new means have destabilized the long community established relations regarding information media handling. As community rules cannot evolve as fast as this technology evolution rate, additional means must be provided to enable the enforcement of those community established rules.

A major concern raised by new digital technologies is the ease to reproduce and distribute media contents. In analogue form, reproduction and distribution was prevented by unavoidable degradations and material constraints. With nowadays digital technology, including Internet developments, perfect copy and transmission of any digital content can be done at very low cost. Moreover perfect reproduction processes make more difficult the determination of the paternity of a work. This situation

causes damage to the established economic system which rewards content creation. New means must therefore be provided to impose rules such as copyright.

Watermarking is one of the different means which can contribute to enforce intellectual property rights. Cryptography can protect content along the transmission, distribution and storage processes. However it does not protect the content once it has been decoded to be viewed by authorized users. Even with secured playing devices, the digital content is eventually transformed in physical ligth or audio wave signals which can be copied through re-digitization. Cryptography therefore does not control subsequent uses. Watermarking aims at providing protection up to the last level of the content handling. In order to reach such protection, it proceeds by robust hiding of a message within the media content itself. This complementary information embedding is achieved by applying imperceptible secret modifications to the content.

The role of this embedded information can be manifold. For copyright, the watermark information can refer to the rights holder. This information, if detected, can prevent illicit usage of the content by indicating the existence of rights on the content. It can also be used a posteriori as a proof of ownership in front of a court. Another option is to use the watermark as a fingerprinting tool. In this case, the embedded message informs about the identity of the user from whom the illicit usage originates.

Watermarking is also proposed for other applications. It can be used to let a content, represented in analogue form, convey a side information. These contents are then said smart. A printed image could for example contain the name of the represented location or the the reference to a web site. Other applications have been proposed such as authentication tool or protected side-channel. However the requirements of these applications for digital content can in many situations be perfectly fulfilled with traditional cryptographic tools and meta data attached to the files. For these applications, the use of watermarking is only justified in mixed digital-analog scenarios. Another exception could be applications where badly implemented transcoding operations could take place such that meta information would be erased from the conveyed digital file.

Although different application scenarios can exhibit specific constraints, a set of important properties is common to most usages of watermarking technology. Following section describe the usual set of requirements for digital watermarking.

1.2 Requirements for a watermarking scheme

An ideal watermarking scheme must satisfy a set of constraints of very various natures. Most intervening techniques are related to the fields of signal transmission, cryptography and human perception psychological phenomena. The design is complicated by the conflicting interdependence of the different constraints. It makes it difficult to study all aspects simultaneously but it appears also hard to successfully isolate the different constraints. The main requirements which should be fulfilled by a watermarking scheme are imperceptibility, security and robustness.

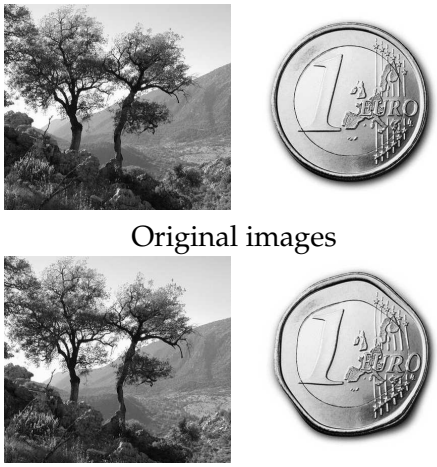
1.2.1 Imperceptibility

One may expect from a watermarking scheme that it does not alter the qualitative and semantic perception of the represented content. It means that both perceptual comfort and interpretation of the representation should remain unchanged after embedding of the watermark information. Figure 1.1 illustrates semantic and qualitative modifications of an image.

Altered Semantic Original image Altered quality

Figure 1.1: *Different modifications of an image.*

Sometimes semantic and quality notions interfere due to the fact that our a priori knowledge influences greatly our sensitivity to modifications. As illustrated in figure 1.2 an identical deformation applied on two different contents does not cause the same nuisance. More generally, the human sensitivity to various distortions is highly dependent on the interactions of these distortions with the content characteristics. The understanding and control of the mechanisms at stake is a complex matter. This issue is partially related to the compression discipline.



Original images

Distorted images

Figure 1.2: *Same distortion applied on different contents.*

Although well aware of these psycho-perceptual phenomena, very few sensitivity assessment tools are available. The evaluation of a distortion severity still relies on an experimental human validation. Three situations can be brought out to evaluate the perceptual nuisance caused by a watermarking process.

In the first case, the user is unable to perceive any difference between the original and watermarked contents. This situation results from a coding resolution higher than the eye sensitivity or exceeding the restitution device precision. It can also be consequent to a psycho-sensitive masking phenomenon.

The second case corresponds to the situation where the user is able to distinguish both content specimens but without judging one better than the other. Applied modifications do not introduce semantic or quality degradation.

In the last case, watermark embedding causes a perceptible and bothering distortion to the content. Depending on the severity of the nuisance and the targeted application, this situation will be considered admissible or to be ruled out. In specific applications, where additional distortion is always present, it may be acceptable that the watermarked content exhibits a relative distortion with respect to the original content.

1.2.2 Robustness

Watermarking only makes sense if you can expect that authorized users will be able to extract and decode the embedded information. However, as the embedder generally does not have full control of the transmission channel and that he is constrained by imperceptibility and security requirements, it cannot be guaranteed that the message be always successfully decoded. One must keep in mind that, although the channel exact characteristics are mostly unknown, one can rely on a general assumption. The watermark detectability must only be ensured as long as the content stays valuable. Indeed one can easily apply a distortion on a content such that watermark extraction is made impossible. However resulting content might be so degraded that it makes no sense trying to protect it anymore. The appropriateness of a scheme for a given application will therefore be measured by the robustness degree to distortions likely to occur in the targeted application.

When addressing the robustness of a watermarking scheme, one considers the most common and likely distortions. Depending on severity and the application, two distortions of identical nature can have different origins. It is sometimes not straightforward to determine whether a distortion results from usual content processing or from ill-intentioned manipulations. Notice that, as malicious users might seek at removing protection from a content, unusual specific distortions can be designed to exploit peculiar weaknesses of a watermarking scheme. Let us describe most common distortions that one should take into account when designing a watermarking scheme.

Compression. Raw digital content representations are huge and highly correlated. Therefore, it is nowadays inescapable to use compression when handling digital content representations. If this operation is performed in a lossless manner, it will have no effect on watermarking robustness. However, as it is most frequent, in order to reach important compression ratios, this operation will remove part of the content information causing perturbations to the watermarking process. An efficient lossy compression algorithm seeks to simplify the coded representation of a content by eliminating less significant information. Ideally, this suppression will only cause very little perceptible distortions. As compression ratio increases, more significant information is left out and perceptual nuisance becomes more important.

One can realize that, if a compression technique perfectly meets its

goals, that is yields a decorrelated representation of the content where all non-significant information is removed, it will inevitably destroy the information corresponding to the watermark. Indeed, the watermarking process introduces modifications which are imperceptible to the user. These modifications should therefore be considered as non significant by the compression algorithm and as a consequence be removed from the coded representation of the content. In order to design a watermarking scheme robust to compression, one should rely on the imperfect character of the compression schemes, or in other words, introduce distortions which will be considered relevant by the compression algorithms. Generally, compression schemes will eliminate first and foremost high frequency components of the content which correspond to detail information. Watermark information should not be exclusively composed of high frequency if it has to resist compression.

Rendering related operations. A wide range of usual manipulations can be performed on a content to better fit one's needs. In image processing, classical operations include contrast enhancing, smoothing, color and luminance histogram modification, denoising. The design of a watermarking scheme should take into consideration the effect of these different operations.

Digital/analogue conversions Most content are converted in a physical form (e.g. sound, light) to be perceived by a human such that a digital-to-analogue conversion occurs. Content reproduction can be performed on physical representations using analogue acquisition device. Depending on the device characteristics, important distortions can take place during this analogue-to-digital conversion. A case-model for such manipulations is the illicit movie reproduction performed with handy cameras in movie theaters.

Geometric deformations Geometric deformations can occur during rendering or acquisition processes. However, the challenge it poses to watermarking schemes is quite specific and is worth a dedicated attention. The design and study of watermarking schemes robust against such distortions is the main subject of this work and will be deeply presented in the following chapters.

Explicitly malicious manipulations Since early research on watermarking, specific content manipulation algorithms have been designed to test the robustness of watermarking schemes. These manipulations, also called attacks, try to exploit expected weaknesses of the proposed schemes. Common attacks used to evaluate the robustness of image watermarking schemes are denoising, jittering, mosaic attack and stirmark manipulation software.

1.2.3 Security

For most watermarking applications, an important requirement is related to security. Indeed watermarking often plays a restricting role on content usage. It aims at preventing forbidden actions or enforcing user's obligations. One can expect that some users try to jeopardize the watermark extraction or the functional model which it relies on. One must also avoid making decisions based on erroneously extracted messages.

Watermarking makes use of cryptographic tools to ensure its security. However, watermarking differs from common cryptography in the sense that it does not necessarily aim at ciphering a message. Watermarking is more closely related to steganography which consists in hiding a secret message within another one in such a way that others can not discern the presence or content of the hidden message. However, watermark presence- and sometimes content- is publicly known. Moreover, watermarking must deal with much stronger robustness constraints than steganography. Primarily concern in watermarking is to make very difficult the removal of the embedded information without important degradation of the supporting content.

As stated by Kerckhoffs' principle, security should exclusively rely on the knowledge of a key. Embedding and detection schemes must be considered known by opponents, security is only function of the uncertainty on the key. One way to break the system is to perform a brute force attack which consists in trying exhaustively all possible keys. Security level is therefore measured in terms of probability. In order to fit security requirements, one must ensure that the number of possible keys is sufficiently large such that exhaustive search becomes computationally infeasible.

Security issues in watermarking are manifold. One must prevent opponents from exploiting the scheme characteristics to succeed in removing important watermark signal power while preserving content information. Opponents should not be able to distinguish watermark components from the original content signal. Partial watermark removal can often jeopar-

dize the whole detection scheme. Even for authorized users watermark signal can not be totally distinguished from content which acts like noise in the detection. Therefore, in order to limit the probability of wrong decisions, one must be able to evaluate the confidence that it can attach to the extracted message.

Other security threats are related to the application security protocol. The availability of multiple specimens of the same content where different watermarks are embedded can enable a collusion attack on the system. This attack can provide to opponents a reliable estimation of the original unwatermarked content and prevent content rights holder from extracting any useful message. One must also prevent opponents from copying watermark from one content to another one. Exploiting reversibility of a scheme, an opponent can sometimes produce fake original content and contest rights legitimacy.

1.2.4 Other desirable properties

A few other properties could be desirable for a watermarking system. These are not mandatory for most applications but can lower implementation complexity and costs.

A first useful property is the versatility of the watermarking scheme. This can refer both to contents and applications. Renewability of the scheme and compatibility with evolving techniques can also bring advantages. Computational power requirements should be kept as low as possible to match practical available resources.

Reversibility of the embedding process, enabling perfect recovery of the original content, can be required for some applications.

Another very useful property would be an asymmetry of the scheme regarding message embedding, detection and extraction from the content, also refered to as public key watermarking. Ideally, everyone should be allowed to read the watermark embedded information but only authorized user would be able to embed or remove it from the content. This functionality, very common in cryptography, has not yet been fully achieved in proposed scheme. It is far from evident that such a scheme exists.

1.3 Practical uses of watermarking / Achievable watermarking systems

Designing a watermarking scheme implies to compromize best among all desirable requirements . For most requirements, practical schemes can only exhibit partial compliance. Existing approaches differ in the level of compliance to each of the different requirements. Therefore, effective watermarking design is only achievable if some constraints can be partially released.

Hopefully, many applications can afford partial release of constraints. Let us expose some considerations that illustrate the relevance of incomplete compliance with the requirements of an ideal watermarking scheme.

Most important, one can optimize its design for the targeted application system. One can benefit from a priori characterization of the cover content. Schemes dedicated to images, songs, or videos will not be the same. They may even differ for different classes of image content. Video application can rely on much higher content data volume than still images. Sometimes the application scenario enables strong constraint releases. In many cases for example, one can rely on the availability of the original unwatermarked content to perform watermark extraction. In some other cases, the system will not be subject to malicious attacks but only to distortions consequent to usual content processing.

The requirement relative to detection probability is also very dependent on the application. In a commercial scenario where watermarking aims at enforcing retribution, a payment imposed to 80 percent of the users could be judged sufficient for the economic viability of the system. In copy tracing application, a successful detection rate of 1 percent could be considered sufficient to dissuade illicit behavior.

In applications where watermarking plays a restricting role, it will most of the time be used in conjunction with other protection mechanisms such as cryptography and legal actions. It can be used to give information about suspected illicit actions which require complementary human investigation for validation. In such systems, watermarking can be considered as a complementary protection whom success in not mandatory.

1.4 Watermarking principles

The watermarking process is usually described as communication over distorting channel problem. The challenge consists in transmitting a mes-

sage through an unknown deforming channel. Figure 1.3 illustrates the structure of a watermarking system. In this communication system, the transmitter is essentially composed of encoding and embedding modules, while the receiver is composed of detection and decoding modules.

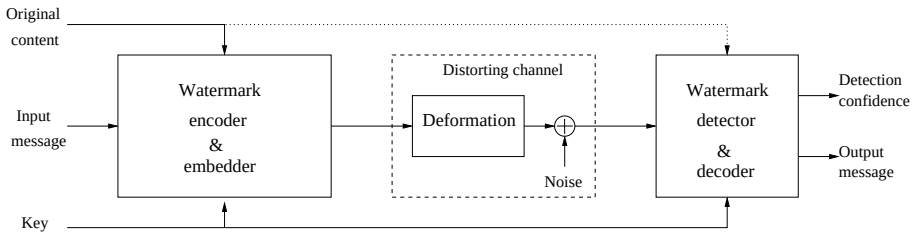


Figure 1.3: *Watermarking system.*

The communication system must be designed to cope with cover signal interference and channel distortions. Solution to the problem will logically be inspired by the quite elaborated theory of digital communications. Important constraints which are not highlighted in figure 1.3 are the limitation on the degradation that the cover content may undergo and the secrecy imposed to prevent opponent from distinguishing cover content and watermark signal. This leads to very low watermark power which in presence of cover signal interference, channel distortions and external noise imposesvery short transmitted messages.

The original cover signal plays a particular role in this model as it is known to the embedder and sometimes also to the decoder. Therefore watermarking is also referred to as a communication problem with side information at the transmitter and possibly at the receiver. This side information at the embedder can be exploited in two different manners. Firstly it helps determining how watermark signal power can be maximized while ensuring its imperceptibility. Indeed, the theory of psycho-visual masking phenomenon shows that the interaction between hidden and host signals should be taken into account in order to guarantee invisibility. Note that less efficient perceptual weighting of the watermark power can also be performed without side information by following ”good practice” rules which modulate watermark power spectrum.

A second way to benefit from cover signal availability is to adapt the coding process to the cover signal characteristics. This supposes that a same message can be represented by several different codes. Established dirty-paper coding theory tells that using this approach with Gaussian sources, watermarking capacity can be made insensitive to cover signal

characteristics. More recently, different work [1, 2] have demonstrated that this property can be extended to many other non-Gaussian sources. Although watermarking sources can not always be precisely modeled, one can expect important benefits from using side information during the watermark coding process.

This work does not aim at providing extensive outline of existing watermarking technology. The reader may refer to existing literature[3, 4] for a more detailed description.

1.5 Present usage and alternatives

Currently, watermarking technology has not yet reached the performance that could justify its massive usage in multimedia applications. However, the ongoing research has yielded impressive progress since the early works. There is no doubt that further research on the subject can still bring improvements and better understanding of the limitations and potentialities of this new technology.

Applications exist already where watermarking technology is used. As previously discussed, in many protection systems currently under development, watermarking resort is planned in conjunction with other mechanisms.

Some of the essential functionalities that are sought in watermarking technology can however be implemented using other techniques. Authentication can be very efficiently handled by cryptographic protocols. Current research is also trying to develop robust identification techniques to design copy and diffusion monitoring systems. Such identification requires efficient database architectures and poses privacy related problems. Finally, few systems rely on secure hardware support and playing devices in order to prevent access to decrypted content. Besides the limitation on usage, such system often end up being cracked leaving decrypted content unprotected.

Watermarking technology must be considered as complementary processing tool which can play a role in well defined application scenarios. Further developments are required for a wide resort of this technology in the multimedia industry.

Chapter 2

The synchronization issue in watermarking schemes

The resistance of watermarking schemes against geometrical distortions has been the subject of quite much research in the last ten years. The ability for a communication scheme to cope with a loss of synchronization is indeed a very difficult issue. Still, the tolerance of the human visual perception in presence of such distortions is surprisingly high and situations where loss of synchronization takes place are numerous. The aim of this chapter is to present an extensive survey of existing works addressing this particular problem. Each of the proposed class of techniques will be analyzed to show which forms and what severity of distortions it is able to survive. The possible security implications of the proposed techniques will also be studied. We will try to point out the strengths and weaknesses of each solution. Special attention will be given to implementation details such as cropping operation which is subsequent to most geometrical distortions. Partial loss of content, change of width to height ratio or modification of the image size have important consequence on some proposed schemes. We will also briefly discuss the difficulty to evaluate the severity of a geometrical distortion.

Keywords: Watermarking, synchronization, geometrical distortions.

Introduction

The present work focuses on the challenge of designing watermarking schemes resistant against desynchronizing distortions. Synchronization issues are of the utmost importance in a communication system. Indeed, a signal bears information only relatively to its original references. Modify-

ing references results in modification of the conveyed information. Robust communications systems require means to recover from a possible loss of the original signal references.

Signal transformations causing desynchronization are common. In watermarking scenarios, their origins are numerous and can be consequent to malevolent manipulations as well as usual processing. With nowadays digital processing ease, the only limitation to such distortions is perceptual comfort.

2.1 Communications over desynchronizing channels

A wide class of communication channels can be described by the linear filter channel with additive noise. In this model, the channel distortion is determined by the shape of the channel impulse response h and the nature of the independent additive noise signal. Given s an input signal, the channel output r is given by

$$\begin{aligned} r(t) &= s(t) * h(t) + n(t) && (2.1)\\ &= \int_{-\infty}^{\infty} h(\tau) s(t-\tau) d\tau + n(t). && (2.2) \end{aligned}$$

where $n(t)$ is noise.

In the above expression, the impulse response $h(\tau)$ is not a function of time variable t. The system is said to be linear time-invariant (LTI). Quite much theory has been developed about communications over such channels. However, an important class of channels is not represented by expression 2.2. In order to describe such channels, one must consider a more general channel expression where impulse response is evolving along time. Such channels are called linear time-variant (LTV) filter channels.

$$\begin{aligned} r(t) &= s(t) * h(\tau; t) + n(t) && (2.3)\\ &= \int_{-\infty}^{\infty} h(\tau; t) s(t-\tau) d\tau + n(t). && (2.4) \end{aligned}$$

Transmission with radio wave signals is an example of a physical system necessitating the LTV channel model. It is common to consider it as a varying multi-path fading channel. The channel impulse response has the form

$$h(\tau; t) = \sum_{k=0}^{N(t)-1} a_k(t) \delta\left[\tau - \tau_k(t)\right] e^{j\theta_k(t)} \quad (2.5)$$

where $N(t)$ is the time-varying number of multi-path components, $a_k(t)$,$\tau_k(t)$ and $\theta_k(t)$ are the random time varying amplitude, delay and phase of each signal path.

In order to deal with such channels, one usually relies on the assumption that time-varying parameters can be considered constant for some given periods of time. The channel model is hence converted to a LTI system which can be more easily handled. The achievement of synchronization can be separated in two phases [5]. The first phase consists in the acquisition of the initial channel characteristics by resolving time and frequency uncertainty, while, in a second phase, one performs fine tracking including optimum sample timing and possibly carrier phase tracking. Training or pilot signals are often used to achieve initial channel estimation. The acquisition step requires a very stable channel state, while tracking only succeeds when characteristics change sufficiently slowly.

Geometrical distortions occurring in image watermarking are best described by a linear space-variant filter channel. The channel impulse response can be expressed as the combination of two filters:

$$\begin{aligned} h(u,v;x,y) &= h_{lsv}(u,v;x,y) * h_{lsi}(u,v) && (2.6)\\ &= \delta(u - d_x(x,y), v - d_y(x,y)) * h_{lsi}(u,v). && (2.7) \end{aligned}$$

The space-variant component of the impulse response h_{lsv} consists in a single space-varying delay or spatial displacement representing most desynchronizing distortions. The second linear component h_{lsi} and the additive noise $n(t)$ model the rest of the distortions such as image compression or rendering. The channel frequency selectiveness is thus fully space-invariant. Note that the geometrical operation consisting in cropping is a space-invariant distortion. All other geometrical deformations cause a space-varying channel behavior.

The major difficulty when dealing with watermarking complex desynchronizing channels is that the constant channel state assumption can be made only over very short periods. Moreover, signal to noise ratio is often so low that neither initial channel state acquisition nor tracking can be performed. We will see that a possible solution is to transform the signal in a new representation space in which the channel exhibits a "space"-invariant behavior. Sometimes it merely enables to consider channel as invariant over larger signal periods.

Another constraint in watermarking systems is that training or pilot signals mechanisms must be kept secret to opponents.

2.2 Classification of geometrical distortions

There are two approaches to address the different forms of geometrical distortions that an image can undergo.

Usually one considers the set of possible distortions in terms of their likelihood to take place. Under this approach the most important distortions will be those caused by most common physical or digital handling processes. Distortions resulting from easily achievable manipulations will also be given much consideration. Excepting some application-specific non-linear physical processes, this classification will probably match the mathematical complexity and degrees of freedom of the deformation models. Attention should therefore be given in decreasing order to the following deformations:

- T: Translation (cropping).
- Rigid or RST: Rotation, scaling and translation.
- Affine or SARST: Shear, aspect ratio, rotation, scaling and translation.
- P: Projective transform.
- Non-linear lens deformation...

Circumstances where such distortions can take place are content editing using image manipulation software, format conversion, print-and-scan operations, analog handy-cam video acquisition, ...

Another approach would apprehend distortions in terms of the amount of nuisance it causes to visual perception. This requires to jointly consider nature and severity of a geometrical deformation. Implicitly, many watermarking algorithms state that complex but tolerable distortions are those which can be well described locally by simpler deformation models such as affine transformations.

Under this approach the set of distortion models that should be considered to address robustness becomes unlimited. Instead, performances should be stated in term of perceptually driven degradation criterion. Although many evaluation criteria have been proposed for non-desynchronizing distortions, very few [6, 7] propositions have been made so far to characterize geometrical deformations. This issue is far from being fully resolved.

Lacking a general evaluation criterion researchers proposed reference deformation model with range of parameters to be tested to compare watermarking schemes performances. A widely used complex deformation model is the deformation known as Stirmark[8, 9]. It consists essentially in a combination of bilinear deformation, global bending, local randomization, interpolation and JPEG compression.

Cropping is an important implementation detail which is seldom discussed. However, as output images cannot include undefined regions, this operation will follow most geometrical deformations. The mathematical expression of the deformation usually does not specify output signal limits. In order to establish robustness of a watermarking scheme, one should mention detailed implementation processes stating whether partial original content was lost, signal center of gravity moved or width to height ratio changed. Figure 2.1 illustrates this often omitted issue.

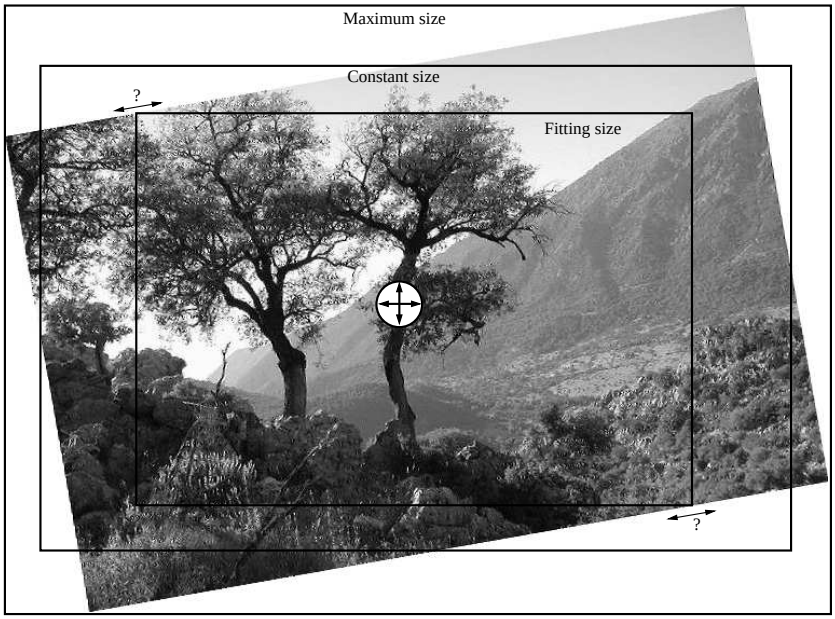


Figure 2.1: *Cropping implementation details.*

2.3 Overview of watermarking schemes dealing with desynchronization

In this section we try to present an exhaustive survey of the watermarking schemes claiming resistance against distortions causing desynchronzations. The classification is organized according to common approaches, reasoning or assumptions in the design of the different schemes. Partial correlation exists between the order of presentation and the chronology or popularity of the different techniques. Some schemes could be categorized in more than one class as they combine several different approaches. However, each work is only cited once, in the most specific class that it belongs to.

2.3.1 A priori knowledge

The first papers (e.g. [10]) addressing the robustness against geometrical distortions considered that the undergone distortion was known at the detection stage. The study only consisted in checking whether the embedded message could still be recovered after a distort-restore process. Given an arbitrary geometrical transformation of the image, the inverse deformation was applied and subsequently the embedded message was extracted.

This consisted in studying the effect of a double interpolation leading to restoration of the original signal on the detection performances. As one might expect, one outcome of this analysis is that high frequency components of the watermark are quite fragile and poorly withstand such operations.

2.3.2 Registration

In some situations, the watermarking scheme can rely on information about the original content to perform watermark detection. These schemes are said non-blind or non-oblivious. The availability of this information depends on the capacity to perform robust identification of the incriminated content. This can be done through soft hashing algorithms combined with efficient database searching techniques. In some applications, one can rely on manual intervention to validate the identification.

In order to recover synchronization, one can therefore use the original undistorted content or stored reference values to establish correspondence between both signals as illustrated in figure 2.2. An inverse deformation

can be estimated and applied to the illicit content before proceeding to the watermark detection.

Signals registration is a widely studied problem in the field of image processing [11, 12]. It plays a crucial role in medical imaging [13]. Important factors in the design of registration algorithms are the assumptions that can be made to characterize the signal content or the relation linking both signals. This justifies the coexistence of multiple techniques, each fitted to specific applications. Among the proposed registration techniques proposed in watermarking, one can find area-based methods [14, 15, 16, 17, 18, 19] and feature-based methods [20, 21, 22, 23, 24]. Other works rely on quasi perfect registration [25]. One might regret that some works do not explicitly state the use of reference from the original content.

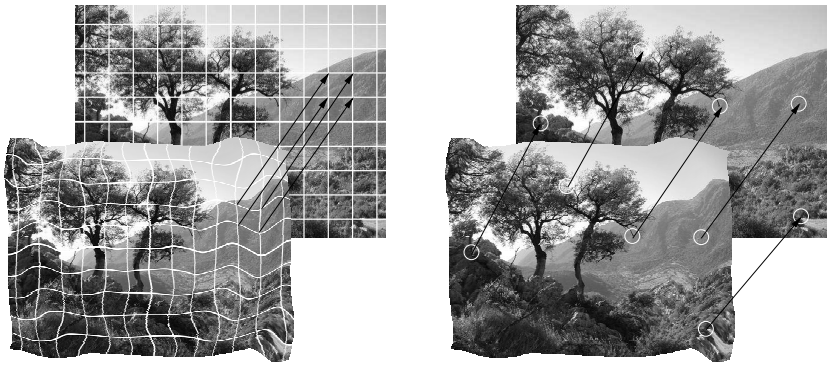


Figure 2.2: *(a)Area and (b)feature-based registration.*

2.3.3 Exhaustive search

This approach consists in considering all deformations that could have taken place, performing accordingly inverse transformation and subsequently performing detection. The embedded watermark is extracted choosing the best detection confidence value which is above appropriated threshold. One must inevitably restrict the search over a set of likely deformation models and a range of distortion parameters. Besides computational constraints, one must carefully study false positive probability as it increases with the size of the search [26, 27, 28].

Considered distortions are generally limited to translation, scaling and rotation. Assumptions on the severity of the distortion can be made to

limit the range of tested parameters. In order to address more complex transform while maintaining reasonable computational cost, detection can sometimes be performed on smaller regions of the image [29, 30] provided sufficient watermark-to-image power ratio is available. Strong hypotheses can be made on the relative continuity or smoothness of the deformation, further reducing the search space [31].

Another mean to reduce search space is to use periodically structured watermarks [32, 33, 34]. It enables to limit search for synchronization over one repetition period. However, one must be careful and prevent opponents from using this organized redundancy to estimate and remove watermark structure.

2.3.4 Synchronization marks

A classical approach in digital communications to identify channel characteristics is the use of training signals also called pilots. These are signals which have known and easily detectable features and therefore do not convey information except their presence. At the receiver, a correct registration of the received signal with the original uncorrupted reference pilot is required to achieve channel estimation.

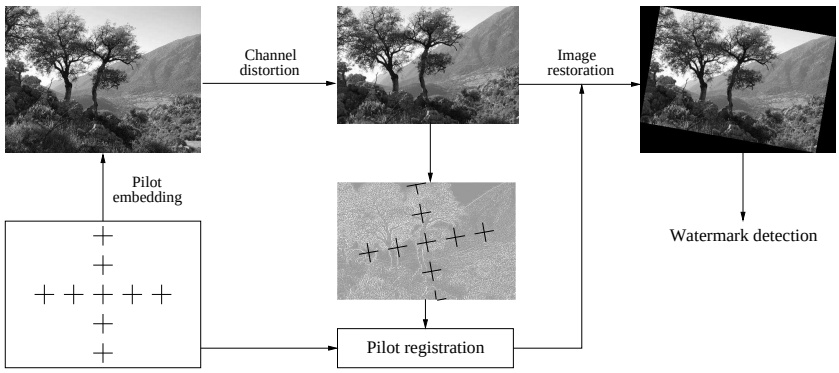


Figure 2.3: *Embedding and registration of synchronization marks.*

In watermarking, such signals have been proposed to fight against geometrical distortions. The detection of these reference signals must be robust to the addressed distortions. This leads to the design of pilots with trivial and clearly identifiable spatial or spectral features. The estimation of the undergone distortion requires an exhaustive search to register detected features with reference pilot.

Several authors propose such an approach performing pilot registration in spatial domain [35, 36, 37]. Others design a reference signal exhibiting strong spectral characteristics, also called template, and proceed accordingly in Fourier related domains [38, 39, 40, 41, 42]. Template registration can often be facilitated using logarithmic and polar mapping of the Fourier representation space [43]. Rotation and scaling distortion reduce to translation in this new representation space, enabling a correlation based detection.

As an alternative to these complementary signals playing the role of reference marks, one can design the informative watermark in such a way that it exhibits robust identifiable features. Such watermark are said to have self-referencing structures. Periodically structured watermarks have been widely proposed [44, 45, 46, 47, 48]. Associated reference marks can be detected in Fourier magnitude spectrum [49] or in the signal autocorrelation function (ACF).

A complementary approach [50] studied the optimal design of synchronization patterns based on the maximization of the Fisher information in a embedder-attacker hiding game.

Compared to exhaustive search approach, using synchronization marks prevents excessive false alarm probability since detection is performed only on suspected (informed) inverse deformation. However, one might expect an increase in missed detection probability or a trade-off between robustness and security issues. This concern was already addressed for template based methods [51] but is also applicable to most other proposed pilots or self-referencing structures.

The following approaches all propose watermark embedding in a transformed domain where channel distortions exhibit "time-invariant" behavior.

2.3.5 Insensitive domain

The most straightforward manner to get rid of spatial synchronization constraints is to express signal in an adimensional space, i.e. a scalar value. Due to capacity objective, this reasoning is applicable only to video watermarking. One can build a watermark with trivial spatial nature but hidden temporal structure.

It has therefore been proposed to embed message in mean luminance value of successive video frames [52, 53]. Other similar works embed spatially robust features along the temporal axis [54, 55]. Although these ap-

proaches exhibit quite insensitive behavior against spatial desynchronization, they are still subject to temporal distortions such as frame dropping, change of frame rate, ...

Another little studied approach is the embedding in the color or luminance representation space [56]. However, robustness to histogram equalization and other color manipulation processes is still challenging.

2.3.6 Fourier magnitude, log-polar mapping, log-log mapping and Fourier-Mellin domain

These transformed domain approaches have been proposed to design watermarking schemes robust to specific class of deformations. They rely on advantageous properties of the Fourier transform. In Fourier domain, magnitude spectrum is insensitive to translation, scaling produces inverse scaling and image rotation yields identical rotation on the spectrum. Performing log-polar mapping of the Fourier domain, rotation and scaling of the image become translations. Combining both transforms as illustrated in figure 2.4, one can design the Fourier-Mellin domain which is insensitive to rigid deformations. Several authors address these kinds of transform [57, 58]. Performing log-log mapping of the Fourier domain provides a representation insensitive to cropping, scaling, and modification of aspect-ratio but not rotation [59]. Discrete implementation of such transforms and their inverse is not straightforward.

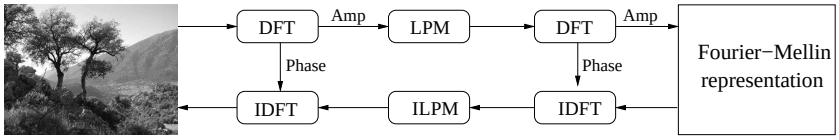


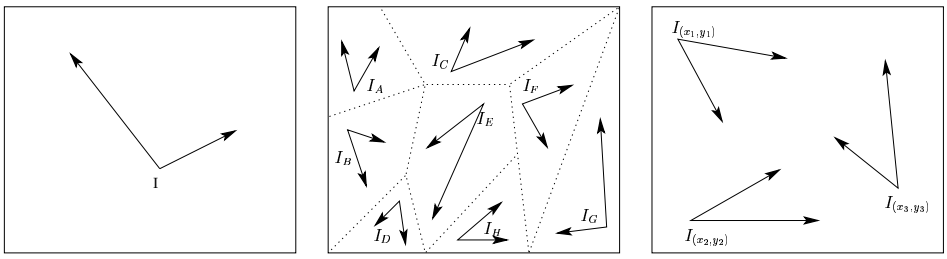
Figure 2.4: *Combining discrete Fourier transforms (DFT/IDFT) and log-polar mapping (LPM/ILPM) to obtain the RST invariant Fourier-Mellin domain.*

2.3.7 Synchronization on content

Most approaches based on signal content use the availability of the image at the embedding stage to perform content normalization. It consists in building reference systems based on robust signal content characteristics. Classical watermark embedding and detection can then be performed on a normalized representation of the image. One expects the content depen-

dent reference system to undergo the same geometrical distortions as the cover signal.

Three different approaches to produce content normalized representations have been proposed. They are illustrated in figure 2.5. In the first group, the entire image signal is expressed in a new global reference system[60]. In the second group, one extracts robust features or objects in the image in order to produce a partitioning of the representation space in several regions. Normalized reference systems are defined over each separated region[61, 62, 63, 64]. The last approach consists in defining a distinct reference system for every location in the image signal [65].



(a) (b) (c)

Figure 2.5: *Different content normalization approaches: (a) Global, (b) region-based, (c) local.*

The main challenge in content based approaches is to be able to cope with partial loss of content in the channel and build robust scale references. Human scale and orientation perception relies on semantic interpretation of the content. Automatic characterization of an orientation is manageable thanks to its cyclic structure, the scale issue on the opposite is intrinsically unsolvable due to its unlimited range. In practical schemes, robustness can nevertheless be achieved for limited amplitude distortions which is satisfactory in many applications.

2.4 Problem statement - Needs

It appears that the synchronization problem in watermarking is still a challenging issue. Current propositions are reliable for handling characterized distortions in specific application scenarios. However, both robustness and security improvements would be mandatory for a wide range of applications. Further refinements are still possible. We believe that fundamental aspects of watermarking have not been exploited to their max-

imum capacity in many proposed approaches. In addition, the so-called robustness provided by several schemes is jeopardized by serious security flaws. Quality assessment tools are missing to correctly address the problem raised by geometrical distortions in watermarking.

In chapter 3, we present a watermarking scheme that we have designed based on periodical spatial patterns and study its related secrecy and robustness issues. We also discuss the detection of its organized structure as synchronization pilot to design affine resilient schemes.

Chapter 4 investigates the content based normalization of a signal. We propose a new local normalization approach and study its robustness under geometrical deformations. We illustrate the use of such representation tool to secure or design robust watermarking schemes.

In chapter 5, we discuss the lack of quality evaluation tools for geometrically distorted images. We present the original approach that we have developed to perform such quality assessment.

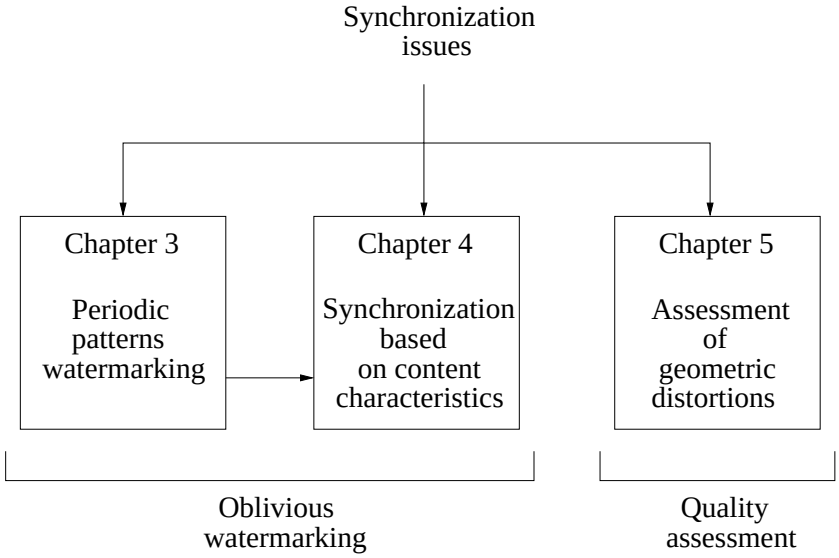


Figure 2.6: *Following chapters description.*

Chapter 3

2-D periodic patterns for image watermarking

The robustness of watermarking algorithms against common geometrical deformations has drawn the attention of many researchers for ten years already. Today, the design of communication systems that are able to recover from loss of synchronization is still an important challenge. In watermarking, the use of periodic structures has been proposed as a mean to fight such distortions. However, the security implications of this periodicity have not always been properly addressed. In this chapter, we first present a method that we have developed to generalize and introduce secrecy in the construction of periodic patterns for watermarking. The resistance against cropping and general affine transformations is presented and the related security and robustness issues are discussed.

Keywords:Watermarking, periodicity, geometrical deformations.

Introduction

Watermarking can be described as a communication over noisy channel problem with specific security constraints. Digital communication systems over noisy channels use channel coding techniques in order to achieve error-free transmissions. These techniques introduce a certain amount of redundancy in the transmitted message which enables a diminution of the rate of error at the price of a lower transmitted information rate. Specific forms of redundancy can enhance the watermark detection performances. However, introducing redundancy can also have

security implications for the watermarking system. These issues will be discussed in the present chapter.

The simplest way to introduce redundancy in a discrete signal is to perform repetition coding, where each symbol of the message is repeated n times and produces a code whose length is n times the original length of the message. In most circumstances, repetition coding is not the most appropriate way to introduce redundancy in a signal. Algebraic and convolutional error coding codes are more complex but also much more efficient channel coding techniques when the channel exhibits sufficiently low error probability. Baudry et al. [66] have studied what is the adequate channel coding strategy using a combination of repetition and BCH or convolutional error coding techniques.

In watermarking systems, the channel is characterized by a very low signal-to-noise ratio. In practical scenarios, only few schemes can achieve perfect rejection of the host signal interference. Therefore some kind of repetition coding will often be required before any other error correcting coding can successfully be used. Moreover, as the communication channel is mostly unknown, one will have to consider the worst case signal-to-noise ratio in the system's design.

Repetition of a set of symbols can be performed in many different ways. Some methods can bring more benefit than others. One specific form of repetition is periodic repetition. One says that a sequence is periodic with period T if the same symbol occurrence can be observed at fixed-size interval of samples.

In watermarking schemes, the use of periodicity in the embedded signal is, besides its channel coding role, motivated by two different but quite related objectives. The first objective is to limit the size of the searching space to one repetition period in methods performing exhaustive search to recover from a loss of synchronization. As illustrated in fig. 3.1 the periodic tiling of an elementary rectangular watermark pattern permits to operate the search for synchronization after a cropping over the area of the size of a single tile. This construction also guarantees that, provided the cropped image remains larger than the elementary tile, it contains an occurrence of every symbol of the hidden message.

The second objective is to benefit from the self referencing structure of the signal. One can analyze the autocorrelation function of the periodic signal to determine which transformation the signal has undergone. This determination is achievable only when the number of periods represented in the signal is sufficiently large.

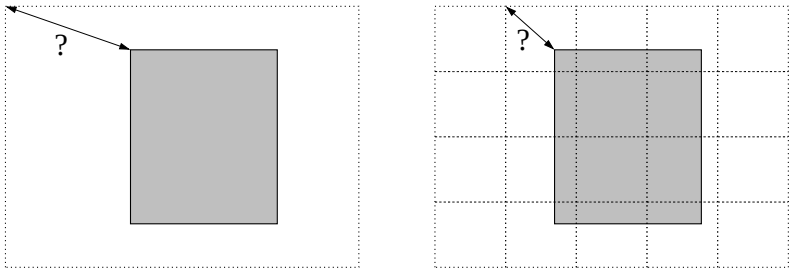


Figure 3.1: *(a) Searching for synchronization with reference marks, (b) tiling an elementary pattern to reduce search space.*

This chapter will present an original generalization method to build periodic n-dimensional discrete signals and set out its advantageous properties for watermarking schemes.

3.1 Weaknesses of watermarking schemes using periodicity

Periodicity, because of its very organized redundancy can introduce security weakness in a watermarking scheme. The channel coding role played by periodicity can also be exploited by unauthorized user to compute an estimate of the embedded watermark through averaging of the signal over the different repetition periods.

Very early papers [67] on watermarking technique already discussed the choice of two-dimensional arrays with useful properties. However, they focused only on cross-correlation properties of rectangular arrays and did not research periodic structures. Existing periodic watermarking schemes [44, 33, 47] propose rigid watermark construction. Indeed, the periodicity results from the tiling of fixed size rectangular elementary pattern as illustrated in fig. 3.1.b . The secrecy of the construction lies only in the nature of this elementary tile. Therefore the repetition periods of the watermark are fixed and publicly known.

An important weakness issue arises in those schemes due to the absence of secrecy in the way the elementary pattern is repeated across the image. This enables any opponent to compute an estimate of the watermark by averaging the signal over the different period repetitions. This opponent would then be able to remove important watermark power from

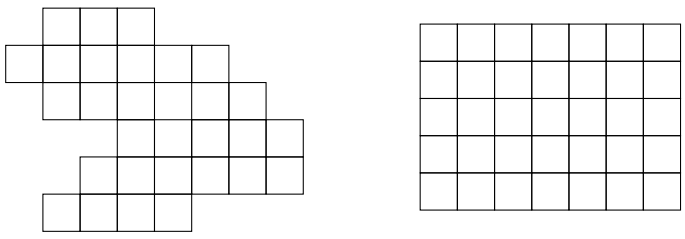
the document or perform a copy-attack [68] on other documents.

The first part of this chapter shows that it is possible to introduce secrecy through a generalization in the construction process of periodic structures. In the second part, we illustrate how one can benefit from periodically structured watermark to estimate undergone affine transformation of the media. We also discuss the security issues in those different usage of periodicity.

3.2 Construction of n-dimensional periodic patterns: a generalization

3.2.1 Problem statement

In the following discussion, we consider finite length discrete multidimensional signals that we refer to as patterns. Each element of the pattern is characterized by an index giving its position in the sequence, and a value belonging to an alphabet of symbols M. In the multidimensional case, the indexes take values in the n-dimensional finite subset K of Z^n. The extend of the pattern is thus given by the set of indexes where a value for the signal is defined. We consider arrays as a category of patterns whose extend results from the inner product of index intervals in each dimension.



(a) (b)

Figure 3.2: *(a) Two-dimensional pattern, (b) Two-dimensional array.*

A n-dimensional pattern w is periodic if there exists $\overrightarrow{T}_1$, $\overrightarrow{T}_2$,..., $\overrightarrow{T}_n$ such that

$$w(\overrightarrow{k}) = w(\overrightarrow{k} + \overrightarrow{T}_i) \qquad \forall i,\ \forall \overrightarrow{k} \in K \mid (\overrightarrow{k} + \overrightarrow{T}_i) \in K. \tag{3.1}$$

When the signal has finite length, this relation must hold only for pairs $(\overrightarrow{k}, \overrightarrow{k} + \overrightarrow{T}_i)$ belonging to the subset of indexes that determine the signal extent.

Given C, a discrete sequence of symbols with length N, we aim at finding a method to construct an arbitrary shaped pattern which contains all the symbols of C in such a way that the pattern is periodic. Moreover, the proportion of each symbol represented in the pattern should tend to the same proportion as in the sequence C when the pattern extent tends to infinity.

3.2.2 Construction scheme

In this section we describe how one can construct different periodic patterns depending on the values chosen as construction keys. The construction method will be described for 2-dimensional patterns, but its extension to n-dimensional patterns is straightforward.

Let S be a 1-dimensional sequence of symbols with length N,

$$S[k], \qquad k = 0..N-1. \tag{3.2}$$

In general cases, no other information about this sequence is known. It could contain N different symbols values. No restriction exists on the length of S.

We start by choosing two keys k_1 and k_2 which can be any integer comprised between 0 and $N-1$. We will explain below which combinations of keys should not be used. The pattern is filled with the elements of the sequence in such a way that there exists in the pattern a constant relation between elements in adjacent positions. If the position (x, y) in the pattern is filled with the i^{th} symbol of the sequence, then we will take the symbol in position $(i + k_1) \bmod N$ in the sequence to fill position $(x + 1, y)$ of the pattern. The construction is illustrated in fig. 3.3. In the same way, the symbol at position (x, y) and the one at position $(x, y + 1)$ are k_2 cyclic positions away in the sequence.

Once a first element is chosen in the pattern, there exists only one way to complete the pattern given the two keys k_1 and k_2.

$$W[x, y] = S[i]; \tag{3.3}$$

$$W[x', y'] = S[(i + k_1 * (x' - x) + k_2 * (y' - y)) mod\ N]. \tag{3.4}$$

Figure 3.4 shows an example construction with initial sequence $S = ['P', 'A', 'T', 'T', 'E', 'R', 'N']$ and construction keys $k_1 = 3$ and $k_2 = 2$ $(N = 7)$.

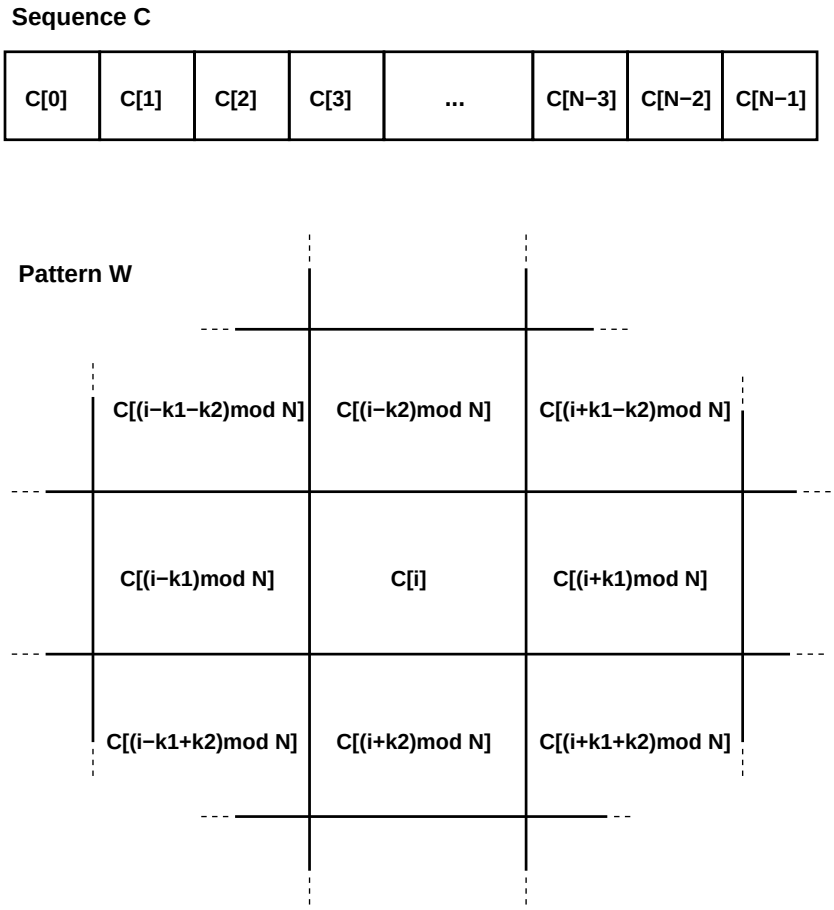


Figure 3.3: *Periodic expansion of a 1-dimensional sequence S onto a two-dimensional pattern*

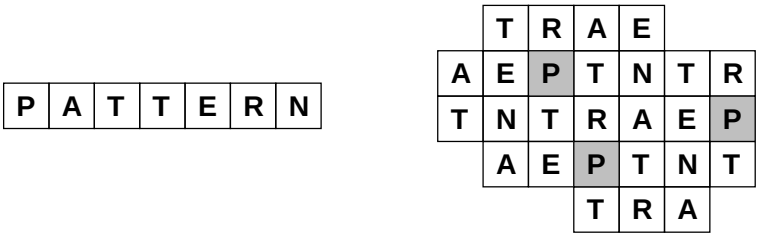


Figure 3.4: *Example pattern construction with construction keys $k_1 = 3$ and $k_2 = 2$ ($N = 7$)*

Some care must be taken while choosing the two keys k_1 and k_2. Indeed, we want that all the symbols of the sequence be represented in the pattern. In order to achieve this, the following condition has to be verified: the greatest common factor between k_1, k_2 and N must be equal to one. When this condition is not satisfied, and say the greatest common factor is m, only N/m out of the N symbols of S are represented in the pattern.

The number of different constructions depends on the length N of the symbol sequence S. If N is prime, then the number of allowed combinations of keys will be N^2. If N is not prime, some combinations will have to be ruled out, and the total number will be slightly smaller. If the factorization of N in prime numbers is given by the following expression,

$$N = f_1^{d_1} \times f_2^{d_2} \times ... \times f_n^{d_n} \tag{3.5}$$

with f_1,f_2,...,f_n being different prime numbers, then the total number of combinations that do not satisfy the above stated condition is

$$N_{excluded} = 1 + \sum_{i=1}^{n} \left[\left(\frac{N}{f_i} \right)^2 - 1 \right] - \frac{1}{2} \sum_{i,j=1(i \neq j)}^{n} \left[\left(\frac{N}{f_i f_j} \right)^2 - 1 \right]. \tag{3.6}$$

The total number of allowed combinations of keys is given by

$$N_{keys} = N^2 - N_{excluded}. \tag{3.7}$$

Figure 3.5 shows the evolution of the total number of suitable combinations of keys in function of the length N of the sequence. One can clearly observe the diminution of the number of combinations for lengths that are multiple of two, three or five.

In the general case where all symbols in S are different, each permutation of symbols in the sequence produces a different pattern owning the same periodic structure. Therefore the total number of different construction of a periodic pattern whose repetition period contains strictly one occurrence of every symbols comprised in a sequence of length N is

$$N_{patterns} = N! \times N_{keys}. \tag{3.8}$$

3.2.3 Reconstruction property

A very interesting property of the pattern construction scheme is the constant relation between symbols located in adjacent positions. It enables reverse processing on the pattern.

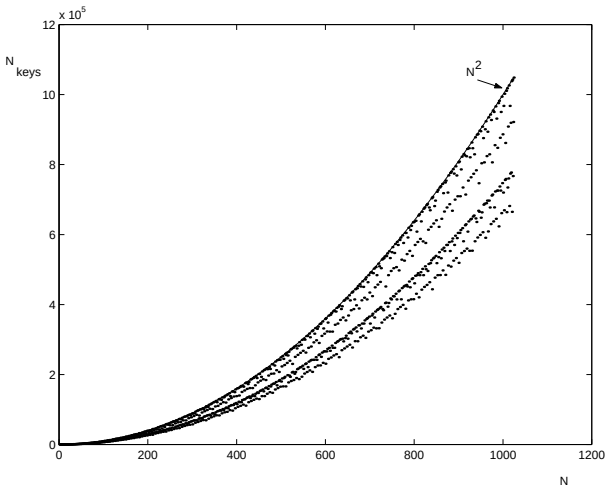


Figure 3.5: *Number of key combinations in function of N*

Let $S[k]$ be the initial ordering of symbols in the sequence before construction of the pattern, that is after a possible permutation of the original sequence. An inverse operation consisting in reconstruction of a sequence $S'[k]$ from the pattern can be performed. It follows from the construction scheme that the reconstructed sequence S' is a circularly shifted version of S whatever position is chosen as reference in the pattern. This is illustrated in figure 3.6 where position $(1, 2)$ was chosen as starting index instead of $(2, 3)$.

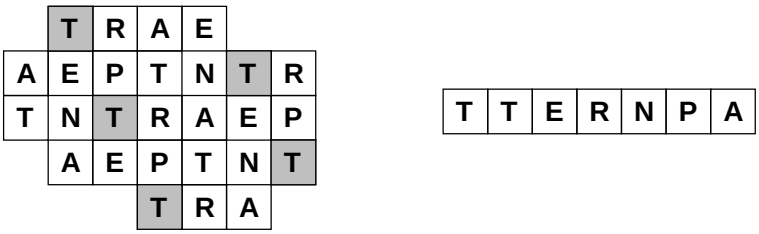


Figure 3.6: *Reconstruction of a circularly shifted sequence*

On the opposite, cyclic permutations of the sequence S produces shifted versions of the periodic pattern in the construction process.

Another consequence is that the 1-dimensional cross-correlation properties of the sequence S are transferred to the two-dimensional constructed pattern. One might for example choose a maximum length se-

quence [69] as initial sequence S to generate a pattern with very good cross-correlation properties.

Note that the construction method does not guarantee that it is possible to obtain a rectangular pattern without truncating repetition periods. This means that 2-D cyclic cross-correlation of an arbitrary shaped rectangular pattern will not necessarily exhibit the same cross-correlation as the sequence. It will however be the case for of few particular arrays. Firstly all arrays of size $N \times N$ whatever combinations of keys are used. Secondly arrays generated by a combination of keys which have common - but different - factors with N. With those keys, the adequate array size is

$$\frac{N}{gcd(N, k_1)} \times \frac{N}{gcd(N, k_2)}. \tag{3.9}$$

3.2.4 Extension to N-dimensional periodic structures

The presented construction can easily be extended to n-dimensional structures. For each dimension, one key has to be chosen. The construction rule is then given by the following expressions

$$W(i_1, i_2, ..., i_n) = S[i]; \tag{3.10}$$

$$W(j_1, j_2, ..., j_n) = S[(i + k_1 * (j_1 - i_1) + k_2 * (j_2 - i_2) + ... + k_n * (j_n - i_n)) mod\ N]. \tag{3.11}$$

The considerations concerning the choice of key values can easily be derived from the 2-dimensional case.

3.3 A spatial watermarking scheme based on generalized 2-D periodic patterns

In this section we present a practical watermarking scheme using the afore described generalized periodic pattern structures. The proposed scheme is a spatial domain additive scheme for grayscale image. The watermark embedding procedure can be expressed as follows:

$$I_w(x, y) = I(x, y) + \alpha(x, y)\, W(x, y), \tag{3.12}$$

where I_w is the watermarked image luminance, I the original image luminance array, α a perceptual weighting factor array and W the watermark array. All arrays have the same size as the original image.

3.3.1 Watermark construction

Let M be a binary sequence of length N_m representing the message to be hidden in the image. A succession of processing steps applied to this sequence M lead to the watermark array. The global procedure is illustrated in figure 3.7.

The first operation consists in performing convolutional error correcting coding on the message sequence M to produce a coded message C with length N_c. The code rate N_m/N_c is limited by the channel bit error probability and the capacity of the cover image. Indeed, the subsequent steps in the watermark construction perform pure repetition coding of the coded sequence C aiming at the achievement of a satisfying bit error probability on the coded message. Above a certain threshold, convolutional coding does not perform better than repetition coding.

In a second step, the bits of the coded message C are randomly repeated to form a new code sequence S with length N_s. This expansion is dependent on key k_0. One should take care that all the bits are equally repeated, such that N_s is a multiple of N_c. This operation can include bit inversion in such a way that an equal number of 1's and 0's is guaranteed in S and therefore that the watermark pattern embedding into the image does not change its mean luminance value.

The role of this expansion is to increase the size of S in order to increase the number of possible different pattern constructions and at the same time control the size of each periodic repetition in the pattern. One has to check that the random repetition does not produce a periodic sequence, otherwise the pattern construction will produce the same structures as if sequence S was truncated to one repetition period.

The next operation is the periodic pattern construction as detailed in previous section. We will call S the generating sequence of the pattern. The pattern dimensions are the same as the cover image. One difference with the description from section 3.2 is that each cell of the pattern covers an array of R_x by R_y pixels in the cover image. The repetition of the same bit value over an array of pixels permits to limit the high frequency components of the watermark. Most high frequencies do not survive common compression and interpolation operations.

The parameters $N_c, N_s, k_0, k_1, k_2, R_x$ and R_y will determine the watermark repetition structure. In a practical application, three parameters have fixed value: the watermark message length N_m, image expected size and the worst channel characteristics. Image expected size means minimum size of image from which the message should be recovered. The rest of the

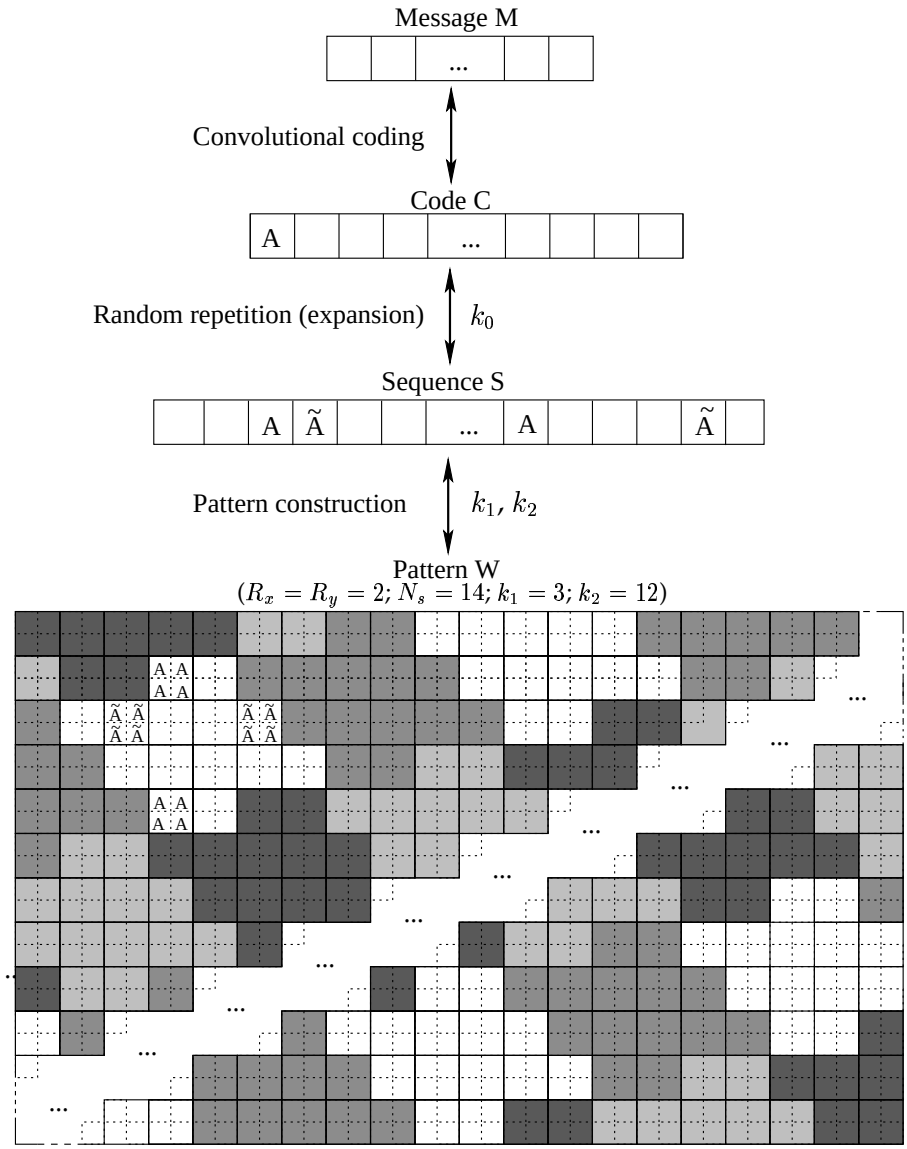


Figure 3.7: *Watermark pattern construction*

parameters should be optimized for each situation.

3.3.2 Perceptual masking

The design of the weighting factor α in equation 3.12 is motivated by the will to minimize the image degradation while maximizing the detection reliability. This leads to the shaping of the watermark signal to fit image characteristics. Most approaches consist in optimizing watermark power distribution with perceptual sensitivity considerations. The easiest way to perform perceptual masking is to apply local scaling to the watermark proportional to a local activity measure of the cover image. An effective measure of local activity is the Laplacian high pass filter

$$L = \begin{bmatrix} -1 & -1 & -1 \\ -1 & 8 & -1 \\ -1 & -1 & -1 \end{bmatrix} /8. \tag{3.13}$$

Another perceptual consideration is the lower sensibility of the human eye to a change of luminance for darker luminance intensity levels. This effect is rendered by Weber's law.

A combination of Laplacian high pass filtering and Weber's law based weighting was chosen as scaling factor α for our method. Other more effective masking methods based e.g. on anisotropic wavelet decomposition analysis could be used. Many authors [70, 71, 72] have proposed human visual sensitivity models for watermarking applications. The comparison of existing perceptual masking models was not addressed in this work.

3.3.3 Detection scheme

The present detection strategy considers the watermarking channel as linear time invariant with additive noise. The proposed detection scheme is essentially correlation based. As the message bits are randomly distributed over the generating sequence S, the pattern elementary period can be considered as spectraly white. From detection theory, we know that correlation detectors are optimum in presence of linear time invariant channels with additive white Gaussian noise (AWGN). However, in watermarking channels, noise is due to the cover image where neighbouring pixels are highly correlated. Detection improvement can be achieved through whitening of the cover image spectrum prior to the correlation operation [73]. This necessitates a decorrelating filter. The following FIR

filter is appropriate for this operation:

$$F = \begin{bmatrix} 1 & -2 & 1 \\ -2 & 4 & -2 \\ 1 & -2 & 1 \end{bmatrix} /4 \tag{3.14}$$

After the image has been filtered, one must proceed to the inverse construction of an estimated generating sequence S', according to the construction keys. The sequence results from the averaging of the different repetitions of the elementary pattern over the image. As pattern cells are spread over R_x by R_y pixels, as many different sequences S' corresponding to the possible cell shifts have to be considered. The sequence leading best final correlation value will be retained. If the image was watermarked with the same keys, the inverse construction process will produce a sequence which is a circularly shifted estimate of the original sequence S used to construct the watermark pattern. One has to retrieve the undergone shift. This is performed through the correlation of the estimated sequence S' with N_c different masks corresponding to each of the different bits in the coded message C. Those masks $m_1, m_2, .., m_{N_c}$ are vectors constructed thanks to the knowledge of key k_0 that was used to distribute the bits of C over the generating sequence S. They are constituted of $1, -1$ and 0's according to the position of the different occurrences of each bit of C in sequence S. Let N be the number of occurrences of each bit of C in S,

$$N = \frac{N_s}{N_c}. \tag{3.15}$$

For each circular shift, the N_c normalized correlation values of sequence S' with the different masks are squared and summed as expressed as follows:

$$d_k = \sum_{i=1}^{N_c} \left[\frac{m_i^T S'_k}{N} \right]^2, \tag{3.16}$$

where S'_k is a cyclic permutation of S'. The shift k leading to the maximum correlation value indicates the most probable undergone circular shift. This maximum correlation value d_{max} constitutes the decision criterion of the watermark detection process:

$$d_{max} = \max_k d_k. \tag{3.17}$$

Considering this shift, an estimated coded message C' is generated where each value results from the averaging of the different occurrences of each

bit in S' according to k_0. The last operation consists in decoding the coded message C' through a Vitterbi soft decision algorithm and produce the decoded message M' .

In order to decide whether the image was watermarked, the decision criterion d_{max} has to be compared to a pre-defined threshold value. The threshold value T can be fixed according to the Neyman-Pearson strategy. This consists in setting a maximum false alarm probability that cannot be exceeded. Two exclusive hypotheses have to be defined:

- H_0 The image was not watermarked.
- H_1 The image was watermarked.

The probability of false alarm is defined as

$$P_{fa} = Prob[d_{max} > T \mid H_0], \tag{3.18}$$

and the probability of missed detection is defined as the probability that we consider the media not watermarked although it is:

$$P_{md} = Prob[d_{max} < T \mid H_1]. \tag{3.19}$$

Under the hypothesis that the image does not contain a watermark and that the image signal was efficiently whitened, the elements of sequence S' are i.i.d Gaussian variables,

$$S'(j) \sim N(0, \sigma^2) \qquad 1 \leq j \leq N_s. \tag{3.20}$$

Each correlation output with one of the mask m_i has therefore a Gaussian distribution

$$\frac{m_i^T S'_k}{N} \sim N(0, \sigma^2/N) \qquad \forall i, k \tag{3.21}$$

which can be normalized to standard normal distribution $\sim N(0, 1)$. Although the elements of S' can exhibit some residual correlation due to imperfect cover signal whitening, each correlation output (Equ. 3.21) results from the random combination of an important number of elements in S' and can reliably be considered as independent variables. Let's denote D_k the random variable describing d_k realizations for a given shift k and p_{D_k} be the probability density function associated to D_k. Under the hypothesis that the N_c correlation outputs for a given shift k are independent, accordingly to equation 3.16 and provided correlation outputs are normalized, p_{D_k} takes the form of a χ^2 distribution with N_c degrees of freedom.

$$p_{D_k|H_0}(x) = \frac{x^{\frac{N_c}{2}-1} e^{-\frac{x}{2}}}{2^{\frac{N_c}{2}} \Gamma(\frac{N_c}{2})} \qquad \forall k. \tag{3.22}$$

The cumulative distribution function is given by the incomplete gamma function γ as expressed in following expression:

$$Pr\left[D_k \leq x \mid H_0\right] = \gamma(x, \frac{N_c}{2}) = \left[\Gamma(\frac{N_c}{2})\right]^{-1} \int_0^x t^{\frac{N_c}{2}-1} e^{-1} dt. \tag{3.23}$$

The detection criterion d_{max} is the maximum value of d_k among all N_s possible shifts k, for a given realization of S'. Expression 3.22 is the distribution of d_k realizations for a fixed shift k or for independent S' realizations. In our scenario, the N_s different detection values d_k are derived combining all realizations from the fixed set of realizations in S'. For this reason, distribution of D_k for varying shifts k will not exactly fit the χ^2 distribution. The way that it will differ from χ^2 distribution is described below.

The mean and variance of a χ^2 distribution with N_c degree of freedom are given by

$$\mu = N_c; \tag{3.24}$$

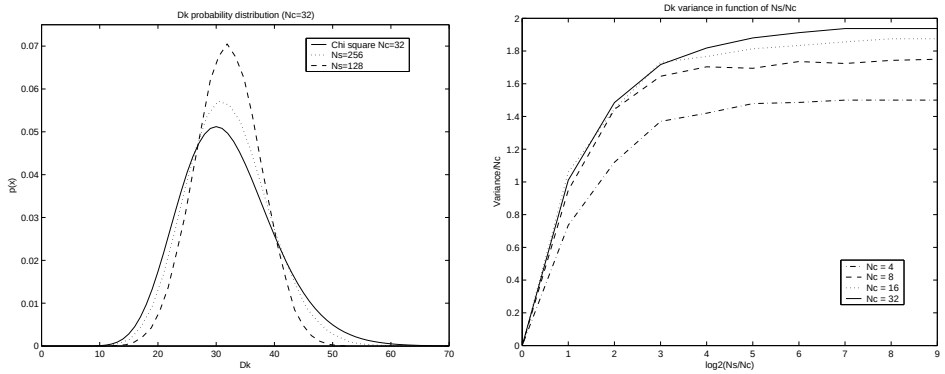
$$variance = 2N_c. \tag{3.25}$$

In our case, distribution p_{D_k} differs from the χ^2 distribution in accordance with the values of N_s and N_c. One can show that the first moment will still be N_c but the variance will take values comprised between 0 and $2(N_c - 1)$ depending on the ratio N_s/N_c.

One can easily verify that, when $N_s = N_c$, all d_k take the same value (N_c) and thus the variance of distribution p_{D_k} is equal to zero. This behaviour is illustrated in figure 3.8. Figure 3.8.a shows p_{D_k} distributions for different N_s values with fixed N_c. Figure 3.8.b shows the evolution of the variance of p_{D_k} as a function of N_s/N_c ratio.

From figure 3.8.b one can realize that expression 3.22 becomes a quite good approximation of p_{D_k} when N_c is large enough and the N_s/N_c ratio is important. The validation of this hypothesis will be illustrated by experimental results in the following section.

In the following, we consider that the elements of S' are independent and that N_c and N_s/N_c are large. Under these assumptions, expression 3.22 being a legitimate approximation the distribution of D_k, one can compute the probability distribution of D_{max}. Since d_{max} results from the maximum value of $d[k]$ over all shifts k, the distribution of variable D_{max} is expressed as the distribution of the maximum of N_s independent realiza-



(a) (b)

Figure 3.8: *(a) Probability distribution of Dk , (b) Variance in function of N_s/N_c ratio.*

tions of a χ^2 variable d_k:

$$p_{D_{max}|H_0}(x) = N_s * p_{D_k|H_0}(x) * \left[1 - \gamma(x, \frac{N_c}{2})\right]^{N_s - 1}. \tag{3.26}$$

The probability of false alarm for a fixed shift k and threshold value T is thus given by

$$P_{fa,k}(T) = Pr[D_k > T] = 1 - \gamma(T, \frac{N_c}{2}), \tag{3.27}$$

while the total probability of false alarm given a threshold T is the probability that the maximum detection value be greater than T:

$$P_{fa,tot}(T) = Pr\left[D_{max} > T\right] = 1 - (1 - P_{fa,k})^{N_s}. \tag{3.28}$$

Given a maximum acceptable false alarm probability, a threshold value T for the decision criterion d_{max} can be derived. Figure 3.9 illustrates the probability mass functions and probability of false detection for D_k and D_{max} computed with fixed N_s and N_c values.

Notice that, when the elementary cell of the periodic pattern covers more than one pixel ($R_x > 1$ and/or $R_y > 1$), a different d_{max} is computed for every $R_x \times R_y$ sub-cell shift. The total number of D_k realizations is thus multiplied by the size of the cell. The new distribution of D_{max} will be obtain using

$$N_{s'} = R_x * R_y * N_s. \tag{3.29}$$

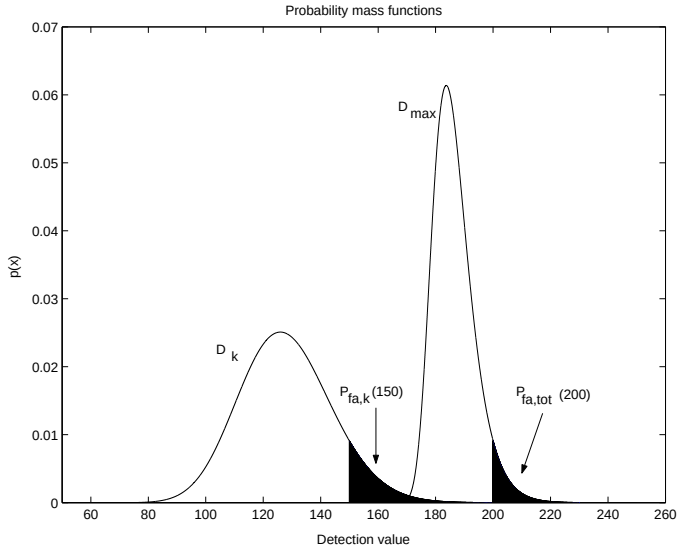


Figure 3.9: *Probability mass functions and probability of false detection ($N_s = 1024$, $N_c = 128$).*

3.3.4 Properties of the watermarking scheme

Whitening of the cover media and detection probability

Experimentation shows that hypothesis 3.20 is quite verified. Pattern structure produces normally distributed variable. Indeed samples originating from distant location in the image are uncorrelated. Figure 3.10 shows the pdf of d_{max} for different test images. Detection value d_{max} was computed over four different unwatermarked images with 5000 different key combinations with $R_x = R_y = 2$. The last image was composed of random Gaussian pixel luminance values. Detection curves of non-watermarked images are quite insensitive to image content.

Figure 3.11 shows that, as discussed in previous section, experimental detection results match more closely theoretical expression of $p_{D_{max}}$ when the N_s/N_c ratio increases.

For schemes designed with small N_s/N_c ratio, one can also experimentally estimate $p_{D_{max}|H_0}$ and set the threshold value to an appropriated level. When N_c is large, these distributions can be reasonably approximated by standard normal distribution such that

$$Pr\left[D_k < x \mid H_0\right] \approx Q\left((x - \mu_{exp})(\sigma^2_{exp})^{-\frac{1}{2}}\right) \tag{3.30}$$

(a) lena 512x512 (b) Boat 512x512 (c) Baboon 512x512

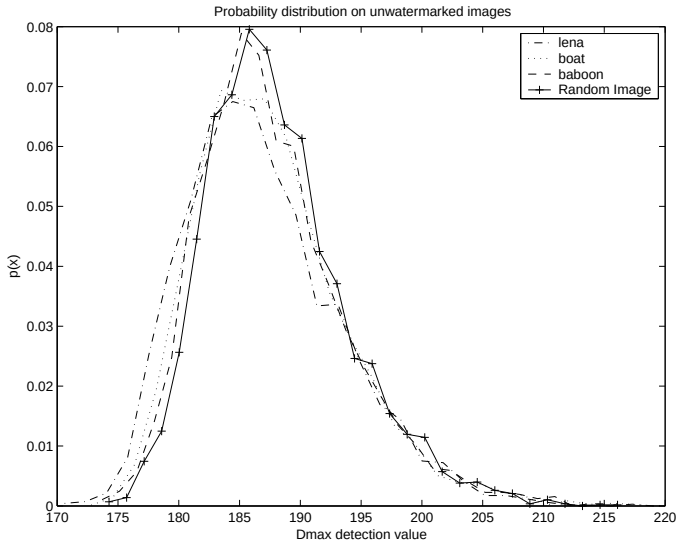


Figure 3.10: *Detection statistic over unwatermarked images ($N_s = 1024, N_C = 128$).*

where

$$Q(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{\frac{y^2}{2}} dy. \tag{3.31}$$

Invariance to cropping

A nice property of the detection scheme is that it is fully insensitive to spatial discrete shifts. As previously described, a loss of reference produces cyclic shifts in the correlation sequence. The detection schemes performs an exhaustive cross-correlation to recover from this cyclic shift. If shifts are fraction of pixels, performances will be slightly degraded due to in-

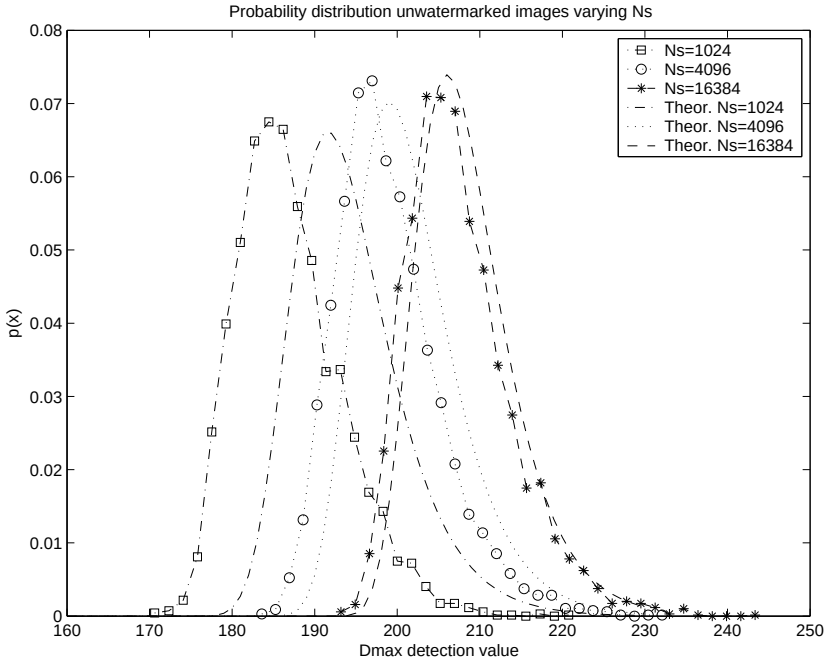


Figure 3.11: *Correspondence between theory and simulation for varying N_s.*

terpolation. Figure 3.12 shows the effect of a fractional cropping (maintaining constant image size) followed by cubic spline interpolation [74] on bit-error rate.

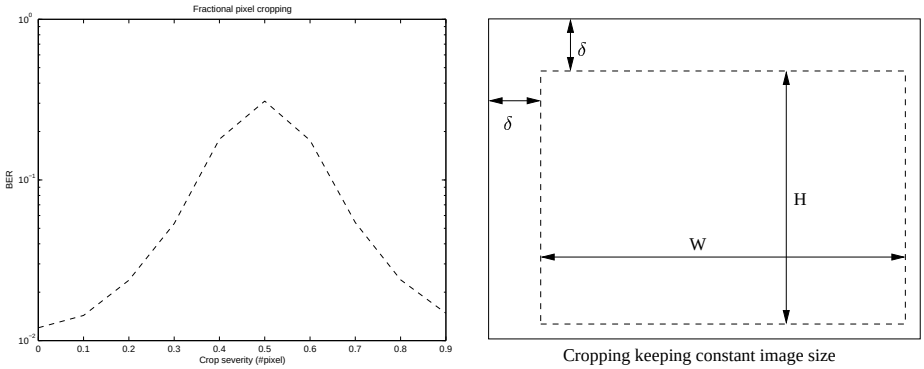


Figure 3.12: *Crop of a fraction of pixel and interpolation.*

This property also permits to boost the detection performances using

side information at the embedding stage. This strategy is also called performing informed embedding procedure [75, 76]. Since the cover media is known to the encoder, one can optimize the coding process in order to adapt the watermark to the channel characteristics. The procedure consists in looking for the shift of the to-be-embedded watermark pattern which leads to the best correlation value with the cover image. The number of different shifts that can be considered is equal to $N_s \times R_x \times R_y$. The resulting increase in performance is illustrated in figure 3.13 using 5000 different key combinations.

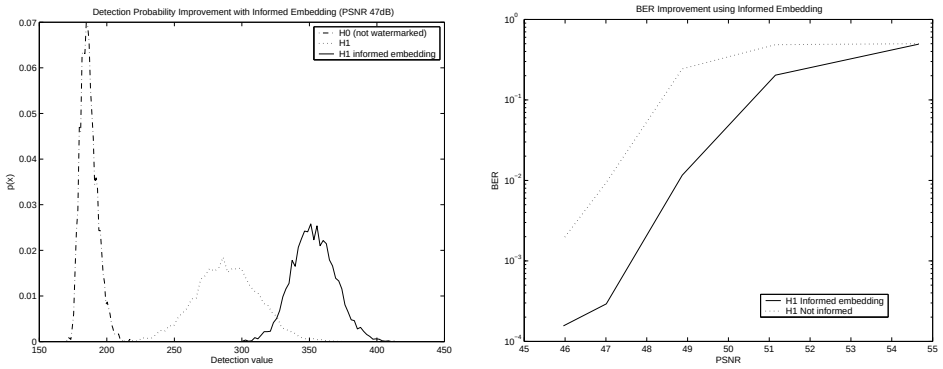


Figure 3.13: *Detection and BER improvement using informed embedding.*

One must keep in mind that exhaustive search for synchronization tends to increase the probability of high detection value on a content which is not watermarked. In order to maintain constant false positive alarm probability, one should therefore increase decision threshold at the price of a higher probability of missed detection [26]. A benefit of the cyclic pattern construction is that the exhaustive search for spatial shifts is always bounded by the size N_s of sequence S as expressed in equation 3.28. This ensures that the false alarm probability is not increased excessively.

When informed embedding procedure is applied, $Pr[d_{max} > x \mid H_1]$ also increases with N_s. This tends to show that it is not necessarily detrimental to increase the size of the space in which exhaustive search is performed. It will however have a computational cost. Figure 3.14 compares detection probability for different sizes of N_s. As N_s increases, detection probability progressively shifts toward higher values. However, as this occurs under both H_0 and H_1 conditions, it is not evident that the required increase of decision threshold value to maintain a constant P_{fa} will lead to an increase of P_{md}.

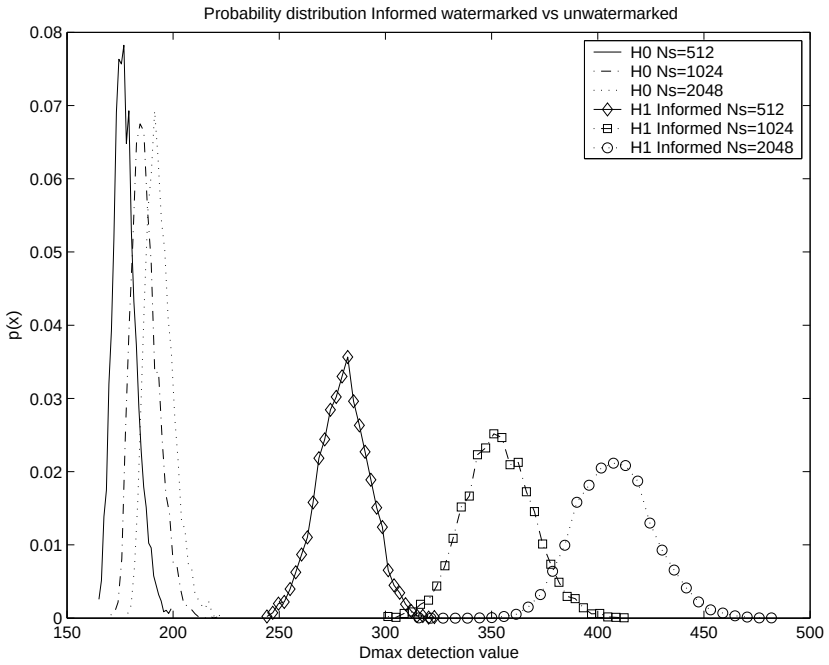


Figure 3.14: *Detection improvement using informed embedding with increasing Ns.*

Such an informed embedding approach to improve resistance against loss of spatial synchronization could be extended to more complex transformation than translation. One might consider rotation, scaling or even very complex transformations. Considering a watermarking scheme which is reasonably insensitive to a class of geometrical distortions, one can attempt to distort watermark structure in a profitable way in order to exploit cover signal interference while ensuring the ability for the scheme to recover from the desynchronization. This is illustrated in figure 3.15. For scheme proceeding by exhaustive search, it is especially true if the space in which synchronization must be recovered is of limited size. This is the case for rotations and also for translation using our cyclic watermark pattern construction. In other words, if the detection scheme is designed to survive any rotation, then the embedding process should adapt watermark pattern considering all possible rotation of the cover media.

For transformations where the space in which we have to look for synchronization is unlimited, such as scaling, hypothesis should be made on the severity of a plausible geometrical distortion. However in these latter

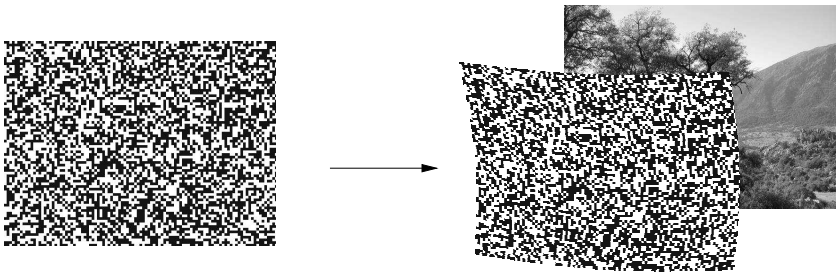


Figure 3.15: *(a) Geometrical adaptation of the watermark to the content.*

situations, in order to be robust, the detector will always need to consider a larger search space than the embedder. Indeed, any geometrical attack might further distort the already deformed watermark pattern. It should be studied whether improvement can be reached enlarging search space for informed embedding purpose.

Security issues

The specificity that also motivated the design of the scheme is the close control on secrecy issues that it provides. Indeed, many different parameters influence the construction process, making the watermark repetition structure unknown to unauthorized users. The length of the generating sequence S plays an important role. Firstly, it determines the total number of different repetition structures which is linked to the computational complexity of an exhaustive search attack. Secondly, it represents the extend of one periodic repetition in the pattern which must be chosen carefully. Indeed, as we will describe in section 3.4 periodic structures can be revealed through autocorrelation or Fourier analysis. However, it can be done only when a sufficient number of repetition periods are observable in the signal. Therefore, in order to ensure secrecy, one must take care that the elementary periodic structure is large enough with respect to the image size. The proposed scheme enables precise adjustments of the construction parameters depending on the image size and the watermark embedding power. One can realize also that the informed coding process provides additional security by making more difficult the exploitation of the availability of different contents watermarked with the same keys.

3.3.5 Video watermarking

A classical discussion in video watermarking is how to use temporal dimension. This new dimension enables to introduce additional redundancy to increase watermark-to-noise ratio. The same considerations can me made as for 2-dimensional media content regarding synchronization issues. Repetition of the same watermark pattern accross multiple video frames makes the scheme less sensitive to frame rate changes, but gives an opponent means to estimate the hidden pattern.

As described in section 3.2.4, our pattern construction scheme can easily be extended to 3-dimensional structures. Successive frames would be watermarked with spatially shifted versions of a same 2D pattern according to the value of a secret temporal key. This watermark has a temporal periodic structure. Such a scheme would exhibit the same properties as the image watermarking scheme described in section 3.3.

3.4 Using periodic structures to estimate undergone geometrical distortion

In communications, a classical approach to inform the receiver about channel characteristics is to use pilot signals. These are signals which have known and easily detectable features and therefore do not convey information. At the receiver, a correct registration of this received signal with the original uncorrupted pilot is required to perform channel estimation.

This technique is used in watermarking to design systems that are able to recover from geometrical distortions. Most approaches rely on the introduction or exploitation of robust singularities in the watermark signal, which can be detected even after various geometrical deformations. This pilot signal which is also embedded into the cover image is often called reference watermark in opposition to the informative watermark which conveys a message.

Two different classes of methods exist. In the first class, the pilot signal is distinct from the informative watermark. It is usually called a template signal and often consists in a signal exhibiting peaks in the magnitude of the Fourier spectrum of the image. Different authors [38, 39, 77, 51] have addressed the use of such pilot signals in watermarking.

In the second class of methods, the pilot signal results from a particular structure of the informative watermark which exhibits exploitable singularities. Periodically structured watermarks have such characteristics.

Indeed, the analysis of the autocorrelation function or magnitude of the Fourier spectrum of such structures reveals peaks organized on a well defined grid alignment. These watermarks are said to be self-referencing. With such structures, the pilot signal does not introduce additional degradation to the image. Several authors [44, 46, 45, 47, 48, 49] have studied the implementation of such methods. The detection of periodicity in a 2-dimensional signal will be the subject of this section.

The reference watermark used as pilot signal must keep its characteristics even after geometrical distortions. One can realize that a two-dimensional periodic signal will remain periodic when the geometrical deformation can be expressed as an affine transformation.

3.4.1 Detection of periodicity in autocorrelation function versus Fourier magnitude spectrum.

The observation of the periodic nature of a finite signal depends on the number of periods that are represented. The periodization of a signal gives a discrete nature to its Fourier representation. When the period becomes large relatively to the observation window, this discrete nature is hidden by the windowing effect and different peaks become harder to distinguish from one another. In the same way, the autocorrelation function of a periodic signal produces peak values for shifts that are multiple of the base period. If the period becomes large, fewer peaks will be observable. In both situations, peaks are organized along a grid which is function of the repetition periods and directions.

When the periodic watermark signal is embedded in the image, detection of these characteristics is complicated by the noise resulting from the cover image characteristics. Therefore, robust detection strategies have to be designed. Few works studied how one can perform detection in low watermark-to-image power ratio. Recently, some authors [49] proposed a method to detect Fourier magnitude peaks using Hough transform. Works proposing autocorrelation based detection [44, 48] did not discuss robust detection strategies. In this section, we describe how one can perform robust detection of periodic watermark structure based on the autocorrelation function and illustrate with results using the watermark construction described in section 3.3.

3.4.2 Grid alignment detection in autocorrelation function

The subsequent steps leading to the grid determination will be illustrated with results coming from the example scenario in figure 3.16. Image Lena (512×512) was watermarked using method from section 3.3 with a PSNR of 44.9 dB. The watermarked image contains 16 repetitions of the elementary pattern. In fig. 3.16.b, a scaling of 111% followed by a rotation of 7 degrees and appropriate cropping was applied to the watermarked image. The periodic grid was recovered and the deformation was inverted to produce image 3.16.c. The 64 bits payload could succesfully be extracted.

(a) Watermarked image (b) Distorted image (c) Restored image

Figure 3.16: *Rotation (7°) and scaling (111%) applied to the watermarked image.*

The first step in the detection process consists in the computation of the autocorrelation function of the estimated watermark. Subsequently, a decorrelating filter is applied in order to further reduce the contribution of the cover image. Peaks are extracted using a sliding observation window and a local threshold. The parameters are chosen to target a number of detected peaks in order to limit the complexity of subsequent steps. In our example, a total of 162 peaks were detected. The location of these detected peaks in the autocorrelation function is represented in figure 3.17, expected locations are illustrated by circles.

The challenge is to identify the peaks that result from the autocorrelation of the periodic pattern. These peaks are organized along a regular grid which can be determined by two vectors $\overrightarrow{a}$ and $\overrightarrow{b}$:

$$\overrightarrow{v} = k\overrightarrow{a} + l\overrightarrow{b}, \tag{3.32}$$

with k and l taking integer values. The grid is defined by the set of points $\overrightarrow{v}$ satisfying expression 3.32. This description supposes that the origin

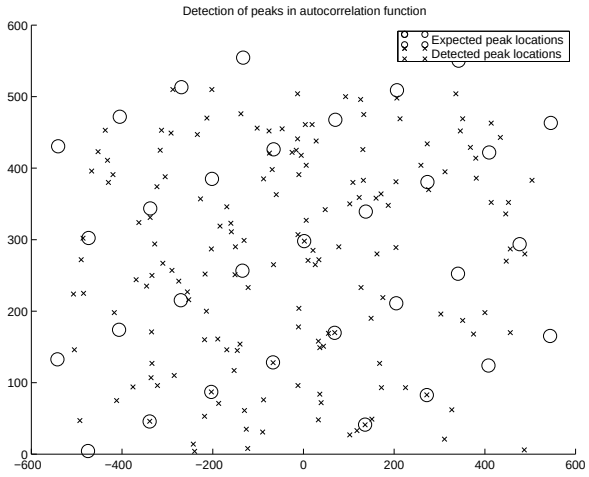


Figure 3.17: *Detection of peaks in the autocorrelation function.*

$(0, 0)$ is part of the grid. The density $\mathcal{D}$ of the grid is defined as the inverse of the L2-norm of the cross product of $\overrightarrow{a}$ and $\overrightarrow{b}$:

$$\mathcal{D} = \frac{1}{\left\| \overrightarrow{a} \times \overrightarrow{b} \right\|}. \tag{3.33}$$

The problem can be stated as follows: given a set of points $\mathcal{G}$, corresponding to detected local maxima in the auto-correlation function, find the largest subset of $\mathcal{G}$ such that all points belong to the same regular grid and $\mathcal{D} < \mathcal{D}_{max}$. The restriction on the value of the grid's density must be set in order to avoid erroneous grid detection. The probability to find a set of points belonging to the same grid increases as the density of the grid becomes larger. When the grid density tends to infinity, any point becomes part of the grid. Therefore $\mathcal{D}_{max}$ must be set relatively to the smallest possible size of the repetition pattern.

Considering all possible subsets of $\mathcal{G}$ becomes computationally unacceptable when the number of points in $\mathcal{G}$ gets large. In order to limit computation time to less than a minute on a common personal computer unit, a maximum of 30 points could be processed. A practical approach is proposed to perform a preselection among the detected peaks.

The preselection proceeds through the computation of a confidence value for each detected peak. All possible combinations of three points $\overrightarrow{v}_1$, $\overrightarrow{v}_2$ and $\overrightarrow{v}_3$ are analyzed. The confidence of each point of the com-

bination is credited if one of the points can be expressed as an integer combination of the two other points:

$$\begin{aligned} \overrightarrow{v}_1 &= k_1 \overrightarrow{v}_2 + l_1 \overrightarrow{v}_3 \qquad k_1, l_1 \in \mathbb{Z} \\ &\text{or} \\ \overrightarrow{v}_2 &= k_2 \overrightarrow{v}_1 + l_2 \overrightarrow{v}_3 \qquad k_2, l_2 \in \mathbb{Z} \\ &\text{or} \\ \overrightarrow{v}_3 &= k_3 \overrightarrow{v}_1 + l_3 \overrightarrow{v}_2 \qquad k_3, l_3 \in \mathbb{Z}. \end{aligned} \tag{3.34}$$

These relations can be verified through the projection of the first vector on each two other vectors. Approximations have to be considered because of the discrete form of the autocorrelation function.

The result of this preprocessing is illustrated in figure 3.18. Each detected peak is represented by a circle whose radius is proportional to the confidence measure. The preselection consists in choosing the 15-25 points with highest confidence measure. An additionnal weighting factor could take into account the varying intensity of the detected maxima in the autocorrelation function.

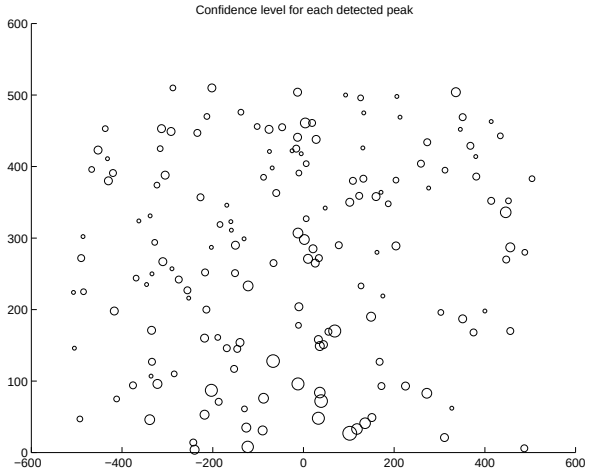


Figure 3.18: *Confidence measure for extracted peaks.*

One can now look for the largest subset of points belonging to the same grid with density $\mathcal{D} < \mathcal{D}_{max}$. All possible subsets have to be considered, starting with the subsets containing the largest number of points. For a given subset of points, the determination of the grid's base vectors $\overrightarrow{a}$ and $\overrightarrow{b}$ can be performed by an iterative algorithm. Two points belonging to

the set are chosen as starting base vectors. At each step, the biggest base vector is replaced by a smaller vector derived from a point not yet part of the intermediate grid. The iteration stops when all points are part of the grid or the density becomes larger than $\mathcal{D}_{max}$. At each step, in order to limit the accumulation of approximation errors, new estimations of the base vectors are computed using a least square error criterion. The first grid that is found with density smaller than $\mathcal{D}_{max}$ is selected. In our example, the subset of points leading to an acceptable density is represented by the black dots in figure 3.19. One can realize that these points correspond with the expected autocorrelation peaks of figure 3.17.

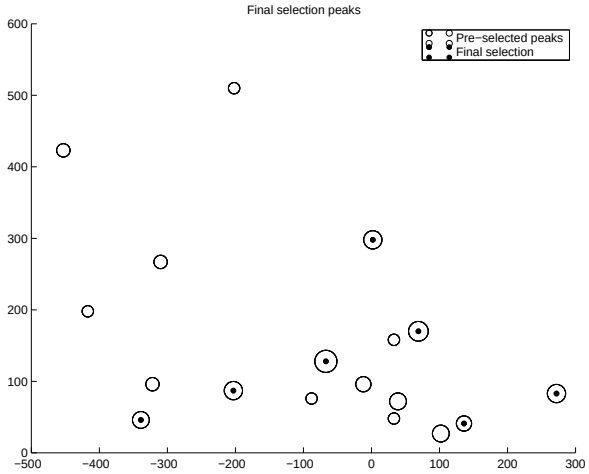


Figure 3.19: *Final selection of peaks.*

3.4.3 Estimation of the undergone deformation and informed detection

Once a regular grid has been detected, the base vectors can be compared with those from the grid that was used to watermark the image. Given the two original base vectors $\overrightarrow{a_o}$ and $\overrightarrow{b_o}$ and detected base vectors $\overrightarrow{a}$ and $\overrightarrow{b}$, there exists only one affine transformation described by matrix A such that

$$\begin{aligned} \overrightarrow{a} &= A\,\overrightarrow{a_o} \\ \overrightarrow{b} &= A\,\overrightarrow{b_o}. \end{aligned} \tag{3.35}$$

Actually, one has to consider 8 different possible affine transformations as vectors $-\overrightarrow{a}$ and $-\overrightarrow{b}$ are also base vectors for the detected grid and $\overrightarrow{a_o}$ and $\overrightarrow{b_o}$ can be permuted.

In order to determine which transformation took place, one can try inverting exhaustively all eight possible transformation and perform watermark detection. One can also restrict the set of transformations to be considered to geometrically acceptable transformations. Indeed, most erroneous estimations will lead to transformations that induce severe perceptual nuisance. One can therefore rule out excessive aspect ratio change, shear or rotations.

This hypothesis on the distortion severity can also be used to improve grid's detection performance and avoid erroneous grid detection. Not only a $\mathcal{D}_{min}$ and a $\mathcal{D}_{max}$ can be derived, but subsets of peaks leading to grid with acceptable density $\mathcal{D}$ can be ruled out if they induce unacceptable geometrical distortion. It also enables to distinguish from periodic structures that are present in the cover image. This approach consists in performing informed detection. When the embedded periodic structure is secret, this information is only available to authorized user.

As previously discussed, the ability to correctly detect the periodic structure depends on the embedding strength but also on the number of periods that are represented in the image signal. Figure 3.20 illustrates the detection performances for different pattern's sizes after a rotation of $7°$ and an appropriate cropping were applied to image Lena. Results were obtained with 100 different key combinations. The larger is the elementary repetition, the less robust is the grid detection.

When the affine deformation is correctly estimated, the message detection is always successfull. The bit error rate is always equal to 0 or close to 50%. The graph indicates that the probability to correctly detect the periodic structure and estimate the undergone deformation increases when the size of the periodic pattern diminishes.

3.4.4 Weaknesses and security issues

One possible weakness of the grid detection scheme is to be fooled by periodic structures that are present in the cover image or added by an opponent. This problem can be overcome only partially through informed detection.

The main security issue relies in the ability for everyone to perform grid detection. It means that, when the periodicity is observable, any op-

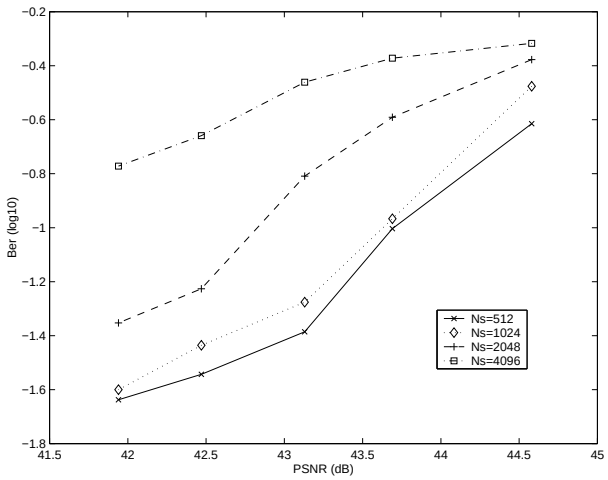


Figure 3.20: *Watermark detection performances after rotation of 7° in function of the embedding strength for different pattern repetition sizes. ($R_x = R_y = 2$, image Lena 512×512)*

ponent can estimate the watermark through averaging over the different repetitions and can effectively remove watermark power from the image. This is due to the fact that the detection of the regular grid characteristic of our pilot signal is achievable by everyone. A similar weakness appears [51] with template reference signals, where the pilot can often be erased from the watermarked image due to its publicly detectable characteristics. In such circumstances, the proposed generalized pattern construction does not provide much improvements with respect to classical tiling of a fixed rectangular pattern. Secrecy enclosed in the pattern construction process is truly effective as long as the periodicity cannot be detected. This undetectability can be ensured using large elementary tiles.

In the current configuration, relying on the detectability of the periodicity of the embedded watermark to detect and invert affine deformations is not secure. In the following chapter, we present the original approach that we have developed to solve this security issue. The idea is to modulate the reference signal with a secret and content dependent signal prior to its embedding into the image. This secret signal exhibits a white power spectrum and can be computed from the image even after rotation, scaling, and cropping operations. At detection stage, the reference signal can be detected only using the secret modulating signal.

3.5 Conclusion

As a summary, we have shown that the use of periodic structures in watermarking can help recover from loss of synchronization such as cropping or even affine transformations. However, in order to ensure the security of the system, one should carefully design the watermark. Watermarks with large repetition periods with respect to the image size are secure but do not provide means to resist against general affine deformations. Watermarks with smaller repetition periods can be designed to be robust against affine deformations but exhibit an important security weakness unless specific hiding stategies are used.

Chapter 4

Synchronizing on Local Content

Using the image content as side-information in a watermarking communication system is legitimate. Indeed, most characteristics of the cover content are left unchanged in the watermarking process. Signal dependency is often proposed to enhance security and prevent copy-attack. However, very few authors studied the use of content to overcome loss of synchronization issues. We present a novel approach that we have developed to design robust reference systems for gray-scale images. We present its utility in specific watermarking schemes and study its performance and limitations.

Keywords: Watermarking, content normalization, synchronization marks, geometrical deformations.

Introduction

The general definition for a signal is a variable characteristic of a physical phenomenon by which information is conveyed through a communication system. The usual way to handle a signal is to describe it as a function of time or space references. The information conveyed by the signal results from the analysis of the signal variation with respect to the references marks. Correspondence between the signal and the reference marks is mandatory to ensure a constant interpretation of the signal. These considerations are also valid for transformed domain representations.

However, human perceptual signals such as audio or visual signals can undergo transformations that do not affect their psycho-visual inter-

pretation. An example is the process of scaling and slight cropping of the edges of an image which does not alter the perceptual interpretation of the image content. Still the signal description as function of the absolute space references marks has been modified and therefore the mathematical interpretation of this space-signal is changed. This difference results from the fact that human perception does not rely on absolute reference to interpret a signal. The human perceptual interpretation process is highly content-based.

Watermarking techniques as most communication systems are very sensitive to signal transformations which produce loss of reference marks. In such processes, the content of the media is not erased but transformed, which impairs the watermark detection. A normalized description based on content would enable a constant mathematical interpretation of a signal, closer to perceptual mechanisms. This chapter addresses the analysis and design of watermarking algorithms using content based mechanisms to resist geometrical deformations.

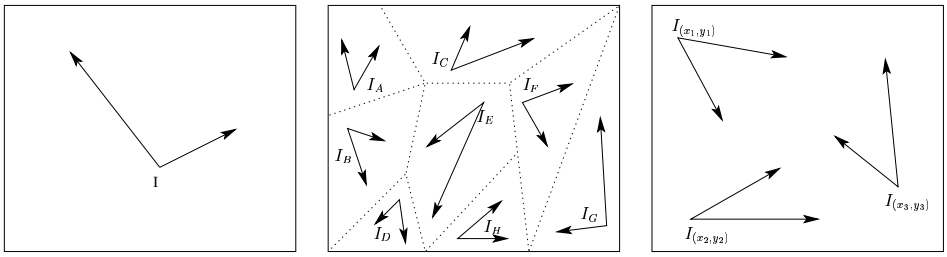
4.1 Watermarking schemes exploiting content normalization

The process of content normalization consists in building reference systems based on the signal content characteristics. Different techniques have been proposed in the literature. In our analysis, we propose a classification of existing solutions in three different groups.

The first group of methods constructs a unique global normalized reference system for the image. The entire image signal is expressed in this new reference system. In the second group, one extracts robust features or objects in the image in order to produce a partitioning of the representation space in several regions. Normalized references are defined over each separated region. The last approach, presented in this chapter, consists in defining a distinct reference system for every location in the image signal.

4.1.1 Global normalization

A first technique was proposed by M. Alghoniemy and A. Tewfik [60]. It consists in extracting global scale and orientation characteristics from the cover image. The watermark embedding and detection are performed on a normalized representation of the image. The used characteristics are the Edge Standard Deviation Ratio (ESDR) and the Average Edges Angle



(a) (b) (c)

Figure 4.1: *Different normalization approaches: (a) Global, (b) region-based, (c) local.*

Difference (AEAD). Edges are defined by wavelet maxima locations. The technique claims robustness against scaling and rotation. However, only very small amplitude rotations can be considered.

Similar approaches were proposed by Alghoniemy and Tewfik [78] and by Dong and Galatsanos [79] using geometric and central moments of the image as reference characteristics. These techniques perform affine normalization providing affine robustness to the watermarking schemes.

Normalization based on global characteristics exhibits important weakness when image content is modified. This occurs inevitably along common cropping operations. Rotation is always followed by a corresponding cropping to hide inclined images borders. Non-symmetric cropping operations are also very common. Every modification of the image content is likely to affect global image characteristics and change image normalization outcome. The content loss issue is seldom considered in global normalization-based watermarking algorithms.

4.1.2 Feature/Object based region normalization

Few authors have proposed to partition the representation space and define normalized reference systems over each separated region.

P. Bas *et al.* [62, 64] use a Harris detector to extract robust features points. They perform a Delaunay tessellation to obtain a partitioning of the image representation space in a set of triangular regions. Prior to watermark embedding and detection, each triangular region is mapped to a reference triangle through an affine transform by modifying two arbitrary vertices of the triangle. In another work, P. Bas [63] watermarks segmented video objects. The region defined by each object is normalized in scale and orientation using principal component analysis.

Those approaches are very promising. However, they suffer from some weaknesses. Robust feature points extraction is not easy and could be fooled by intentional manipulation. Moreover, Delaunay tessellation is quite sensitive to even few erroneous detected points. Object based normalization relies on the availability of robust segmentation tools, which is still challenging the research community.

4.1.3 Local normalization

One can think of several approaches to normalize a signal using local content characteristics. However, few of them exhibit the required properties for a watermarking application. The normalization should be robust to common geometrical transforms and the normalized space should be sufficiently large to parametrize a secret. Note that the expression of the pixels coordinates in the new reference systems is not necessarily bijective and changes for each considered location. New coordinates spaces may be finite and 1-dimensional.

A very simple but little practical systems can be considered to illustrate this class of normalization. Consider a function f which transforms the three color components of a pixel into a new scalar value. This new value plays the role of coordinate in the new 1-dimensional representation space. If f is appropriately designed, the pixel coordinates in this new reference system can be made roughly invariant to geometrical deformations and small pixel value modifications.

The weakness of the above content normalized representation is the difficulty of using it in a watermarking scheme while fulfilling robustness and security requirements simultaneously. To overcome this problem, we propose to consider the local neighborhood of a pixel to build the reference system. This enables to introduce secrecy in the construction of the new reference system. The drawback of the proposed approach is that it is not robust against general affine transform but only rotation, scale and translation (RST). However, if the considered neighborhood is small, most tolerable transforms can be reasonably approximated by a RST model. In next section we present the method to build a local reference system based on neighborhood luminance analysis.

4.2 A local and content based reference system for gray-scale images

We present a method to build a local-content normalized reference system reasonably resistant to scaling, rotation and other common transformations altering pixels values as JPEG compression for example. A reference system for two-dimensional signals is composed of an origin location and two non-aligned vectors. Upon affine transformation, the new signal is determined by the transformed reference origin and vectors. In a RST model of deformation, the transformed coordinate system is fully defined by the origin and one vector which informs about the scale and orientation of the transformed signal.

In our approach, each location in the image has its own reference system in which the considered location is the origin point of the coordinates plane. The proposed method consists in extracting robust scale and orientation characteristics for each considered location (pixel) in the signal. This content dependent coordinate system (peculiar to each considered location) follows the deformation that the local neighborhood undergoes. The interpretation of the signal sample in this normalized coordinate system is therefore invariant to these deformations.

4.2.1 Construction of the reference system

Our method performs an analysis of the luminance values in the neighborhood of each pixel as depicted in figure 4.2. Let $i(x, y)$ represent the luminance value of the image signal at position determined by the absolute Cartesian coordinates (x, y). Let $i_{x,y}(r, \theta)$ be the luminance of the image signal defined in polar coordinates relatively to position (x,y):

$$i_{x,y}(r, \theta) = i(x + r\ cos\ \theta, y + r\ sin\theta). \tag{4.1}$$

For each position (x, y), a reference radius $r_{ref}(x, y)$ is computed. It is defined as the radius of the smallest circle centered in (x, y) for which the mean luminance along the perimeter equals the mean luminance computed over the disk of same radius. If M_{circle} and M_{disk} represent the mean

luminance over the circle and disk of radius r centered on location (u, v),

$$M_{x,y,disk}(r) = \frac{1}{\pi r^2} \int_0^r \int_0^{2\pi} i_{x,y}(r,\theta)\, r\, d\theta\, dr \tag{4.2}$$

$$M_{x,y,circle}(r) = \frac{1}{2\pi r} \int_0^{2\pi} i_{x,y}(r,\theta)\, r\, d\theta \tag{4.3}$$

then the reference radius can be defined as

$$r_{ref}(x,y) = \min \left\{ \mathbf{r} \in \mathbf{R}^+ \mid \mathbf{M_{x,y,disk}}(\mathbf{r}) = \mathbf{M_{x,y,circle}}(\mathbf{r}) \right\}. \tag{4.4}$$

It is easy to show that an equivalent definition for this reference radius is the smallest radius where the first derivative of the disk mean luminance equals zero. The computation of this value for every location in the image can be expressed as differences of convolution operations. It can therefore efficiently be performed in Fourier domain.

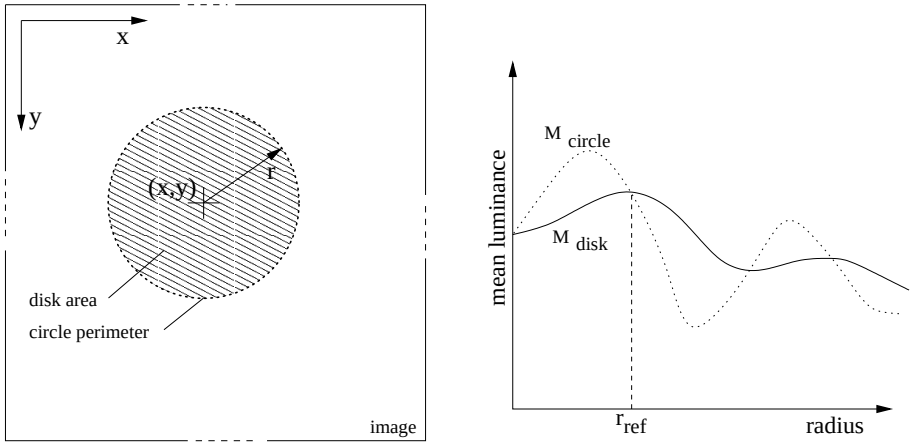


Figure 4.2: *Luminance mean value analysis.*

Given this extracted reference radius r_{ref}, which provides a robust scale information, an orientation can be extracted as depicted in figure 4.3. The signal luminance $i(r,\theta)$ along the perimeter of a circle of radius r_{ref} is analyzed and the direction where luminance is maximum is retained as reference orientation θ_{ref}:

$$\theta_{ref}(x,y) = arg \max_{\theta \in [\mathbf{0};\mathbf{2}\pi]} i_{x,y}(r_{ref},\theta). \tag{4.5}$$

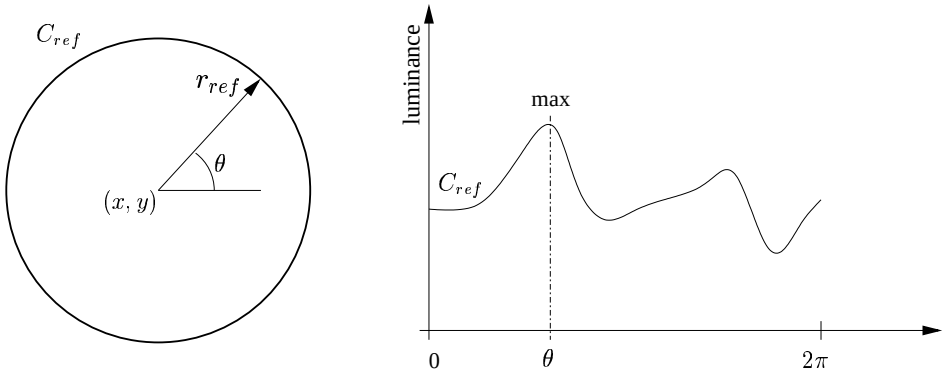


Figure 4.3: *Reference orientation definition.*

The image signal can now be expressed in a new reference system where the origin is the considered location (x, y) and reference base vectors can be derived from r_{ref} and θ. If the signal undergoes transformations which are limited to rotations, scalings and translations, recovering these two parameters r_{ref} and θ_{ref} in each location is sufficient to recover the robust reference systems attached to each of these locations.

4.2.2 Limitations

In the reference detection process described here-above we did not consider the digital nature of our real signal. In our image application, the signal is discrete with finite and possibly varying extent. This will introduce different difficulties in our detection process.

A first problem arises from the discrete nature of the image signal and mean luminance computations. For very small radius, the functions $M_{disk}(r)$ and $M_{circle}(r)$ exhibit a quite chaotic behavior which is not robust under signal deformation. Any solution with very small radius value must therefore be ruled out. An alternative is to set a desired radius value and look for the closest radius satisfying relation 4.4. Both approaches introduce scale dependent factors which are source of error in the presence of scaling operations.

Since both functions tend to evolve toward the mean luminance of the image, we can expect a solution to relation 4.4 for a large number of pixels in the image. However, for an important amount of pixels, it will not lead to a solution within the signal boundaries. Another rule must therefore be

used when no satisfying radius can be found. We decided to choose the radius leading to minimum first derivative of M_{disk}:

$$r_{ref}(x,y) : arg \min_{\mathbf{r}\in[\mathbf{r_{min}};\mathbf{r_{max}}]} \frac{dM_{x,y,disk}}{dr}(r). \tag{4.6}$$

In the following discussions we will refer to alternative reference radius definitions.

- Type A: The reference radius is defined as the smallest radius satisfying relation 4.4 but bigger than a threshold value r_{th} (typically $r_{th} = 5$).
- Type B: The reference radius is defined as the radius satisfying relation 4.4 which is closest to a targeted radius value r_{tg}.

For easier analysis of robustness, the following definition will also be used:

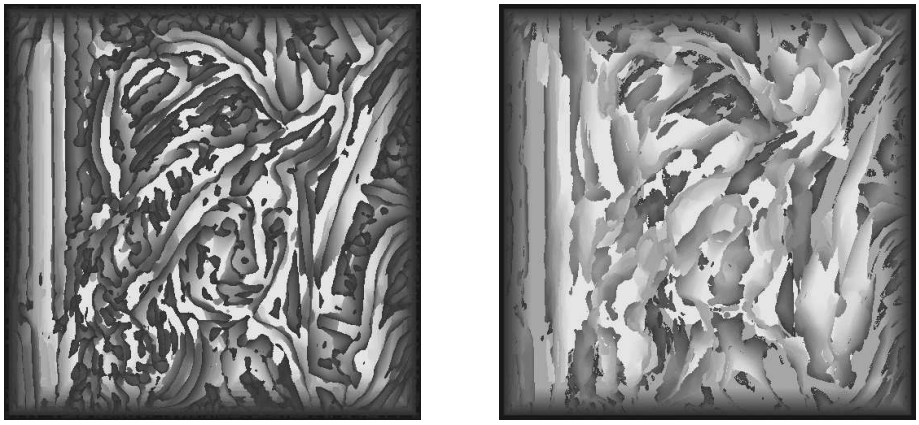
- Type C: The reference radius has a fixed value r_f, identical for all locations in the image.
- Type D: The reference radius has a fixed value r_{fa} which is adapted when the studied deformation involves a scaling.

The latter definition is useful to study reference orientation robustness independently from reference radius robustness. Indeed, the reference radius must be known before the reference orientation can be extracted.

Figure 4.4 illustrates the values of type A and B reference radius detected on image Lena (512×512). High luminance intensities indicates large detected reference radius. One can clearly observe that, within small regions, the reference radius evolves smoothly. Sharp discontinuities show up at regions boundaries.

It can also be noted that, although the reference radius computation process is public, it cannot be intentionally modified by an unnoticeable manipulation of the image since it is computed with low frequency characteristics of the signal. Moreover, reference radii of different locations within the image are intrinsically linked together. Therefore, it would be very difficult to forge reference values for an important fraction of the image with modifying severely the image content.

Computing mean image luminance value over regions of increasing size at different locations comes down to some kind of multi-resolution analysis. The reference radius determination corresponds to the selection of a characteristic resolution for each location.



(a) Type A reference radius (b) Type B reference radius

Figure 4.4: *Reference radius computed on image Lena.*

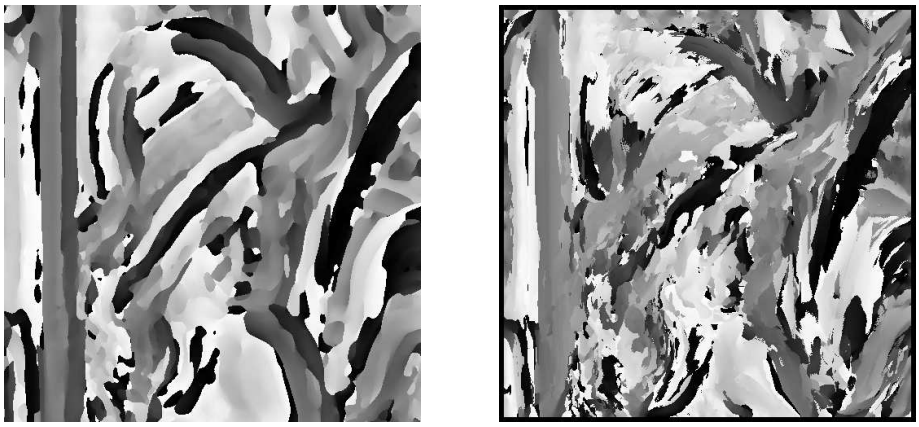
The above method corresponds to use of a cylindrical analysis function. Other choices for the analysis function arepossible. Different considerations must be taken into account in the determination of a suitable function. Isotropic characteristics are required to make the process invariant to the rotation of the content. It should have limited spatial extend in order to limit the errors caused by a modification of the content at the image border. Indeed, the fraction of pixels whose reference values will be affected by a cropping operation will depend on the spatial extend of the analysis function. Advantageous spectral characteristics can limit the influence of the high frequency components of the image, which are less robust. Tests were conducted using trapezoidal analysis functions. However this choice does not lead to improvements. Note also that the choice of the analysis function can be used as a secret parameter in the process leading to the determination of the reference system.

In the above method, the characteristic resolution is defined as a resolution where the first derivative of the computed mean value is the smallest. Other characteric resolutions can be chosen. One can for example define the reference resolution as the resolution where this derivative takes the highest value. We make therefore the following definition:

- Type E: The reference radius is defined as the radius where the derivative of the mean luminance over the disk takes the highest absolute value.

The rule used to extract the reference orientation θ is quite arbitrary.

One could choose other characteristics. However, this approach offers the best robustness among several envisaged solutions. The proposed extraction of the reference orientation, which is repeated on each pixel of the image, cannot be expressed in terms of convolutions. Figure 4.5 illustrates the reference orientation measured on image Lena. The luminance range corresponds to angular values comprised in the interval $[0 - 2\pi]$. The left image results from the use of a fixed reference radius value for the whole image, while the right image uses the type B measured reference radii from figure 4.4.b.



(a) (b)

Figure 4.5: *Reference orientation computed on image Lena using (a) a type C reference radius, (b) a type B reference radius.*

The usefulness of the system relies on a relative spatial smoothness of the extracted reference values. Under signal deformation, the reference system might be computed on locations requiring signal interpolation. We desire that the extracted values at interpolated locations be quite similar to neighbouring original values. The extracted reference values should therefore exhibit a continuous character and have a limited number of sharp discontinuities.

In order to lower the contribution of high frequency components of the signal to the reference values, an additional mean filtering operation is performed before the reference values are extracted. Although this operation introduces scale dependency, we will show that it improves the global robustness of the system.

4.2.3 Robustness of the reference system

The process yielding the reference system has a very high computational cost. Therefore simulations were conducted on a limited number of test images. The chosen set of test images is illustrated in figure 4.6, representative of a large set of contents. All images have the same size (512×512).

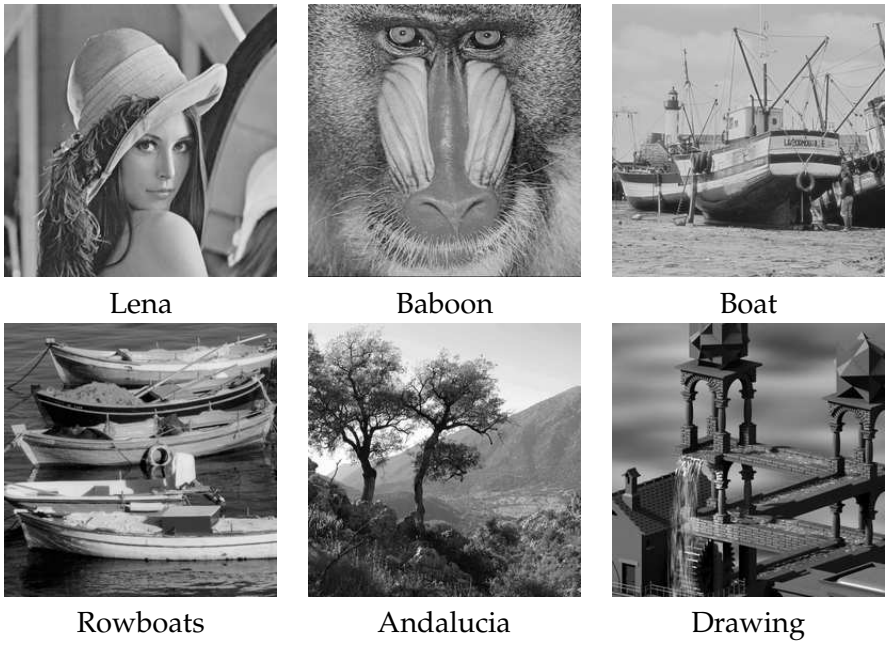


Figure 4.6: *Test images.*

The robustness of the reference system will be characterized by comparing the reference radius and orientation computed before and after various image manipulations. Most studied manipulations involve geometrical distortion, therefore transformed reference values will be compared to expected values obtained applying the same displacement to the reference values that were computed on the original image. This evaluation process is depicted in figure 4.7.

Given a tested geometrical deformation T, let us consider T_{RST} as a combination of rotation, scaling and translation (RST) which best matches the applied deformation T:

$$T_{RST} : \begin{pmatrix} x' \\ y' \end{pmatrix} = s \begin{pmatrix} cos\ \alpha & sin\ \alpha \\ -sin\ \alpha & cos\ \alpha \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} t_x \\ t_y \end{pmatrix}. \qquad (4.7)$$

When the deformation is purely RST, T_{RST} corresponds exactly with T. In other cases, T_{RST} is a rigid approximation of the actual undergone deformation using a least square optimization of the displacement error. We restrict however our analysis to deformations that do not differ to much from pure rigid transformations.

Let r_{ori} and θ_{ori} be the reference values derived from the original image signal. Let r_{dis} and θ_{dis} be the values extracted from the distorted image. When the applied deformation T is known, one can reasonably predict how the reference values will be modified after the transformation. The new extraction is expected to yield values very similar to the predicted values r_{pre} and θ_{pre}, as expressed in following expression:

$$r_{dis}(x,y) \approx r_{pre}(x,y) = s \times r_{ori}(T^{-1}(x,y)); \tag{4.8}$$

$$\theta_{dis}(x,y) \approx \theta_{pre}(x,y) = \alpha + \theta_{ori}(T^{-1}(x,y)). \tag{4.9}$$

The error distribution between predicted and computed reference values v_{pre} and v_{dis} will be centered on zero. In order to characterize robustness, two different measures will be considered. The first measure, R_ϵ, is the proportion of pixel locations where absolute error is smaller than a threshold ϵ.

$$R_\epsilon = \frac{\#\{\ (x,y)\ \mid\ |v_{pre}(x,y) - v_{dis}(x,y)| \leq \epsilon\}}{N_{tot}}. \tag{4.10}$$

The second measure, R_v, is the standard deviation of the error.

Figure 4.8 illustrates implementation details for rotation and shearing manipulation tests. In both situations, a subsequent cropping is performed on the subject image in order to yield a rectangular shaped image without undefined image content. Remaining image area is maximized.

As explained in previous section, there is a high probability that pixel positions close to image boundaries will have little robustness against geometrical distortion that involves loss of content. This behavior is illustrated on figure 4.9. As the proportion of affected location is proportional only to image outline, we decided to discard a forty pixels-wide border region for the R_ϵ and R_v measurements.

Figures 4.10 and 4.11 show the robustness performances of the reference radius and orientation measurements. Only scaling and rotation operations were considered. Further robustness analysis will be provided in the following section where the reference system is used in a watermarking scheme. A few observations can already be made.

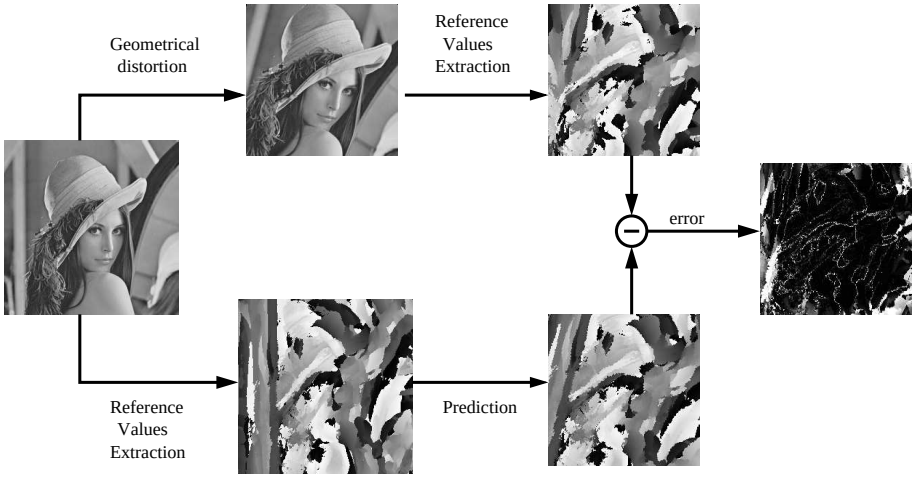
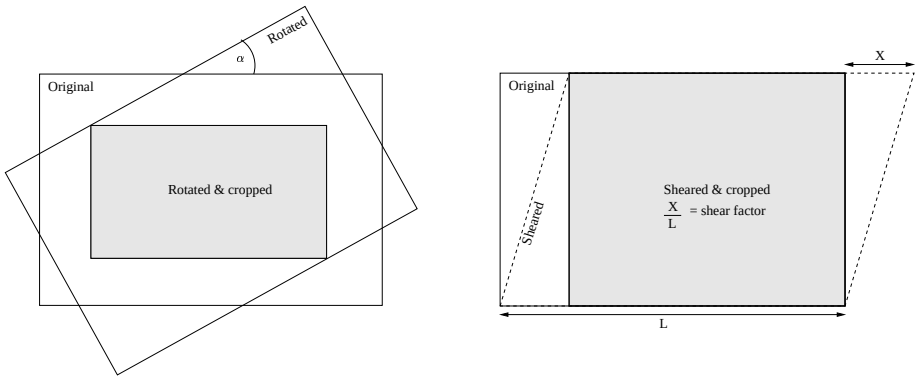


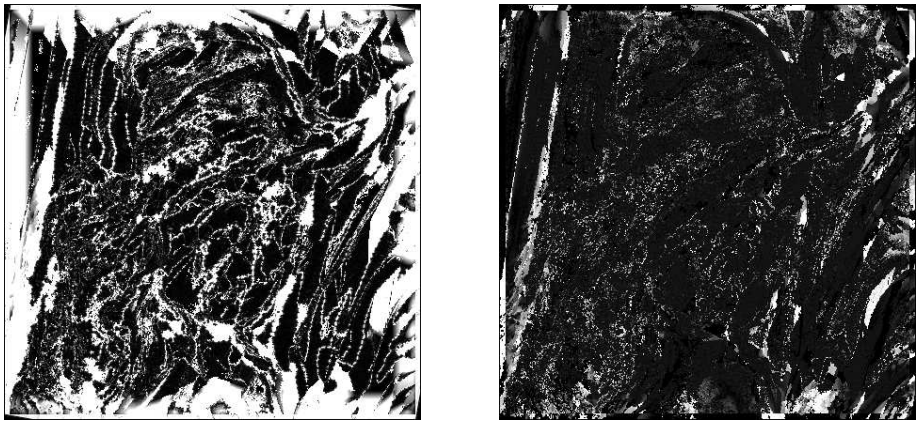
Figure 4.7: *Robustness evaluation process.*



(a) Rotation (b) Shearing

Figure 4.8: *Details of rotation and shearing implementations.*

Scaling: In figure 4.10, one can compare type A and type B radius robustness to scaling and realize that type A performs better than type B only when the scaling factor is markedly different from one. For no or very gentle scaling operations, setting a desired reference radius value is profitable. For severe scaling, looking for the smallest radius satisfying the rule performs better. The type C curve shows that using a fixed (i.e. not dependent on content) reference radius outperforms both radius measures as long as scaling remains very gentle (5%). The type D radius curve illustrate the harmful scale dependence introduced by the mean filtering



(a) Reference radius error (b) Reference orientation error

Figure 4.9: *Higher error probability on image borders after rotation (10°) and cropping manipulation.*

operation.

Rotation: In figure 4.11, one can clearly observe that the type B radius performs better than the type A when pure rotation is applied to the image. Type C curve illustrates errors introduced by interpolation operations and discontinuities of the reference values.

One must specify the role that is played by the reference system to be able to tell whether the achieved robustness is satisfactory. In the following section we present how one can use this content based reference system to build robust secret binary partitions of an image.

4.3 Hiding structured watermarks using robust content based binary modulation

As described in previous chapters, a widespread technique to fight against geometrical distortions in watermarking systems, is the use of structured watermark signals. By structured watermarks we refer to periodically structured watermark signals - also called self-referencing watermark - and other watermarks exhibiting particular (e.g. spectral) characteristics - also called template or pilot-signals. These techniques rely on the detection of the strong characteristics of the watermark signal to estimate and invert the undergone affine distortions.

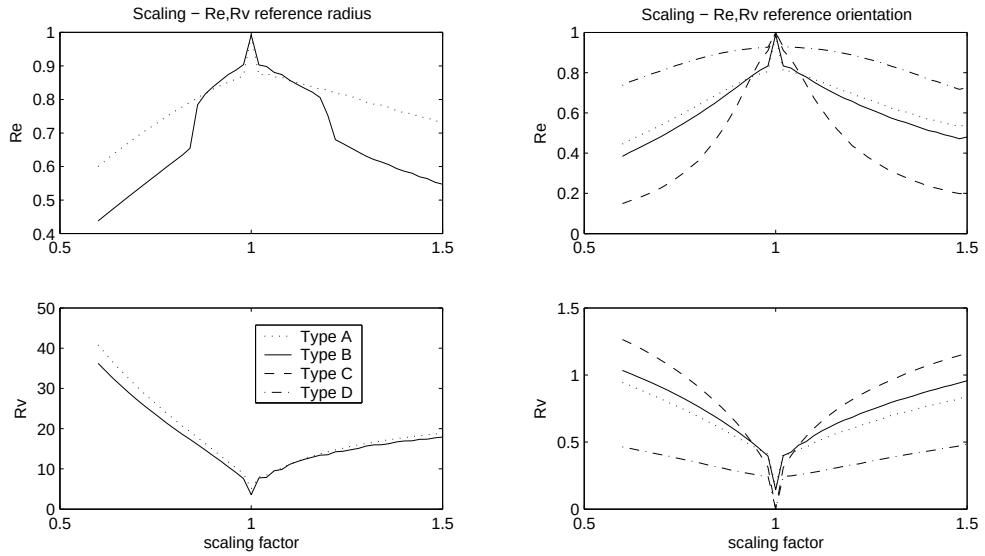


Figure 4.10: *Robustness of the reference values to scaling.*

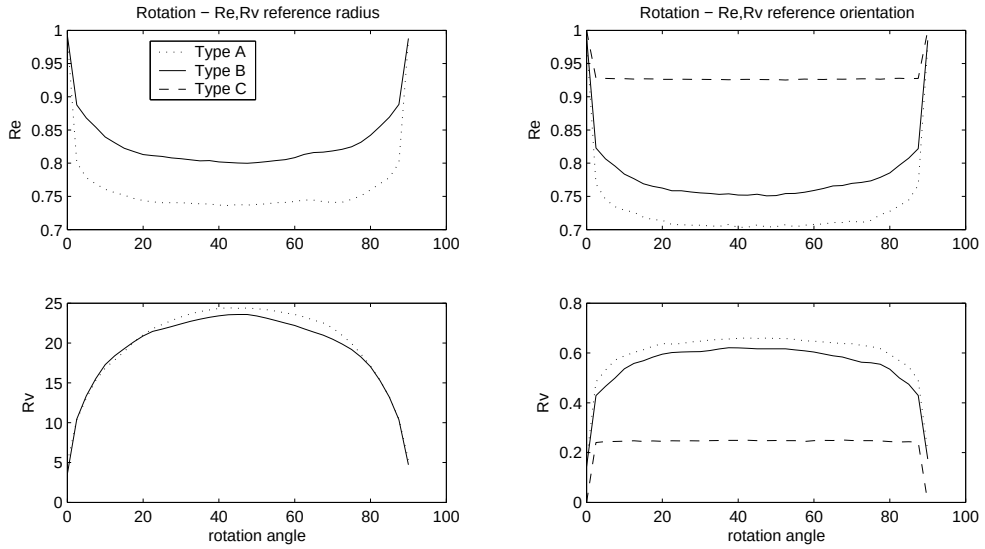


Figure 4.11: *Robustness of the reference values to rotation.*

The main drawback of these approaches is the weakening of the cryptographic issue in the hiding process. Indeed, signal characteristics that

are used to invert distortions are publicly detectable. This means that any opponent can perform detection with the aim of estimating and removing watermark signal or intentionally introduce fake characteristics in order to fool the watermark detection.

We propose to hide the characteristics of a structured watermark w_o through the modulation with a spread spectrum secret signal p. Provided the power spectral density function of the secret signal has a sufficiently large bandwidth, this operation will produce an efficient whitening of the watermark spectrum preventing unauthorized user to detect its structure. The new scrambled watermark signal w_s can be expressed as follows:

$$w_s(x, y) = w_o(x, y)\ p(x, y). \tag{4.11}$$

The original watermark signal w_o can be recovered through a demodulation operation using the same secret signal p:

$$w_o(x, y) = \frac{w_s(x, y)}{p(x, y)}. \tag{4.12}$$

The main challenge is to find a procedure such that it becomes possible to perform demodulation operation after some unknown geometrical distortion occurred. Indeed, $w_s(x, y)$ and $p(x, y)$ must be perfectly synchronized in order to recover w_o as outcome of the demodulation step.

The proposed solution is to build the secret spread-spectrum (or pseudo-random) signal p relatively to a content based reference system. This will ensure that the secret modulating signal undergoes exactly the same geometrical distortions as the watermark w_s which is embedded into the image signal. We propose to use bipolar $(-1, 1)$ pseudo-random secret signals that we refer to as the secret mask or secret partition. The restriction to bipolar $(-1, 1)$ secret signals makes modulation and demodulation operations identical. Figures 4.12 and 4.13 show block diagrams of our proposed watermarking approach.

This content dependence also prevents opponents from exploiting the availability of different contents watermarked with the same keys.

The following section describes a method to build secret binary signals using the content based reference system presented in previous section. The use of such modulating signals in a watermarking scheme using self-referencing structures is demonstrated in section 4.3.3.

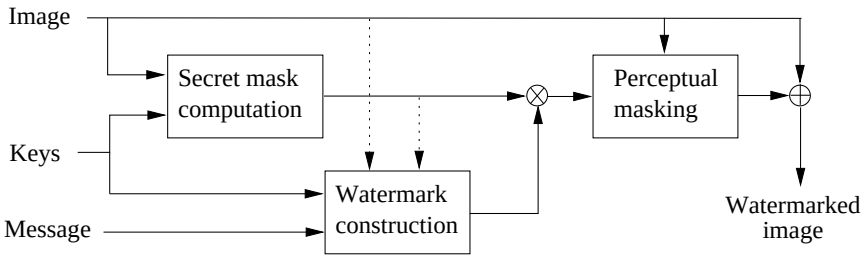


Figure 4.12: *Watermark embedding using secret content dependent modulation.*

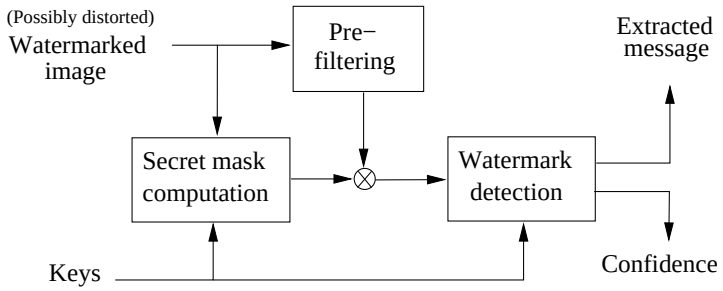


Figure 4.13: *Watermark detection using secret content dependent modulation.*

4.3.1 Construction of a content based two-valued secret partition

In possession of a reference system, it becomes quite easy to build a secret pseudo-random binary signal. However, as described in section 4.2, our reference system is very particular since it changes for each considered location. Its origin is always on the considered signal sample. Therefore the secret function cannot use the sample's coordinate indexes to parametrize the secret signal value since all locations in the signal have the same coordinates indexes (which is the origin of their reference system). The solution is to build the secret partition by extracting, for each considered location in the signal, a one-bit hash value through analysis of the signal content relatively to the reference system attached to this location.

A very large number of hash functions could be considered although some restrictions should be considered. Firstly, one should avoid relying on signal value outside the reference disk for the considered location since it may correspond to locations outside the image limits. Secondly, one should build the secret function based on low frequency characteristics of the signal in order to be robust against small signal distortions such as interpolation and compression.

A general approach is to use a function f parametrized by a secret key k and whose probability density function can be estimated. A threshold value t can be set such that

$$P[f(k,x,y) > t] = P[f(k,x,y) < t] = 0.5\ . \tag{4.13}$$

The expression of the binary hash function is

$$h(k,x,y) = \begin{cases} 0 & f(k,x,y) \leq t, \\ 1 & f(k,x,y) > t \end{cases} . \tag{4.14}$$

We propose a hash function based on the analysis of maximum luminance directions in the neighborhood of the considered location. This method is described below.

Given the reference radius r_{ref} defined in section 4.2, a binary value is extracted for each pixel according to the following procedure. Two radii r_1 and r_2 are chosen relatively to the reference radius associated to the pixel's location:

$$r_1 = k_1 * r_{ref}, \tag{4.15}$$

$$r_2 = k_2 * r_{ref}. \tag{4.16}$$

Subsequently, as shown in figure 4.14, two luminance curves C_1 and C_2 are computed along the perimeters of two concentric circles of radius r_1 and r_2. These two curves are summed together to yield a new curve C_t :

$$C_1(\theta) = i(r_1,\theta), \tag{4.17}$$

$$C_2(\theta) = i(r_2,\theta), \tag{4.18}$$

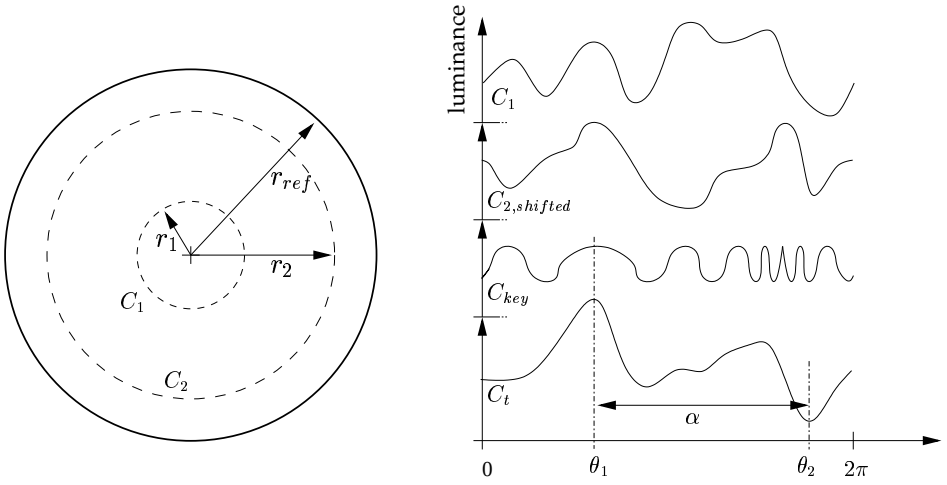
$$C_t(\theta) = i(r_1,\theta) + i(r_2,\theta), \tag{4.19}$$

with $\theta \in [0, 2\pi]$. Along C_t, the angular distance α between the position of the maximum and the position of the minimum determine the binary hash value for the considered pixel:

$$h(x,y) = \begin{cases} 0 & \alpha \leq \pi \\ 1 & \alpha > \pi \end{cases} \tag{4.20}$$

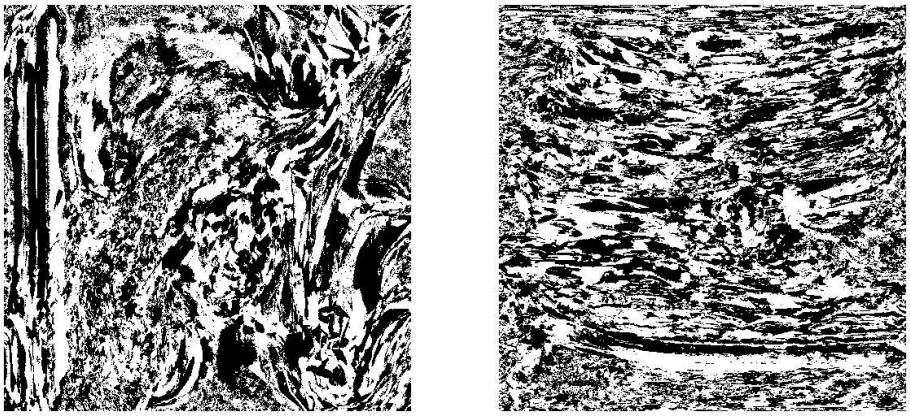
Since the method relies on content dependent references, the proposed process to extract the binary value is not sensitive to scaling and rotation of the signal. This requires however that the reference radius value be correctly recovered after the transform.

Figure 4.15 illustrates the binary mask appearance for images Lena and Rowboats. One can realize that the original image content partially shows through the binary mask.



(a) (b)

Figure 4.14: *Mask value computation.*



(a) (b)

Figure 4.15: *Mask appearance using (a) Lena and (b) Rowboats.*

4.3.2 Secrecy and robustness of the binary partition

The secrecy of the partitioning relies in the two keys k_1 and k_2 parameterizing the radius of circles C_1 and C_2. Figure 4.14 illustrates how more secrecy can be introduced through different means.

Firstly, a secret angle k_s can be used to shift curve C_2 before it is added to curve C_1 and therefore provide a different curve C_t. Secondly, we are

not limited to two circles to generate C_t. One can decide to sum up a secret number of shifted curves computed along concentric circles. Thirdly, after the maximum value is found on C_t, a secret curve C_{key} can be summed to C_t before looking for the minimum value. We must take care that this secret curve be symmetrical with respect to the position of the maximum value of C_t in order to keep an equal probability for each binary value.

In order to evaluate the amount of secrecy in the partition, we will compare partitions generated with different values for the keys. We will measure the fraction of pixels that yield the same extracted binary value in the partition. A fraction close to fifty percent indicates a complete mismatch of the partitions. Figure 4.16 shows the sensitivity of the partition to the choice of the k_1 factor and k_s angular shift. One can observe the error on the partition recovery when different parameters k_1 and k_s are used to extract the binary hash. Other means proposed to increase secrecy of the partition were not tested. Since mask bit error rate is a continuous function of the extraction parameters, one should ensure that an opponent cannot rely on information about the embedded watermark signal to perform gradient search mask determination.

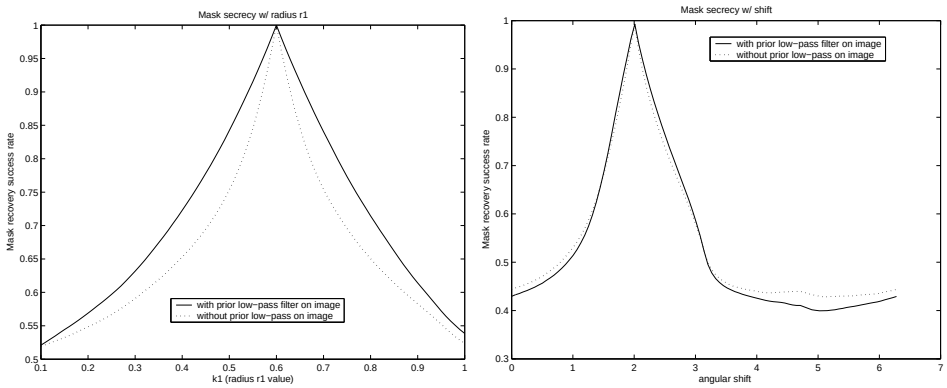


Figure 4.16: *Mask dependence on secret parameters (original parameters:* $k_1 = .6$, $k_s = 2$*).*

There is actually a trade-off between secrecy level and robustness. Indeed robustness is favoured when bit extraction is based on low frequency characteristics. On the opposite, increasing the secrecy requires relying on larger amount of information to parametrize the hash value computation. This can be achieved only by taking into account higher frequency components of the signal or by analysing a larger signal portion. The latter

solution must be limitted to resist cropping operations. As described in section 4.2.2, problems rise at the borders of the image when cropping is applied. The computing of the reference radius and of the binary value cannot be performed normally. Indeed, the neighborhood of pixels located near the border will change and this will introduce errors when recovering the partition. Another important characteristic of the constructed mask is linked to robustness and secrecy. The optimal masking signal is one which exhibits the same spectral characteristics as a white noise. A signal with advantageous masking properties will therefore enclose more secrecy but exhibits less robustness.

Figure 4.19 and 4.17 show the proportion of mask values correctly recovered after rotation or scaling of the original content. The same observations can be made as for reference values in section 4.2.3. Additional curves for the Type E reference radius are displayed. The secret partition is quite robust against rotation as almost 85% of the bits are systematically recovered. A large scaling factor however proves fatal to the partition recovery.

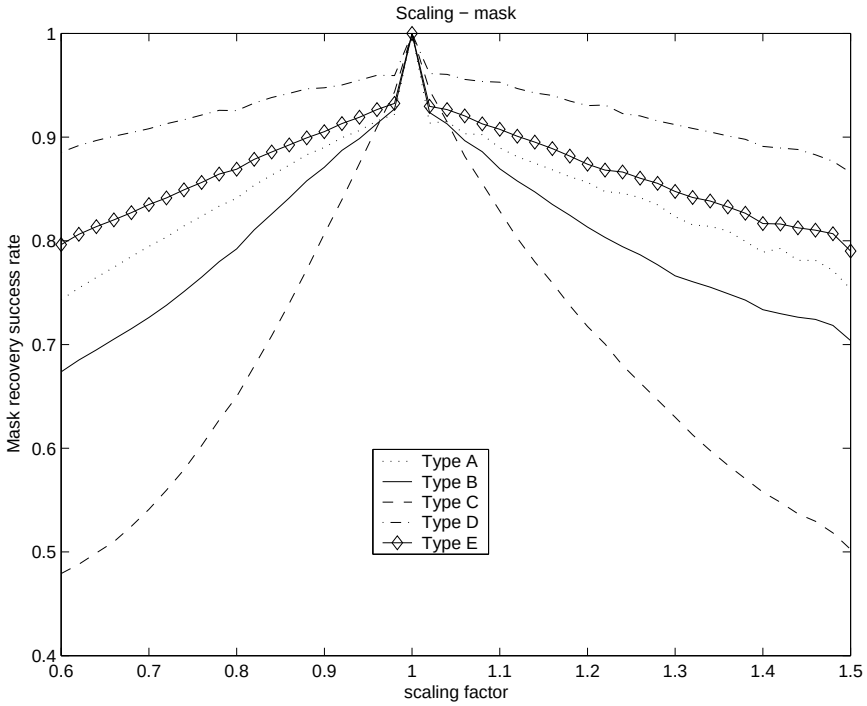


Figure 4.17: *Mask robustness to scaling.*

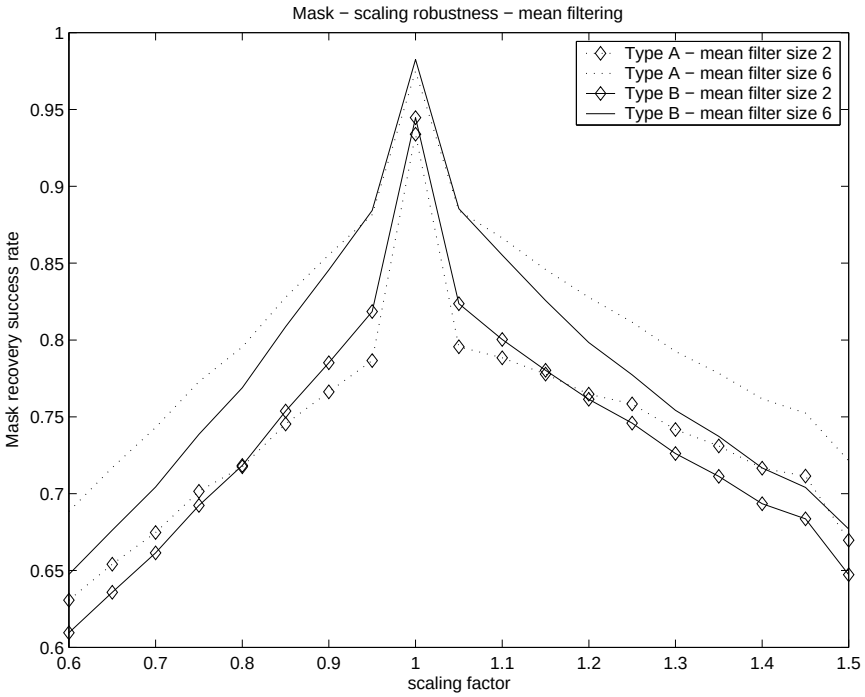


Figure 4.18: *Influence of prior mean filtering on robustness to scaling.*

Figure 4.20 illustrates the mask robustness against JPEG compression and distortion consequent to watermark embedding. Both operations cause limited degradation on the mask recovery.

In figure 4.21, one can observe the robustness of the mask under shearing and modifications of aspect ratio. Although the reference system is not designed to resist such deformations, one can observe that the mask is only progressively degraded. The reference system can cope with very slight shears and aspect ratio changes.

4.3.3 Structured watermark detection using content modulation

In this section, we present the performance of the content modulation technique on a watermarking scheme relying on periodical structure detection to recover from affine deformations. The watermark pattern construction and periodical structure detection are described in chapter 3.

The periodical structure (pilot) and watermark detection process is depicted in figure 4.22. Notice that the mask is computed twice at the de-

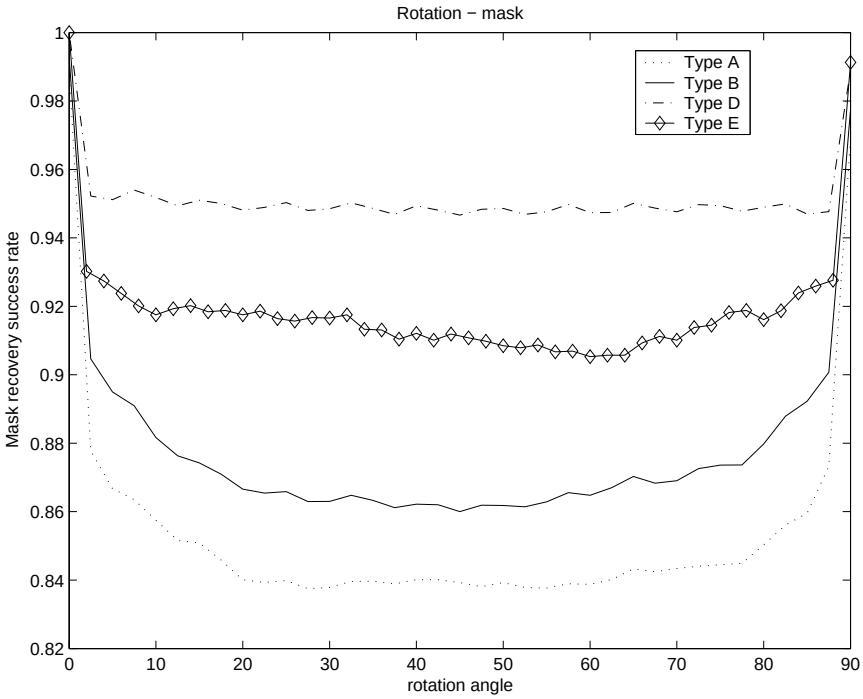


Figure 4.19: *Mask robustness to rotation.*

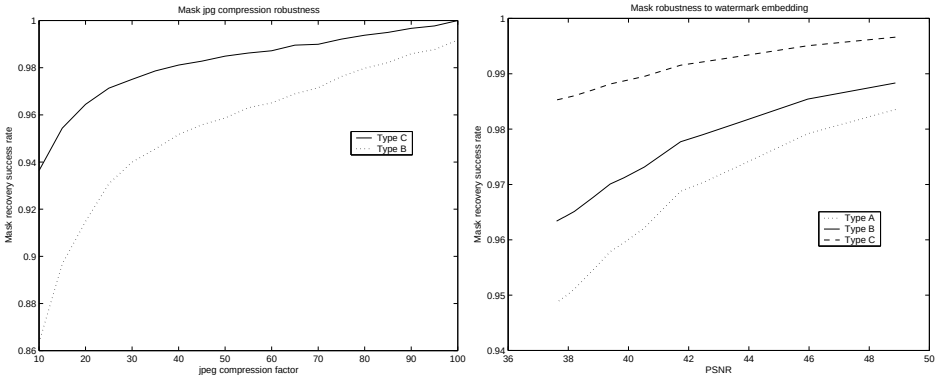


Figure 4.20: *Mask robustness to compression and watermark embedding.*

tection stage. It is indeed computed again after deformation is inverted in order to achieve lower error rate on watermark message extraction.

Figure 4.23 illustrates the expected masking effect of the secret con-

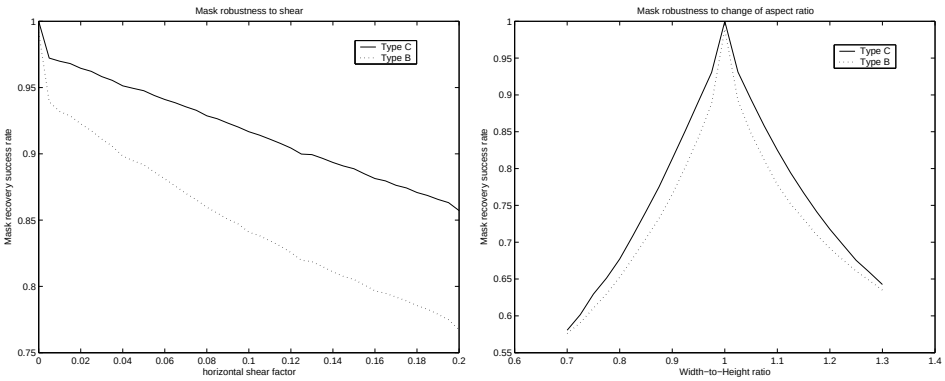


Figure 4.21: *Mask robustness to shearing and change of aspect ratio.*

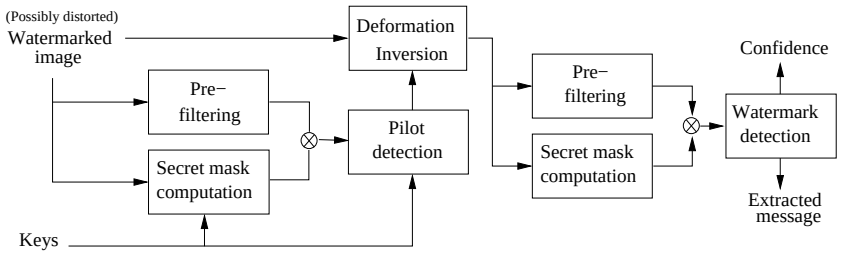
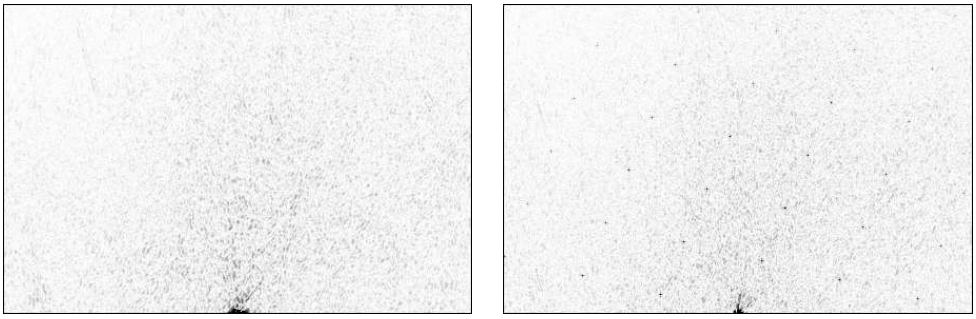


Figure 4.22: *Pilot and watermark detection using secret content dependent modulation.*

tent dependent modulation on the detectability of the auto-correlation synchronization marks. Image 4.23.a shows the auto-correlation function using erroneous binary partition. Image 4.23.b results from the demodulation with the appropriated partition before computing auto-correlation.

Finally, figure 4.24 shows the performances of the global watermarking system. It can be compared to figure 3.20 from previous chapter where no secret modulation is used. Notice however that, in this testing scenario, an additional scaling operation is applied to the image. Increased security is achieved at the cost of a slightly lower robustness. The critical step is the correct detection of the synchronization marks. When deformation can be successfully inverted, results indicate that watermark extraction is achieved without error (i.e. bit error rate is either 0 or close to 50%).

Notice that the size of the protected content after rotation and cropping amounts 459x459 pixels. Due to the high error rate close to borders,



(a) (b)

Figure 4.23: *Masking of synchronization marks: auto-correlation function (a) without mask demodulation, (b) using secret mask demodulation.*

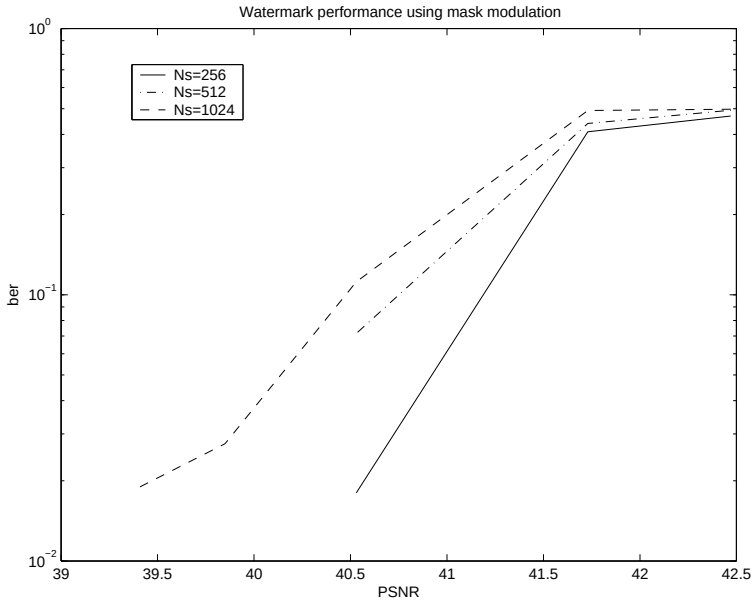


Figure 4.24: *Watermark recovery using mask modulation. (Type B mask, rotation 7°, scaling 95%, 64 bit message, 512x512 Lena).*

the useful image portion is further reduced. One can expect important performance improvements on larger content size.

Previous results show that the scheme will most probably hardly survive important scaling operations. The robustness of the mask against scaling is relatively limited. A solution consists in considering a set of dif-

ferent possible scaling factors and perform several detection accordingly. Reasonable robustness to small scaling factors enable to only consider a limited number of different scalings. Using this approach , it would even be preferable to rely on the type C radius extraction which exhibits still better robustness to rotation while being equivalently robust to small scalings.

4.4 Further developpments

The reference system build on signal content characteristics is not fully robust against considered deformations. Direct large payload message embedding relying on these references is compromised.

We demonstrated however that a two stage watermark detection using pilot signal synchronization and a content based hiding scheme can achieve robustness. This approach provides additional security to the many scheme exploiting synchronization marks to recover from geometrical distortions.

Complementary work should deeper investigate the secrecy level of the mask construction process. We also believe that robustness improvements can be reached in the reference radius extraction scheme. A modification of the analysis function could replace the problematic mean filtering operation. This approach still needs experimental validation.

Chapter 5

Quality assessment of geometrically distorted images

Performing a geometrical transformation on an image produces modifications that can affect the observer perceptual sensitivity and can result in harmful degradations. The ability to quantify this nuisance is valuable to many image-related disciplines, including watermarking. Traditionally, the measure of the degradation consequent to the modification of an image only addressed the pixel value modification. However, the severity of a geometric distortion cannot be measured with such criteria. In this chapter, we present an innovative method to assess the distortion introduced by complex geometric deformations. The distortion metric is expressed in term of how closely the applied transform can be approximated by a simpler transformation model (e.g. RST transform, affine transform). Using the proposed measure, we consider different schemes for the characterization of complex image distortions. Eventually, we discuss how human validation tests could be conducted.

Keywords: Quality assessment, geometrical distortion.

Introduction

Geometrical deformations play an important role in the design of watermarking algorithms. The ability to quantify the amplitude of such distortions can be useful for different aspects in the development of watermarking schemes.

The complexity of the deformation model is only partially linked to the human perceptual sensitivity. Although it is clear that a watermarking

algorithm should be resistant to all possible cropping (as long as enough content is still available), it does not need to be resistant to all possible affine transforms. Indeed, important shear or aspect ratio deformations will produce non valuable resulting images. Similarly, only a small range of the possible projective deformations should be considered. Beyond RST transforms, the general mathematical model of the transform is not sufficient to qualify the perceptual distortion (which is intrinsically linked to watermark requirements). A relevant measure of degradation could help specify which are the distortions that a watermarking scheme should survive. This constitute a first motivation to look for a method to measure the distortion introduced by a geometrical deformation.

Watermarking robustness to geometrical deformations is generally envisaged relatively to a particular model of transformation which corresponds to a specific application scenario. Very few algorithms have been presented that can cope with complex geometrical transformations. Most techniques are resistant to a particular form of transformation thanks to a specific property of their scheme. They often claim being resistant to more complex transformations under the assumption that those can be locally considered as simpler transformation. Many of the mentioned algorithms can indeed be adapted to extend their robustness to more complex deformations. This enhancement is possible when one can consider the global complex deformation that was applied to the image as a juxtaposition of simpler deformations. This approximation is more or less accurate depending on the particular global deformation. Crop resistant algorithms can be enhanced to RST resistant methods [30] provided scaling and rotation have limited amplitude. Some algorithms [47, 29, 62] claim to be resistant against stirmark-like deformations (e.g. bilinear transform, global bending and local sinusoidal distortion) using this property. The complexity to which a particular method can be extended is not evident to state. The success always depends on the model and severity of the applied distortion. It is therefore not straightforward to compare performances of different methods unless they are tested with identical deformation models. However, an infinite number of distortion models could be used to perform such tests. The relevance of a particular model of deformation with respect to watermarking requirements should be studied. A method to assess the increase of complexity represented by a particular deformation with respect to a simpler deformation model could help assessing the exact extent of the robustness of a watermarking scheme.

The essence of watermarking is that it makes use of perceptual tol-

erance to small distortions to hide information within other signals. Imperceptible distortions are applied to the image to yield the watermarked content. However, most existing watermarking schemes introduce only synchronous distortions in the embedding procedure. Geometrical distortion has been very little exploited as an embedding technique. Deformations which do not degrade the content could be applied to adapt the cover content to our needs. We could ensure that the cover content interacts constructively with the watermark to be conveyed. This approach is illustrated in figure 5.1. But distortion itself could also be used to embed information. In a non oblivious scenario, registration could be used to decode a message from the observed distortion (e.g. [80, 81]). Figure 5.2 illustrates how one could parametrize a distortion by a message. Using the same approach, the screen of a movie theater could be distorted in order to identify the origin of illicit movie copies. In a blind scheme, one can displace robust feature points and organize them in meaningful way.

Figure 5.1: *(a) Adapt watermark to content or (b) adapt content to watermark.*

Interpolation inevitably introduces degradations. However, scenarios exist where original content is available in very high resolution. Distributed content intended to consumer use can be watermarked during the downsampling process. Deformation could also be used as a means to fight collusion attacks. These approaches require a precise determination of the distortions which can be considered as imperceptible.

The understanding of perceptual sensitivity to geometrical distortions can also be exploited by an opponent to perform efficient attacks on watermarked contents. However, such malicious manipulations can often rely on manual human validation and therefore already outperform automated quality assessments.

All these considerations advocate to look for a method to characterize

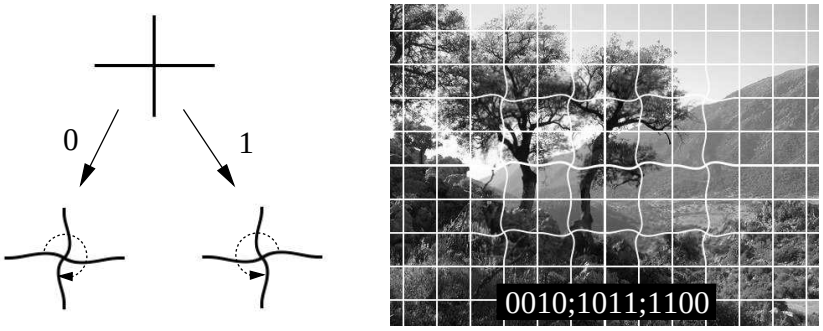


Figure 5.2: *Distortion as support of the hidden information.*

and evaluate the perceptual degradation caused by a geometrical deformation on an image. Image quality assessment is a very important issue in image related disciplines [82]. It has been studied for long and various quality metrics have been proposed [83]. The most basic metric is the Peak Signal-to-Noise Ratio (PSNR) defined as

$$PSNR = 20\log_{10}\frac{255}{\sqrt{\frac{1}{HW}\sum_{i=1}^{W}\sum_{j=1}^{H}\left(I(i,j)-I'(i,j)\right)^2}}, \tag{5.1}$$

where H and W represent the height and width of the image, I and I' represent the intensity signal of the original and modified images. This definition supposes a 8-bit coding of pixel intensity values. This metric is thus related to the mean squared difference between original and modified pixel values. Using established knowledge of the Human Visual System (HVS), many researchers (e.g. [84]) have proposed more elaborated distortion metrics which combine localization, frequency and orientation of the distortion signal. Such approaches can also take into account the interaction of the distortion with the characteristics of the content. Efficient metrics are based on wavelet analysis of both the image content and the distortion signal.

However, existing approaches do not consider that the distortion may involve a desynchronization of the original content. Distortion is defined as an additive signal corresponding to the pixel-to-pixel difference between original and distorted content. Gentle geometric distortions, such as small rotations, lead inevitably to huge distortion measures which do not reflect the induced perceptual effect. In present chapter[1], we address

[1]The work presented in this chapter results from the collaboration with I. Setyawan

this issue by proposing an approach to assess the perceptual degradation caused by the desynchronization of an image signal.

5.1 Measure of desynchronization severity

We aim at characterizing the amplitude of the distortion introduced by an arbitrary geometrical transformation. Geometrical transformations can have very different mathematical expressions and cause little or severe distortion. As the complexity of the transform model increases, it is not straightforward to compare the severity of the distortion introduced by different transformations. Our approach relies on an intuitive perceptual premise. We propose to quantify the amplitude of the distortion by evaluating how closely the transformation can be locally approximated by a smaller order transformation model such as translation (T), rotation-scaling-translation (RST-rigid) or shear-aspect-rotation-scaling-translation (SARST-affine). Our premise relies in the assumption that there exists a class of geometrical deformations which do not cause perceptual degradations. We call to this class of deformations the reference model. Preliminary perceptual tests show that the choice of a low order model of deformation limited to rotation, scaling and translation (RST) could correspond to human sensitivity. However the choice of this specific reference model requires experimental validation.

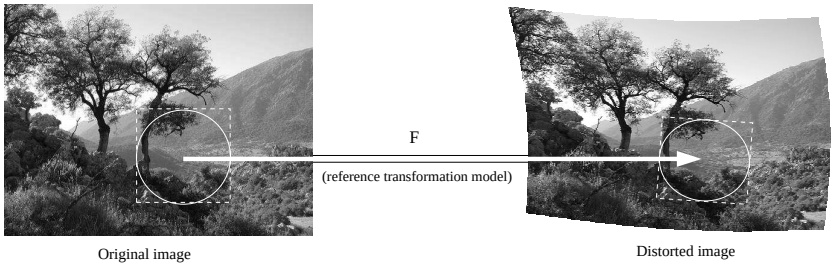


Figure 5.3: *Approximation through a low order transformation model.*

The distortion metric consists in a norm which expresses how different is the observed distortion from the reference class of non-degrading distortions. The process is illustrated in figure 5.3. Considering a region of the image and given the reference (small order) transformation model F, we estimate the parameters of F such that F best approximates the observed

and has been the subject of different publications [6, 85].

distortion. Once the optimization is performed, a distortion measure can be obtained by computing the residual error of the approximation. A characterization of the uniformity and frequency of the distortion can be made by computing this approximation over different regions in the image. In section 5.2, we illustrate the use of this approach to evaluate the severity of geometrical transformations.

We envisage two different methods to find the parameters of the transformation which best approximate the observed distortion. Each method leads to a different optimization criterion.

5.1.1 Approximation using a displacement matching criterion.

This method relies on the availability of a displacement measure for each pixel of the image. This field of vectors can be obtained either through the exact knowledge (mathematical expression) of the undergone transformation, or through an estimation method based on the comparison of the distorted image with an available copy of the original. The first approach relies on the analytical description of the underlying global distortion, while the second approach performs registration between original and distorted images to obtain an estimated field of displacement vectors.

Considering a reference transformation model (e.g. RST) and a field of displacement vectors for a given region of the image, one looks for the transformation parameters which best correspond to the observed displacement field. These parameters can be computed using a least square error optimization. The optimization criterion consists in the mean squared error J_d of the resulting approximation.

Let (x_i, y_i) be a set of original coordinates and (u_i, v_i) the corresponding set of coordinates transformed by the analyzed deformation D. The least square error optimization consists in finding the set of transform parameters $(p_1, p_2, .., p_n)$ that minimizes the cost function J_d. Let F be the simple geometric transformation function used to approximate the global distortion,

$$\begin{pmatrix} x'_i \\ y'_i \end{pmatrix} = F(\mathbf{p}, x_i, y_i) \tag{5.2}$$

where

$$\mathbf{p} = \begin{pmatrix} p_1 \\ p_2 \\ ... \\ p_n \end{pmatrix}. \tag{5.3}$$

The cost function to be minimized can then be expressed as

$$\min J_d = \min_{\mathbf{p}} \sum_i b_i \left\| \begin{pmatrix} u_i \\ v_i \end{pmatrix} - T\left(\mathbf{p}, x_i, y_i\right) \right\|^2, \tag{5.4}$$

where b_i is a weighting factor which can differentiate regions based on image content characteristics. When b_i are chosen equal to one and the reference geometric transformation F is the RST model,

$$\begin{pmatrix} x_i' \\ y_i' \end{pmatrix} = A \begin{pmatrix} cos\theta & sin\theta \\ -sin\theta & cos\theta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} e \\ f \end{pmatrix}, \tag{5.5}$$

this optimization yields a linear system whose solution is given by following expression:

$$\begin{aligned} \theta &= atan\left(\frac{S_2}{S_1}\right); \\ A &= \frac{sin\theta\ S_1 + cos\theta\ S_2}{\left(\frac{\sum x_i \sum x_i}{N} + \frac{\sum y_i \sum y_i}{N} - \sum(x_i^2 + y_i^2)\right)}; \\ N\ e &= \sum_i u_i - A\left(\sum_i x_i\ cos\theta + \sum_i y_i\ sin\theta\right); \\ N\ f &= \sum_i v_i + A\left(\sum_i x_i\ sin\theta - \sum_i y_i\ cos\theta\right); \end{aligned} \tag{5.6}$$

where

$$S_1 = -\sum u_i y_i + \frac{\sum u_i \sum y_i}{N} + \sum v_i x_i - \frac{\sum v_i \sum x_i}{N}, \tag{5.7}$$

$$S_2 = -\sum u_i x_i + \frac{\sum u_i \sum x_i}{N} - \sum v_i y_i + \frac{\sum v_i \sum y_i}{N}. \tag{5.8}$$

The residual error is given by the following expression:

$$\begin{aligned} J_{d,min} &= \sum_i {u_i}^2 + \sum_i {v_i}^2 + A^2\left(\sum_i x_i^2 + \sum_i y_i^2\right) \qquad (5.9) \\ &\quad + \sum_i e^2 + \sum_i f^2 - 2e\sum_i u_i - 2f\sum_i v_i \\ &\quad + 2A\ cos\theta\left(e\sum_i x_i + f\sum_i y_i - \sum_i u_i x_i - \sum_i v_i y_i\right) \\ &\quad + 2A\ sin\theta\left(e\sum_i y_i - f\sum_i x_i + \sum_i v_i x_i - \sum_i u_i y_i\right) \qquad (5.10) \end{aligned}$$

5.1.2 Approximation using an signal intensity matching criterion.

In this second approach, we do not assume knowledge of the underlying function describing the global distortion. Instead, only the original (I) and the distorted (I') images are available. A reference geometric transformation (e.g. rigid or affine) is applied on the original image I to produce an intermediate image I''. A predefined range of parameters $\mathbf{p}$ are tested until an optimal transformation is found. This registration problem can be solved using exhaustive search, gradient search or coarse-to-fine approaches. The optimization criterion is derived from direct pixel value (e.g. luminance and/or color) comparison. The function J_s to be minimized is the residual approximation error between I'' and I', which is computed as follow:

$$\min J_s = \min_{\mathbf{p}} \sum_i \left(I'(x_i, y_i) - I\left(F\left(\mathbf{p}, x_i, y_i\right)\right)\right)^2 \tag{5.11}$$

where I and I′ refer to the luminance value of the original and distorted images and F is the transformation which produces I''. The error measurement in Equation 5.11 is valid if we assume that only geometric distortion has occurred and there are no global luminance modifications (e.g., brightness or contrast changes) between the original and the distorted images. Such a signal registration approach represents computationally expensive operations.

5.2 Characterization of the deformation

Considering the deformation undergone by a region in the image, the above methods provide a measure of the fitting accuracy of an optimal approximation by a reference (low order) transformation model. Minimized J_d and J_s values reflect the mismatch between the optimal low order approximation and the actual undergone deformation.

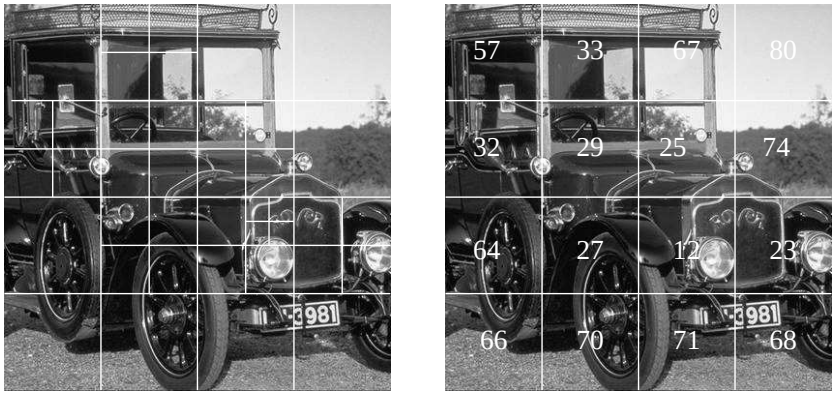
In the first case, J_d corresponds to a mean displacement error, while in the second case J_s represents a mean signal intensity difference. Two important factors are linked to these measures: the size R and the center location (x, y) of the region in the image that was considered performing the measurement. These two factors parametrize J_d and J_s measurements.

Two different analyses can be conducted to yield a characterization of the distortion in the image. The first analysis investigates the uniformity of

the distortion across the image. The second analysis provides a frequency-like locality characterization of the distortion.

5.2.1 Uniformity

Different regions in the same distorted image can exhibit different distortion amplitudes and natures. In order to evaluate this disparity, one must perform the approximation process considering differently centered, but possibly overlapping, subregions. One can either impose the size R of the subregions and observe how the mismatch measure J evolves, or one can set an arbitrary mismatch criterion J_{max} and measure, at different locations within the image, what is the maximum size of the subregion that can be considered. Figure 5.4 illustrates both approaches to evaluate the distortion uniformity.



Fixed J
Measured R

Fixed R
Measured J

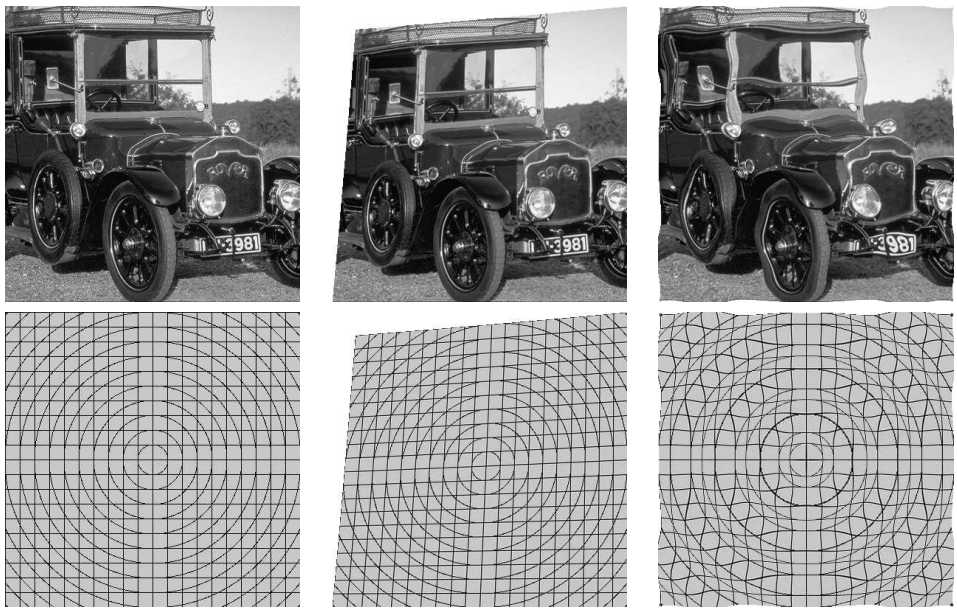
Figure 5.4: *Uniformity characterization.*

Distortion characterization can also reduce to the mean and variance of the metric over the whole image. One could also consider that distortion level is determined by the most severely affected region of the image.

5.2.2 Frequency

Another analysis can be performed by considering the evolution of the mismatch measure J as a function of the considered region size R. One can distinguish local and global behaviors of the distortion. Figure 5.5 illustrates this notion on severely distorted images. One can observe that

the bilinear deformation has a strong global distorting behavior because its mismatch measure strictly increases with the size of the considered region. On the opposite, the sinus based deformation rapidly reaches a maximum mismatch level and then oscillates close to this maximum value.



original bilinear deformation sin-based deformation

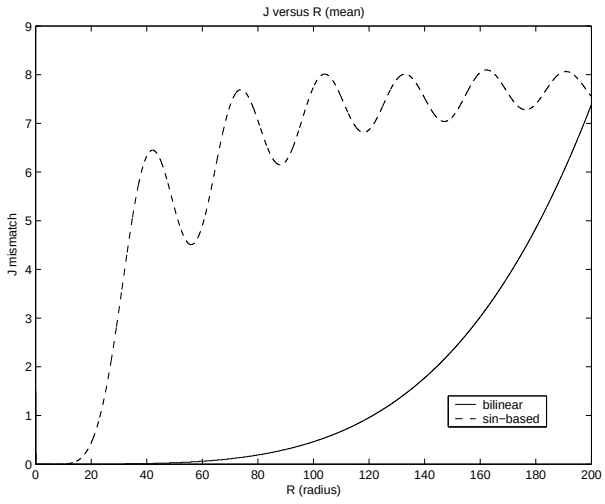


Figure 5.5: *Frequency characterization.*

This frequency analysis shows that, performing the above uniformity analysis, different choices for the observation region size or for the maximal mismatch criterion can lead to opposite conclusions when comparing two distortions. Experimental validation should therefore study the human sensibility to the frequency characteristics of the distortion.

5.3 Content dependence of the perceptual nuisance.

The mismatch measures are sensitive to the type of information that is used to perform the approximation optimization. The J_d mismatch can indeed be computed with the analytical expression of the distortion or with estimated displacements obtained through a registration process. Both approaches could not yield identical approximations. Over flat regions, the registration approach will not be able to perform motion estimation. Severe distortions over these flat regions will therefore not be taken into account in the J_d mismatch measure. The same will happen with the J_S mismatch measure. Such content dependence can also be introduced in the J_d optimization process using region weighting factors. This behavior better corresponds to human perception. Indeed, a human observer will also less likely notice distortions in flat areas.

An analogy can be made with conventional distortion metrics. The PSNR metric does not take into account content characteristics. Elaborated metrics on the opposite, try to take into consideration the interaction between content and distortion. In the same way, efficient geometric distortion metric should perform multi-resolution analysis of the distortion and compare it with content.

On the opposite, one might seek to characterize the distortion caused by a rendering device and therefore rather not be dependent on a specific content.

5.4 Conclusion

The interaction of the content with the distortion shape is a very complex psychological phenomenon. A priori knowledge of the represented content greatly influences our sensibility to modifications. A severe distortion on the face of a well-known personality will cause more nuisance than the same distortion on the branches of a tree. Such distinction cannot be handled by automated processes. As illustrated in figure 5.6, semantic

Figure 5.6: *Influence of semantic on perceived quality.*

information plays a very important role in the way we perceive geometric distortions.

In order to evaluate the correctness of a distortion metric one must rely on intensive human validation. Experimentations aiming at the evaluation of the correspondence between human sensitivity and our approach to perform quality assessment has been conducted by I. Setyawan [86]. Initial results are promising and confirm the relevance of our perceptual premise. Further work should investigate the combined frequency-localization characterization of the distortion and its interaction with image content.

Conclusion

This work was carried out within the scope of the recent but rapidly evolving field of digital watermarking. We investigated the challenging issue represented by the resistance to geometrical deformations and loss of synchronization. During this work, our attention was essentially focused on robustness and security concerns.

In this very active field of research, the task necessitated a continuously updated analysis of newly published solutions. As a result, we produced an extensive classification of the existing approaches to solve the synchronization issue.

Within this ongoing research, our principal contributions consisted in innovative approaches and important improvements in different aspects of the issue.

We developed a generalized construction method for periodic pseudo-random patterns. Based on these patterns, we designed a spread spectrum watermarking scheme with enhanced secrecy properties. We investigated the detection probabilities and the interaction between exhaustive search detection and informed coding strategies. Finally, a scheme for the detection of periodic structure and for the inversion of affine deformation was presented. We showed that the choice of the periodic repetition size involves a trade-off between robustness and secrecy.

Thereafter, we studied the security flaw caused by the lack of secrecy in pilot-registration approaches. We proposed an innovative hiding scheme to remedy to this issue. Our solution involves the extraction of robust local references from the content signal. Using this content normalized interpretation, we showed how one can design secret binary mask and modulate pilot signals in watermarking scheme. The efficiency of the approach is demonstrated on pilots derived from periodic structures.

Eventually, we addressed the assessment of the degradation introduced by a geometrical distortion. We proposed a simple intuitive premise based on local approximations to model the human perceptual sensitivity

to such distortions. Different angles of analysis were studied to describe and compare the degradation amplitude of different geometrical transformations.

Further improvements could be investigated for several of our developments.

Informed encoding strategies can be extended in many schemes resilient to loss of synchronization. In our periodic watermark insertion scheme, we performed optimization with respect to translation of the content. Affine optimization of the watermark pattern could be envisaged.

Our hiding scheme, which relies on content normalization, can still be optimized. The resilience of our reference system to non-rigid deformations could be analyzed. One could look for an affine invariant reference system and compare performances with the current reference system. Interaction between secrecy and robustness could be deeper studied.

Experimental validation of the geometrical degradation measure should be performed. A correct assessment of degradation amplitude could be exploited to optimize existing schemes and design new ones. One could rely on imperceptible geometric deformations of the content in the watermark embedding process.

We believe that, in watermarking, important aspects related to geometrical deformations have not been exploited to their maximum capacity. Similarly, security implications of existing schemes have not been exhaustively envisaged. Potential research on the subject of watermarking and on geometrical distortions is thus far from exhausted.

Publications list

1. D. Delannay and B. Macq, Generalized 2-D cyclic patterns for secret watermark generation, in Proc. of ICIP 2000 - IEEE Signal Processing Society - International Conference on Image Processing, Vancouver, Canada, vol. 2, pp. 77-79, September 10-13, 2000.

2. D. Delannay,J.-F. Delaigle and B. Macq, Compensation of Geometrical Deformations for Watermark Extraction in the Digital Cinema Application, in Proc. of SPIE Electronic Imaging 2001 - Security and Watermarking of Multimedia Contents III, San Jose, vol. 4314, pp. 149-157, February,2001.

3. Damien Delannay, Jean-François Delaigle, Benoit Macq, Joan Maria Mas Ribés and J. Nivart, Integrated fingerprinting in secure digital cinema projection, in Proc. SPIE 47th Annual Meeting - Application of Digital Image Processing XXIV; Andrew G. Tescher Eds., San Diego, USA, vol. 4472, pp. 167-174, July 29 - August 3, 2001.

4. D. Delannay and B. Macq , Method for hiding synchronization marks in scale and rotation resilient watermarking schemes, in Proc. of SPIE Electronic Imaging 2002, Security and Watermarking of Multimedia Contents IV, Edward J. Delp III, Ping W. Wong Eds., San Jose", vol. 4675, pp.548-554, February, 2002.

5. Damien Delannay, Iwan Setyawan, R.L. Lagendijk and Benoit Macq, Relevant modelling and Comparison of geometric distorsions in watermarking systems, in Proc. of SPIE 47th Annual Meeting - Optical Science and Technology - Applications of Digital Image Processing XXV, Andrew G. Tescher Eds., Seattle, USA, vol. 4790, pp. 200-210, July 1-11, 2002.

6. D. Delannay, C. de Roover and B. Macq, Temporal alignment of Video Sequences for Watermarking Systems, in Proc. of SPIE Elec-

tronic Imaging 2003, Security and Watermarking of Multimedia Contents V, Edward J. Delp III, Ping W. Wong eds., Santa Clara, vol. 5020, pp. 481-492, January, 2003.

7. Iwan Setyawan, Damien Delannay, B. Macq and R. L. Lagendijk, Perceptual quality evaluation of geometrically distorted images using relevant geometric transformation modeling, in Proc. of SPIE Electronic Imaging 2003, Security and Watermarking of Multimedia Contents V; Edward J. Delp III, Ping W. Wong, eds.,vol. 5020, pp. 85-94, Santa Clara, January, 2003.

8. Frédéric Lefèbvre, Damien Delannay, A. Gueluy and Benoit Macq, A print and scan optimized watermarking scheme, in Proc. IEEE Fourth Workshop on Multimedia Signal Processing, Cannes, France, October 3-5, pp. 511-516, 2001.

9. Patrick Bas, Damien Delannay and J.M. Chassery, Tatouage d'images fixes, chapitre de l'ouvrage Tatouage de Documents Audiovisuels Numériques, F. Davoine and S. Pateux eds., Traité IC2, Hermes Science, mars 2004.

10. Damien Delannay and Benoit Macq, 2-D Periodic Patterns for Image Watermarking, chapter of Optical and Digital Techniques for Information Security, Bahram Javidi eds., Springer-Verlag, Berlin, June 2004, ISBN:0-387-20616-7.

Bibliography

[1] A. S. Cohen and A. Lapidoth, "Generalized writing on dirty paper," in *International Symposium on Information Theory (ISIT)*, p. 227, (Lausanne, Switzerland), July 2002.

[2] U.Erez and R.Zamir, "Achieving 0.5 log(1+snr) over the additive white gaussian noise channel with lattice encoding and decoding," *IEEE Transactions on Information Theory* , submitted May 2001, revised September 2003.

[3] I. Cox, M. Miller, and J. Bloom, *Digital Watermarking*, vol. ISBN: 1-55860-714-5, Morgan Kaufmann Publishers, 2002.

[4] F. Davoine and S. Pateux, eds., *Tatouage de Documents Audiovisuels Numériques*, Hermes Science, traité IC2 ed., mars 2004.

[5] J. G. Proakis, ed., *Digital Communications*, ch. 13, pp. 695–753. McGraw-Hill International Editions, 1995. ISBN 0-07-113814-5.

[6] D. Delannay, I. Setyawan, R. Lagendijk, and B. Macq, "Relevant modelling and comparison of geometric distorsions in watermarking systems," in *Proc. of SPIE 47th Annual Meeting - Optical Science and Technology - Applications of Digital Image Processing XXV; Andrew G. Tescher; Eds.*, **4790**, pp. 200–210, (Seattle, USA), July 1-11 2002.

[7] X. Desurmont, "A study on robust image watermarking algorithms against geometric attacks," Master's thesis, DEA Université de Paris XI, Institut d'Electronique Fondamentale, France, September 2001.

[8] F. Petitcolas, R. Anderson, and M. Kuhn, "Attacks on copyright marking systems," in *Inf. hiding 2nd workshop,*, S. V. LNCS, ed., **1525**, pp. 219–239, 1998.

[9] F. A. P. Petitcolas and R. J. Anderson, "Evaluation of copyright marking systems," **1**, pp. 574–579, Proceedings of IEEE Multimedia Systems'99, (Florence, Italy), 7-11 June 1999.

[10] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," Tech. Rep. 95-10, NEC Research Institute, Princeton, NJ, USA, 1995.

[11] B. Zitova and J. Flusser, "Image registration methods: a survey," *Image and Vision Computing* **21**, pp. 977–1000, 2003.

[12] A. Goshtasby, "Registration of images with geometric distortions," *T-GRS* **26**, pp. 60–64, 1988.

[13] J. B. A. Maintz and M. A. Viergever, "A survey of medical image registration," *Medical Image Analysis* **2(1)**, pp. 1–36, 1998.

[14] F. Davoine, P. Bas, P.-A. Hébert, and J.-M. Chassery, "Watermarking et résistance aux déformations géométriques," *In J.-L. Dugelay, ed., Cinquième journées d'étude et d'échanges sur la compression et la représentation des signaux audiovisuels (CORESA'99)* , (Sophia-Antipolis, France), 14-15 Jun 1999.

[15] G. W. Braudaway and F. Mintzer, "Automatic recovery of invisible image watermarks from geometrically distorted images," in *Security and Watermarking of multimedia contents II, SPIE*, **3971**, (San-Jose CA, USA), January 2000.

[16] P. Loo and N. G. Kingsbury, "Watermarking using complex wavelets with resistance to geometric distortion," in *The 10th European Signal Processing Conference (Eusipco 2000)*, (Tampere, Finland), 5-8 September 2000.

[17] P. Loo and N. G. Kingsbury, "Motion estimation based registration of geometrically distorted images for watermark recovery," in *in Security and Watermarking of Multimedia Contents, part of SPIE Electronic Imaging*, **4314**, (San Jose), Jan 2001.

[18] D. Delannay, J.-F. Delaigle, B. Macq, J. M. M. Ribés, and J. Nivart, "Integrated fingerprinting in secure digital cinema projection," in *SPIE 47th Annual Meeting - Application of Digital Image Processing XXIV; Andrew G. Tescher; Eds.*, **4472**, pp. 167–174, (San Diego, USA), July 29 - August 3 2001.

[19] P. Dong, J. Brankov, N. Galatsanos, and Y. Yang, "Geometric robust watermarking based on a new mesh model correction approach," *IEEE Int. Conf. on Image Processing ICIP* , (Rochester, NY, USA), 2002.

[20] B. Natarajan, "Robust public key watermarking of digital images," *HP Laboratories Technical Report, no. 97-118* , pp. 1–10, october 1997.

[21] N. F. Johnson, Z. Duric, and S. Jajodia, "Recovery of watermarks from distorted images," in *Lecture Notes in Computer Science*, Springer-Verlag, ed., *Proceedings, Third Information Hiding Workshop* **1768**, pp. 318–332, (Dresden, Germany), 29 September - 1 October 1999.

[22] Q. Sun, J. Wu, and R. Deng, "Recovering modified watermarked image with reference to originale image," in *Proc. SPIE*, pp. 415–424, January 1999.

[23] I. Ozer, M. Ramkumar, and A. Akansu, "A new method for detection of watermarks in geometrically distorted images," in *Proceedings of IEEE International Conference on Accoustic, Speech, and Signal Processing (ICASSP) 2000*, 5-9 June 2000.

[24] S. Kay and E. Izquierdo, "Robust content based image watermarking," in *WIAMIS 2001 - Workshop on Image Analysis for Multimedia Interactive Services*, (Tampere, Finland), 16-17 May 2001.

[25] I. Agung and P.Sweeney, "Method for combating random geometric attack on image watermarking," *IEE Electronics Letters* **37**, pp. 420–421, 29 March 2001.

[26] J. Lichtenauer, I. Setyawan, T. Kalker, and R. Lagendijk, "Exhaustive geometrical search and false positive watermark detection probability," in *SPIE Electronic Imaging 2002, Security and Watermarking of Multimedia Contents V*, (Santa Clara), January 2003.

[27] J. L. T. Kalker and G. Depovere, "Modelling the false-alarm and missed detection rate for electronic watermarks," in *Workshop on Information Hiding*, S. L. N. on Computer Science, ed., pp. 329–343, (Portland, OR), 15-17 April 1998.

[28] M. L. Miller and J. A. Bloom, "Computing the probability of false watermark detection," in *Information Hiding*, pp. 146–158, 1999.

[29] F. Hartung, J. Su, and B. Girod, "Spread-spectrum watermarking : Malicious attacks and counterattacks," in *Security and Watermarking of multimedia contents, SPIE*, **3657**, (San-Jose CA, USA), January 1999.

[30] A. Tefas and I. Pitas, "Multi-bit image watermarking robust to geometric distorsions," in *IEEE-ICIP'2000*, (Vancouver, Canada), 2000.

[31] S. Baudry, P. Nguyen, and H. Maître, "Estimation of geometric distorsions in digital watermarking," *In IEEE- ICIP 2002* , (Rochester (USA)), September 2002.

[32] V. Solachidis and I. Pitas, "Circularly symetric watermark embedding in 2-d dft domain," *ICASSP'99* **6**, pp. 3469–3472, (Phoenix, Arizona), 15-19 March 1999.

[33] M. Maes, T. Kalker, J. Linnartz, J. Talstra, G. Depovere, and J. Haitsma, "Digital watermarking for dvd video copy protection," *IEEE Signal Processing Magazine* **17**(5), pp. 47–57, 2000.

[34] D. Delannay and B. Macq, "Generalized 2-d cyclic patterns for secret watermark generation," in *ICIP 2000 - IEEE Signal Processing Society - International Conference on Image Processing*, **2**, pp. 77–79, (Vancouver, Canada), September 10-13 2000.

[35] W. Bender, D. Gruhl, and N. Morimoto, "Techniques for data hiding," *tech. rep., MIT Media Lab* , 1996.

[36] M. Kutter, F. Jordan, and F. Bossen, "Digital signature of color images using amplitude modulation," in *Proc. SPIE Storage and Retrieval for Image and Video Databases*, **3022**, pp. 518–526, (San Jose, California), 1997.

[37] M. Alghoniemy and A. H. Tewfik, "Progressive quantized projection watermarking scheme," *Proc. of the 7th ACM International Multimedia Conference* , pp. 295–298, (Orlando, FL), Nov. 1999.

[38] D. Fleet and D. Heeger, "Embedding invisible information in color images," in *IEEE-ICIP'97*, **1**, pp. 532–535, (Santa Barbara (Cal) Usa), 1997.

[39] A. Herrigel, J. J. K. O. Ruanaidh, H. Petersen, S. Pereira, and T. Pun, "Secure copyright protection techniques for digital images," in *In David Aucsmith ed., Information Hiding*, L. N. o. C. S. Springer Verlag,

ed., **1525**, pp. 169–190, (Berlin, 1998. (Second International Workshop IH'98, Portland, OR, USA, April 15-17, 1998)), 1998.

[40] F. Deguillaume, G. Csurka, J. J. K. O. Ruanaidh, and T. Pun, "Robust 3d dft video watermarking," **Vol. 3657 of SPIE Proceedings**, pp. 113–124, Electronic Imaging '99: Security and Watermarking of Multimedia Contents, (San Jose CA, USA), 23-29 January 1999.

[41] S. Pereira and T. Pun, "An iterative template matching algorithm using the chirp-z transform for digital image watermarking," in *Pattern Recognition, 33, 1*, pp. 173–175, January 2000.

[42] C. Serdean, M. Ambroze, M. Tomlinson, and G. Wade, "Dwt based video watermarking for copyright protection invariant to geometrical attacks," in *International Symposium on Communication Systems, Networks and Digital Signal Processing*, (Staffordshire University, UK), July 15-17 2002.

[43] S. Pereira, J. J. K. O. Ruanaidh, F. Deguillaume, G. Csurka, and T. Pun, "Template based recovery of Fourier-based watermarks using log-polar and log-log maps," *In IEEE Multimedia Systems 99, International Conference on Multimedia Computing and Systems* **1**, pp. 870–874, (Florence, Italy), 7-11 June 1999.

[44] M. Kutter, "Watermarking resisting to translation, rotation and scaling," *Proc. of SPIE, Multimedia Systems and Applications* **3528**, (Boston, MA, USA), November 1-6 1998.

[45] S. Voloshynovskiy, F. Deguillaume, and T. Pun, "Content adaptive watermarking based on a stochastic multiresolution image modeling," *In Tenth European Signal Processing Conference (EUSIPCO'2000)* , (Tampere, Finland), September 5-8 2000.

[46] C. Honsinger and M. Rabanni, "Data embedding using phase dispersion," in *In Proc. Int. Conf. on Information Technology*, 2000.

[47] S. Voloshynovskiy, F. Deguillaume, and T. Pun, "Multibit digital watermarking robust against local nonlinear geometrical distorsions," in *IEEE-ICIP'01*, (Thessaloniki, Greece), 7-10 October 2001.

[48] M. Alvarez-Rodriguez and F. Perez-Gonzalez, "Analysis of pilot-based synchronization algorithms for watermarking of still images," *Signal Processing -Image Communication* , pp. 611–633, sep 2002.

[49] F. Deguillaume, S. Voloshynovskiy, and T. Pun, "A method for the estimation and recovering from general affine transforms in digital watermarking applications," in *SPIE Electronic Imaging 2002, Security and Watermarking of Multimedia Contents IV*, (San Jose), February 2002.

[50] P. Moulin and A. Ivanovic, "The fisher information game for optimal design of synchronization patterns in blind watermarking," in *Proc. IEEE Int. Conf. on Image Proc.*, **2**, pp. 550–553, (Thessaloniki, Greece), October 2001.

[51] A.Herrigel, S. Volosjynovskiy, and Y. Rytsar, "The watermark template attack," in *Security and Watermarking of multimedia contents III, SPIE*, (San-Jose CA, USA), January 2001.

[52] J. Haitsma and T. Kalker, "A watermarking scheme for digital cinema," in *IEEE-ICIP'01*, **2**, pp. 487–489, (Thessaloniki, Greece), 7-10 October 2001.

[53] Y. Zhao and R. Lagendijk, "Video watermarking scheme resistant to geometric attacks," *IEEE Int. Conf. on Image Processing ICIP* , (Rochester, NY, USA), 2002.

[54] I. Setyawan, G. Kakes, and R. L. Lagendijk, "Synchronization-insensitive video watermarking using structured noise pattern," in *SPIE Electronic Imaging 2002, Security and Watermarking of Multimedia Contents IV*, (San Jose), February 2002.

[55] C. B. X. Niu, M. Schmucker, "Video watermarking resisting to rotation, scaling and translation," in *SPIE Electronic Imaging 2002, Security and Watermarking of Multimedia Contents IV*, January 2002.

[56] D. Coltuc and P. Bolon, "Watermarking by histogram specification," **Vol. 3657 of SPIE Proceedings**, pp. 252–263, Electronic Imaging '99: Security and Watermarking of Multimedia Contents, (San Jose CA, USA), 23-29 January 1999.

[57] J. J. K. O. Ruanaidh and T. Pun, "Rotation, scale and translation invariant spread spectrum digital image watermarking," *Signal Processing* **66**, pp. 303–318, May 1998.

[58] C. Lin, M. Wu, J. A. Bloom, I. Cox, M. Miller, and Y. Lui, "Rotation, scale, and translation resilient public watermarking for images," *Proceedings of the SPIE, Security and Watermarking of Multimedia Contents* **3971**, pp. 90–98, 2000.

[59] C.-Y. Lin, "Public watermarking surviving general scaling and cropping: An application for print-and-scan process," Multimedia and Security Workshop at ACM Multimedia 99, (Orlando, FL, USA), Oct 1999.

[60] M. Alghoniemy and A. H. Tewfik, "Geometric distortions correction in image watermarking," in *Conference Electronic Imaging, Proceedings of SPIE Vol. 3971, Security and Watermarking of Multimedia Contents II* **3971**, pp. 82–89, (San Jose, CA), January 24-26 2000.

[61] M. Kutter, S. K. Bhattacharjee, and T. Ebrahimi, "Towards second generation watermarking schemes," in *IEEE-ICIP'99*, **1**, pp. 320–323, (Kobe, Japan), October 1999.

[62] P. Bas, J. Chassery, and B. Macq, "Robust watermarking based on the warping of predefined triangular patterns," in *Security and Watermarking of multimedia contents, SPIE*, **3971**, pp. 99–109, (San-Jose (CA)), January 2000.

[63] P. Bas and B. Macq, "A new video-object watermarking scheme robust to object manipulation," in *IEEE-ICIP'01*, (Thessaloniki, Greece), 7-10 October 2001.

[64] P. Bas, J.-M. Chassery, and B. Macq, "Geometrically invariant watermarking using feature points," *IEEE Transactions on Image Processing* **11**, pp. 1014–1028, September 2002.

[65] D. Delannay and B. Macq, "Method for hiding synchronization marks in scale and rotation resilient watermarking schemes," in *Proc. of SPIE Electronic Imaging 2002, Security and Watermarking of Multimedia Contents IV; Edward J. Delp III, Ping W. Wong; Eds.*, **4675**, pp. 548–554, (San Jose), February 2002.

[66] S. Baudry, J.-F. Delaigle, B. Sankur, B. Macq, and H. Maître, "Analyses of error correction strategies for typical communication channels in watermarking," *Signal Processing* **81**, pp. 1239–1250, June 2001.

[67] A. Tirkel, R. van Schyndel, and C. Osborne, "A two-dimensional digital watermark," in *in Proc. of Digital Image Computing, Technology and Applications (Dicta'95)*, pp. 378–383, (University of Queensland, Brisbane, Australia), December 6-8 1995.

[68] M. Kutter, S. Volosjynovskiy, and A.Herrigel, "The watermark copy attack," in *Security and Watermarking of multimedia contents II, SPIE*, **3971**, pp. 371–380, (San-Jose CA, USA), January 2000.

[69] F. MacWilliams and N.J.A.Sloane, "Pseudo-random sequences and arrays," in *Proc.IEEE*, **64**, pp. 1715–1729, Dec 1976.

[70] J. F. Delaigle, C. DeVleeschouwer, and B. Macq, "Watermarking algorithm based on a human visual system," *Signal Processing* **66**, pp. 319–336, May 1998.

[71] R. B. Wolfgang, C. I. Podilchuk, and E. J. Delp, "Perceptual watermarks for digital images and video," *Proc. of the IEEE* **87**(7), pp. 1108–1126, 1999.

[72] S. W. Martin Kutter, "A vision-based masking model for spread-spectrum image watermarking," *IEEE Trans. Image Processing* **11**, pp. 16–25, January 2002.

[73] G. Depovere, T. Kalker, and J. Linnartz, "Improved watermark detection reliability using filtering before correlation," in *IEEE-ICIP'98*, **I**, pp. 430–434, (Chicago (IL, USA)), October 1998.

[74] M. Unser, "Splines: A perfect fit for signal and image processing," *IEEE Signal Processing Magazine* **16**, pp. 22–38, November 1999.

[75] I. J. Cox, M. L. Miller, , and A. L. McKellips, "Watermarking as communications with side information," in *Proc.of the IEEE*, pp. 1127–1141, (Special Issue on Identification and Protection of Multimedia Information), July 1999.

[76] S. Voloshynovskiy, F. Deguillaume, S. Pereira, and T. Pun, "Optimal adaptive diversity watermarking with channel state estimation," in *In SPIE Photonics West, Electronic Imaging 2001, Security and Watermarking of Multimedia Contents III, No. paper 4314-74*, E. W. Wong, E. J. Delp, ed., (San Jose, CA, USA), January 21-26 2001.

[77] S. Pereira and T. Pun, "Fast robust template matching for affine resistant image watermarking," *In International Workshop on Information Hiding, Vol. LNCS 1768 of Lecture Notes in Computer Science* , pp. 200–210, (Dresden, Germany), 29 September - 1 October 1999.

[78] M. Alghoniemy and A. H. Tewfik, "Geometric distortion correction through image normalization," in *IEEE International Conference on Multimedia and Expo (III)*, pp. 1291–, 2000.

[79] P. Dong and N. P. Galatsanos, "Affine transformation resistant watermarking based on image normalization," *International Conference on Image Processing* , (Rochester, NY), September 2002.

[80] M. Maes and C. M. van Overveld, "Digital watermarking by geometric warping," in *IEEE- ICIP'98*, **II**, pp. 424–429, (Chicago (IL, US)), October 1998.

[81] P. Rongen, M. Maes, and K. van Overveld, "Digital image watermarking by salient point modification: practical results," **Vol. 3657 of SPIE Proceedings**, Electronic Imaging '99: Security and Watermarking of Multimedia Contents, (San Jose CA, USA), 23-29 January 1999.

[82] "Methodology for the subjective assessment of the quality of television pictures," *ITU-R Recommendation BT.500-7* .

[83] "Special issue on image quality assessment," *Signal Processing* **70**, 1998.

[84] A. Beghdadi and B. Pesquet-Popescu, "A new image distortion measure based on wavelet decomposition," *(invited) Proc. IEEE ISSPA2003* , (Paris, France), 1-4 July 2003.

[85] I. Setyawan, D. Delannay, B. Macq, and R. L. Lagendijk, "Perceptual quality evaluation of geometrically distorted images using relevant geometric transformation modeling," in *Proc. of SPIE Electronic Imaging 2003, Security and Watermarking of Multimedia Contents V; Edward J. Delp III, Ping W. Wong, eds.*, **5020**, pp. 85–94, (Santa Clara), January 2003.

[86] I. Setyawan and R. L. Lagendijk, "Human perception of geometric distortions in images," in *Proc. of SPIE Electronic Imaging 2004, Security and Watermarking of Multimedia Contents VI; Edward J. Delp III, Ping W. Wong, eds.*, (San Jose), January 2004.

[87] D. Delannay, J.-F. Delaigle, and B. Macq, "Compensation of geometrical deformations for watermark extraction in the digital cinema application," in *SPIE Conference 4314 - Security and Watermarking of Multimedia Contents III*, **4314**, pp. 149–157, (San Jose), February 2001.

[88] D. Delannay, C. de Roover, and B. Macq, "Temporal alignment of video sequences for watermarking systems," in *Proc. of SPIE Electronic Imaging 2003, Security and Watermarking of Multimedia Contents V; Edward J. Delp III, Ping W. Wong, eds.*, **5020**, pp. 481–492, (Santa Clara), January 2003.

[89] F. Lefèbvre, D. Delannay, A. Gueluy, and B. Macq, "A print and scan optimized watermarking scheme," in *IEEE Fourth Workshop on Multimedia Signal Processing Proc.*, pp. 511–516, (Cannes, France), October 3-5 2001.