2013

Resilient Digital Image Watermarking Using a DCT- Component Perturbation Model

Jonathan Blackledge
Technological University Dublin, jonathan.blackledge@tudublin.ie

Oleksandr Iakovenko
Odessa National Polytechnic University, Ukraine

Recommended Citation

Blackledge, J., Iakovenko, O. :Resilient Digital Image Watermarking Using a DCT- Component Perturbation Model in (Carr,H., Grimstead, I., eds) EG UK Theory and Practice of Computer Graphics, forthcoming. doi:10.21427/f8mb-3d82

EG UK Theory and Practice of Computer Graphics (2011)
Hamish Carr, Ian Grimstead (Editors)

Resilient Digital Image Watermarking using a DCT-component Perturbation Method

J. Blackledge[1] and O. Iakovenko[2]

[1]Dublin Institute of Technology, Ireland
[2]Odessa National Polytechnic University, Ukraine

Abstract

The applications of the Discrete Cosine Transform (DCT) for Computer Generated Imagery, image processing and, in particular, image compression are well known and the DCT also forms the central kernel for a number of digital image watermarking methods. In this paper we consider the application of the DCT for producing a highly robust method of watermarking images using a block partitioning approach subject to a self-alignment strategy and bit error correction. The applications for the algorithms presented include the copyright protection of images and Digital Right Management for image libraries, for example. However, the principal focus of the research reported in this paper is on the use of print-scan and e-display-scan image authentication for use in e-tickets where QR code, for example, are embedded in an full colour image of the ticket holder. This requires that a DCT embedding procedure is developed that is highly robust to blur, noise, geometric distortions such as rotation, shift and barrel and the partial removal of image segments, all of which are considered in regard to the resilience of the method proposed and its practical realisation in a real operating environment.

Categories and Subject Descriptors (according to ACM CCS):
I.3.3 [Computer Graphics]: Picture/Image Generation—D.2.11 [Software Engineering]: Software Architectures—Information hiding I.4.3 [Image Processing and Computer Vision]: Enhancement—Geometric correction I.4.3 [Pattern Recognition]: Models—Structural

1. Introduction

Watermarking digital images has become a common concern with regard to copyright protection and Digital Rights Management. The principal aim is to design algorithms which provide for the authentication of both single or multiple image frames by hiding information in an image that is encrypted or otherwise [Bla02]. A large amount of copyright information now resides in digital image form especially with regard to the growth of electronic publishing and the future of networked multimedia systems is becoming increasingly conditioned by the development of efficient methods to protect ownership rights against unauthorised copying and redistribution. Digital image watermarking has emerged as a candidate to solve this problem and since the mid-1990s there has been a convergence of a number of different information protection technologies whose theme is the hiding (as opposed to encryption) of information. We thus present a brief introduction on watermarking and Steganography in the following section.

1.1. Watermarking and Steganography

Information hiding can refer to either making additional information imperceptible or keeping the existence of the information secret. Important sub-disciplines of information hiding are Steganography and watermarking which are concerned with techniques that are used to imperceptibly convey information. However, they are two different and distinct disciplines. Watermarking is the practice of hiding a information (copyright information, for example) about an image without degrading its quality in such a way that it is expected to be permanently embedded into the data and can be detected at a later date. Steganography is the study of the techniques used to hide one message inside another, without disclosing the existence of the hidden message or

making it apparent to an observer that it exists. Digital image watermarking and Steganography are thus distinguished from each other as follows ([CMB02], [AP98] and [PK99]): (i) Steganography is the 'art' of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message whereas the information hidden by a digital watermarking system (which can also refer to the application of visible watermarks, commonly used to protect image samples, for example, from unauthorised use) is always associated with the object to be protected or its owner (Steganographic systems focusing on just hiding information); (ii) the purpose of Steganography is to provide for the covert communication between two parties whose existence is unknown to a possible attacker, a successful attack being the detection of the existence of this covert communication; (iii) watermarking has an additional requirement of its robustness against possible attacks so that even if the existence of the hidden information is known, it should be hard for an attacker to destroy the watermark (Steganography being mainly concerned with the non-detection of hidden data while watermarking is concerned with potential removal by a pirate); (iv) Steganographic communications are usually point-to-point (between sender and receiver) while watermarking techniques are usually one-to-many and while Steganography is primarily concerned with the capacity of hidden information and its impact on perception, watermarking can focus on the robustness of relatively small amounts of hidden data compared to the size and resolution of the host.

1.2. Principal Components of Digital Watermarking

All watermarking schemes share the same generic building blocks: Watermark embedding and information extraction [HW99].

1.2.1. Watermark Embedding (Signature Casting)

The embedded data is the watermark that one wishes to embed. It is usually hidden in data referred to as a cover, producing the watermarked cover. The inputs to the embedding system are the watermark, the cover and an optional key (including system parameters). A key is used to control the embedding process so as to restrict detection and/or recovery of the embedded data to parties who know of it. The watermarked cover may face some intentional and/or unintentional distortion that may affect the existence of the watermark.

1.2.2. Watermark Detection System (Extraction)

The inputs to the detection system are the possibly distorted watermarked cover, the key and depending on the method, the original cover or the original watermark. Its output is either the recovered watermark or some kind of confidence measure indicating how likely it is for a given watermark at the input to be present in the work under inspection. Many current watermarking schemes may be viewed as spread-spectrum communication systems whose aim is to send the watermark between two parties with two sources of noise; noise due to the original cover and noise due to processing.

1.3. Fragility and Robustness of Watermarked Images

One of the most important issues in modern image watermarking development concerns the issue of robustness. In general, image watermarking methods fall into two basic categories: Fragile Watermarks and Robust Watermarks. Fragile watermarks can be destroyed as soon as the image is modified in some way. They are usually applied to detect modifications of the watermarked data rather than conveying unreadable information. Compared to cryptographic techniques with regard to data authentication, there are two significant benefits that arise from using a watermark: (i) the signature becomes embedded in the message; (ii) it is possible to create 'soft authentication' algorithms that offer a multi-valued measure that accounts for different unintentional transformations that the data may have suffered instead of a binary True/False answer given by cryptography-based authentication.

Robust Watermarks have the property that is not feasible to remove them or make them useless without destroying the image at the same time. This usually means that the mark should be embedded in the most robustly significant components of the object. It also means that the hidden information, or at least a significant portion of it, can be recovered subject to distortion from geometric features, noise and blur etc. that occur when the image is printed and scanned, for example, or when it is transmitted in a noisy environment and/or compressed for archiving.

With regard to the generic robustness of a watermarked image, the principal goal is to prevent attacks designed to diminish or remove the presence of a watermark from its associated content while preserving the content so that it is not made redundant after an attack has taken place. Important examples of 'robustness to attacks' are as follows:

Additive Noise. This may happen (unintentionally) in certain applications such as D/A (printing) and A/D (scanning) converters or from transmission errors. It can happen intentionally by an attacker who is trying to destroy the watermark (or make it undetectable) by adding noise to the watermarked cover.

Filtering. Linear filtering such as low-pass filtering (e.g. a Gaussian Blur) or non-linear filtering such as median filtering.

Collusion Attack. In some watermarking schemes, if an image has been watermarked many times using different keys, it is possible to collect many such copies and 'average' them into a composite image that closely resembles the original image and does not contain any useful watermarking data [MM97].

Inversion Attack (elimination attack). An attacker may try to estimate the watermark and then remove it by subtracting the estimate or reverse the insertion process to perfectly remove the watermark. This means that an attacked image can not be considered to contain a watermark at all (even using a more sophisticated detector). Note, that with different watermarked objects, it is possible to improve the estimate of the watermark by simple averaging.

Lossy Compression. This is generally an unintentional attack which often appears in multimedia applications. Nearly all digital images that are currently distributed via the Internet are in compressed form. Lossy image compression algorithms are designed to disregard redundant perceptually-insignificant information in the coding process. Watermarking tries to add invisible information to the image in such a way that it is not perceptually significant. An optimal image coder will therefore simply remove any embedded watermark information. However, even state-of-the-art image coding such as JPEG 2000++ does not achieve optimal coding performance and therefore there is a 'distortion gap' that can be exploited for watermarking.

1.4. About this Paper

A very commonly used image watermarking method is based on the replacement of Least Significant Bits (LSB) in data samples of host images with bits of hidden data. However, this approach is not applicable with common multimedia file formats as modern compression techniques often distort LSB during the compression process. Common examples are JPEG and MPEG formats which store multimedia information in the form of rounded (nearest integer) spectral components using the (Discrete) Cosine Transform. Quantisation in a spectral domain distorts data in the spatial domain. This leads to the near complete elimination of LSB embedded data during compression operations. However, while LSB embedding can not be applied in the spatial domain, it can still be applied in spectral domain. Thus, the Discrete Cosine Transform (DCT) coefficients of a JPEG image can be the subject of LSB based watermarking. In this paper we address a method that uses a spectral embedding pattern approach on a block-by-block basis. The focus of the method is on the generation of very high resilience full colour image watermarking that can be used on a print-scan basis or an e-display-scan basis for applications that include e-tickets in which QR codes are embedded in an image of the ticket holders portrait, for example. After providing a brief overview of watermarking techniques, we consider a new block based DCT approach and present details of its performance to various attacks associated with low resolution scans of an image watermarked using the algorithms developed. The originality of the method given relates to the detail associated with DCT based embedding technique used and the extraction processes applied (including a new self-alignment method based on the watermark) which 'reflect' the authors original contribution to the field.

2. A Short Overview of Image Watermarking Techniques

Image watermarking algorithms fall into two fundamental categories, spatial techniques and transform techniques. Spatial techniques embed information by direct data modification. They are usually simple to implement, require low computational cost but tend to be less robust. Transform techniques encoded information by modifying the coefficients obtained from a discrete transformation using transforms such as the Fourier Transform, Cosine Transform, Wavelet Transform, Walsh Transform, Wigner Transform, Affine Transform and others. In fact there is no effective limit to the type and/or number of transforms that can be applied in principle if a valuable and computationally cost effective algorithm can be designed that is functional within the constraints placed on the operational characteristics of the watermarking application under consideration. This is why there is, as yet, no provable unique watermarking algorithm that is optimal with regard to all constraints and, in turn, why so many algorithms have been considered in the literature as detailed in [Bla02] and references therein. On the other hand, there are a large number of methods that can be strictly or loosely classified within the context of the Wavelet Transform, the difference being related to the exact wavelet that is applied.

If $I_{i,j}$ denotes a digital images, then a transform $\hat{T}$ is applied to yield a matrix of coefficients $c_{i,j}$

$$c_{i,j} = \hat{T}[I_{i,j}]$$

These coefficients are then modified in some way (e.g. by the replacement of selected elements with new values relating to the watermark information) thereby generating a new matrix $C_{i,j}$ such that

$$J_{i,j} = \hat{T}^{-1}[C_{i,j}] \sim J_{i,j}$$

where $\hat{T}^{-1}$ denotes the inverse operator. This process relies on both the existence and the computational stability of the transform $\hat{T}$ and its inverse $\hat{T}^{-1}$ and can be applied either to the image in its entirety on a block-by-block basis where the size of each block is an integer fraction of the image size thereby providing a greater degree of freedom for the embedding on information. It can also be applied to the individual channels associated with the colour model applied to a colour image thereby providing a further degree of 'colour embedding space'. In most cases, the embedded information can be of an encrypted form although this can place certain constraints on the watermarking scheme with regard to the need to decrypt the information subject to distortions due to an attack on the host image and/or watermark data [Bla08], [YK10] and [LW10].

Although, as mentioned before, the proliferation of watermarking schemes is a due to a lack of uniqueness criteria in respect of the transform $\hat{T}$ that is used, certain transforms are based on 'optically significant' kernels that are related to the field of mathematical modelling and computational physics [SZ06]. For example, Fresnel optics is based on a unique quadratic phase factor in which the Point Spread Function has the form $\exp[i\pi(x^2+y^2)/f\lambda]$ where f is the focal length and λ is the wavelength associated with the 'imaging system' [Bla05]. The same quadratic form occurs in the field of statistical mechanics, for example, yielding wavelets such as the 'Heatlet' with bi-orthogonal scaling polynomial properties [She00] and in quantum mechanics in which the fundamental solution to the one-dimensional Schrödinger equation is determined by a 'Chirplet' of the form (for normalised units) $\exp(ix^2/2t)/\sqrt{2\pi it}$ [Tsa06]. The application of a tensor product of such Chirplets to provide a set of four two-dimensional Chirplets yields very high resilience to noise using a block watermarking scheme [BI13].

Image watermarking methods have also been developed which make use of the non-deterministic wavelets and use a process known as 'Stochastic Diffusion' which has the advantage of encrypting the watermark by default [BAR11a] and can be applied to full colour image watermarking using three hosts images [BAR11b] and [BAR13]. In this case, the transform $\hat{T}$ is based on a convolution operation with the watermark and the inverse transform $\hat{T}^{-1}$ on a correlation. Thus, if $W_{i,j}$ denotes the 'watermark image' then

$$J_{i,j} = \hat{T}[W_{i,j}] + rI_{i,j}$$

where r is the 'Image-to-Watermark Ratio' and where both arrays are taken to be positive, real and normalised. The transform can be based on the application of any Point Spread Function (stochastic or otherwise) that is a phase only function since in Fourier space (using the convolution theorem and using a 'tilde' to denote the Discrete Fourier transform - DFT)

$$\widetilde{J}_{i,j} = \exp[-z\theta(i,j)]\widetilde{W}_{i,j} + r\widetilde{I}_{i,j}$$

where $z \equiv 0 + \sqrt{-1}$ and $\theta(i,j)$ is the phase spectrum, recovery of the watermark being based on the result

$$\widetilde{W}(i,j) = \exp[z\theta(i,j)][\widetilde{J}_{i,j} - r\widetilde{I}_{i,j}] \sim \exp[z\theta(i,j)]\widetilde{J}_{i,j}$$

given that $\hat{T}^{-1}I(i,j) \sim 0$. This approach can be used to embed a significant amount of image information content suitable for image self-authentication, for example, or on a block-by-block basis to embed less information but with greater resilience to an attack. In view of this approach, the method reported in this paper uses the DCT rather than the discrete Fourier transform. While the DCT does not provide the same phase only function option for watermarking an image (because the output of the DCT is real only) it does provide similar options within the context of 'frequency space modification' in a way that is compatible with standard image compression methods.

3. Block Embedding Based Watermarking

One of the principal methods for developing robust, as opposed to fragile watermarking algorithms, is to apply a block embedding technique. This is because pixel-by-pixel embedding can be affected by virtually any digital and optical image distortion. To overcome this problem some regions (blocks) of an image should be used for embedding watermark 'symbols' which, in practice, are numerical values (binary, integer or both) that code the information to be embedded. The idea of block embedding lies in splitting the image into a number of blocks, and embedding hidden text symbols into each block separately. The blocks may, in principle, be irregular, but block regularity is the norm. To extract the watermark from the image, it is processed and analysed blockwise. Each block of the image can have a limited number of permitted states and during application of the watermark extraction process, each block is analysed with regard to its proximity to a defined state, the most likely state then being accepted as one of the extracted symbols as illustrated in Figure 1.

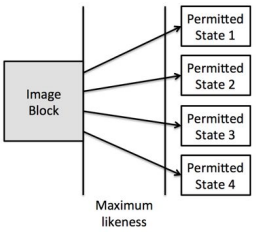

Figure 1: *During the extraction of a watermark, each image block is analysed with regard to its proximity to four permitted states. The maximum likeness criterion is used to determine the 'closest' state.*

Block embedding can yield a high level of robustness and can cope with a modification to **any** pixel in an image block as well as with some types of distortion or 'attacks' that are common to optical image transmission. These include the following:

- image re-sampling and blur (typically a Gaussian blur);
- barrel/pincushion and perspective distortion;
- tone curve modification.

These properties allow us to consider not only digital image distortion but also natural optical image deformation. The watermark, which is robust to these deformations, can then be transmitted as an embedded codec in the host image through an optical channel. However, in order to enhance the resilience of a watermark to the above, the quantity of information that can be used in the watermark is reduced. A number of diverse block modification techniques can be developed including those briefly discussed in Section 2, for example, but in this paper we focus on DCT coefficient mod-

ification which can be viewed in terms of a pattern addition process.

3.1. DCT Coefficient Embedding Algorithms

The DCT produces a set of real coefficients that, on a block-by-block basis can be modified to embed the watermark data. In this section, we provide an overview of the algorithm developed for this purpose. The algorithm has been designed with a specific focus on optimising performance in terms of robustness to e-display-to-scan distortions where the (watermarked) image is captured using a low resolution mobile phone camera, for example. Compared to the application of the DTC for e-to-e watermarking scheme, this requires that the watermark is particularly robust to distortions of noise and blur which are discussed later in the paper. The algorithm developed assumes, by default, the use of full 24-bit colour images which provides greater 'colour space' for the watermarking procedure than a grey level image and is used as part of the embedding process.

3.1.1. Outline of the Watermark Embedding Algorithm

1. The host or container image I_c is converted from RGB to YCbCr colour mode. Only colour channels C_b and C_r are modified during the embedding processes. This is because embedding in a brightness channel is more noticeable thereby requiring smaller amplitudes perturbations.
2. Each colour channel is split into number of regular blocks of pixels B_k^B (blue) and B_k^R (Red), $k = 1,2,...,L$, each block being taken to be a matrix of pixel values:
$$B = \left[b_{i,j}\right], i = 1,2,...,M, j = 1,2,...,N$$
The dimensions of each block (M and N) are chosen to keep the block shape as close to a square as possible.
3. The embedding data h is protected with an error correction code, resulting in data extension:
$$\mathbf{h}'_t,\ t = 1,2,...,2L$$
4. The two-dimensional Discrete Cosine Transform (DCT) is performed on each block:
$$X_{m,n} = \sum_{i=0}^{M-1}\sum_{j=0}^{N-1} b_{i,j}\cos\left[\tfrac{\pi}{M}\left(i+\tfrac{1}{2}\right)m\right]\cos\left[\tfrac{\pi}{N}\left(j+\tfrac{1}{2}\right)m\right],$$
where $X_{m,n}$ are the DCT spectrum components of block B_k, $m = 1,2,...,M, n = 1,2,...,N$.
5. DCT components of a block are then modified according to one of a number of possible patterns and, for simplicity, the system design for two embedding patterns P_0 and P_1 is described. Each pattern replaces some of the DCT components with exact values and represents one bit of the embedded data $\mathbf{h}'_t$. For example:
$$P_0 : \left[X_{4,6} = 0, X_{6,4} = -A, X_{10,8} = 0, X_{8,10} = A\right]$$
$$P_1 : \left[X_{4,6} = A, X_{6,4} = 0, X_{10,8} = -A, X_{8,10} = 0\right],$$
where A is the amplitude of the spectral perturbation whose specific value affects the watermark visibility and system robustness characteristics. The choice of the exact embedding patterns has great significance on the robustness and visibility of the watermark. The patterns are chosen in a way that makes the system robust to carrier image modification which is addressed later on in this paper.
6. The two-dimensional Inverse Discrete Cosine Transform (IDCT) is performed on the perturbed spectrum $X'_{m,n}$:
$$B' = \left[b'_{i,j}\right] = \mathrm{IDCT}\left(X'_{m,n}\right)$$
7. The modified blocks B'_k are concatenated in the same manner as in the initial image forming new colour channels C'_b and C'_r and these (modified) channels combined with the intact lightness channel to produce the resulting watermarked image I'_c which is converted back to RGB colour space.
8. The watermarked image is saved in one of a number of image storage formats, being insensitive to image compression settings with the exception of *lowest quality* compression in lossy formats, such as JPEG. The watermarked image can then be printed or displayed on a monitor for application of the extraction process which is described in the following section.

3.1.2. Outline of the Watermark Extraction Algorithm

1. The watermarked image I'_c, displayed on a monitor or printed on paper, is captured on a digital camera where the average phone camera quality is taken to be generally sufficient for extraction, the critical capturing distance and orientation depending on a number of parameters, including the embedding amplitude A, embedding patterns P, image size and number of blocks L.
2. The image is aligned and cropped by any accessible means to match the original image as discussed in Section 3.1.1.
3. Conversion to YCbCr colour mode is performed with only the colour channels C_b and C_r being analysed.
4. Each channel is split into blocks B_k as used in the embedding procedure discussed in the Section 3.1.1.
5. The Discrete Cosine Transform is performed for each block:
$$\mathrm{X} = [X_{m,n}] = \mathrm{DCT}\left(\mathrm{B}_k\right)$$
6. The spectrum of each block is then evaluated to detect the presence of each pattern. The most likely identifying pattern in each block yields one bit of the embedded data and for the embedding patterns discussed in Section 3.1.1, each embedded bit is determined by:
$$\mathbf{h}'_t = \begin{cases} 0 & \text{if } (X_{8,10} - X_{6,4}) > (X_{4,6} - X_{10,8}), \\ 1 & \text{otherwise.} \end{cases}$$
7. The Recovered data $\mathbf{h}$ is then obtained from $\mathbf{h}'$, using an error correction code.

In the following section, the principal results associated with a series of optical and numerical experiments are provided that yield a quantitative assessment of the algorithms in terms of the resilience of the watermark data to a range of attacks.

4. Evaluation of the DCT Embedding Algorithm

We consider a container image I_c shown in Figure 2 which is a full 24-bit colour image and has a size of 500×500 pixels and where its colour channels C_b and C_r are split into $k = 11 \times 12 = 132$ blocks each, the size of each block being B_k is 40×44 pixels.

Figure 2 also shows a typical example of a screen shot obtained using a mobile phone camera for the watermarked image displayed on an LCD exhibiting Moire fringes.

Figure 2: *Container image used for evaluation of the DCT embedding algorithms (left) and an example of a watermarked image obtained from an LCD screen using a mobile phone camera (right).*

The embedding data **h** consists of 71 bits and after application of error-correcting code BCH(255,71) the length of coded data is 255 bits [MS77]. This code is capable of correcting up to 30 bit errors and more up-to-date codes such as LDPC can be used to boost system efficiency. Taking each block to carry one bit, the total number of available embedding bits is $2L = 264$. However, since $264 - 255 = 9$, there are nine extra blocks in the lower right hand corner of the image which are not affected by the watermarking procedure, five of these blocks belonging to C_b and four to the C_r channel. On this basis, we consider the resilience of the algorithms presented in Section 3.1.1 and Section 3.1.2 to the 'attacks' discussed in the following sections.

4.1. Robustness to Additive Noise

As long as the system uses Forward Error Correction, the Bit Error Rate is not an optimal parameter for performance evaluation. The system is designed to be bit-error free and so an evaluation is focused on a relationship which connects error robustness with watermark intensity, given that the watermark is extracted properly. The robustness of the system to noise is highly dependent on the embedding rate R which relates the spectral perturbation intensity to the original spectrum intensity. The noise intensity is expressed in terms of the percentage of image intensity with measurements being performed in the following manner: (i) the embedding rate R is fixed; (ii) the noise intensity is raised until error correction fails; (iii) the most intensive noise, allowing errorless extraction, is taken as a 'reference marker'. The result is shown in Figure 3 which includes an example of the most intensive case of additive Gaussian noise that does not affect the watermark data.

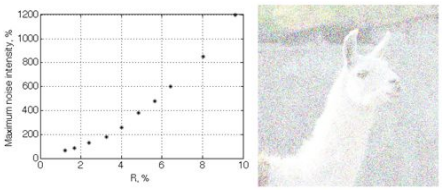

Figure 3: *Watermark noise robustness for different embedding rates R (left) and an example of a high noise rate corresponding to a case which does not affect the watermark data.*

4.2. Robustness to a Gaussian Blur

Robustness to image blurring depends on the particular set of DCT-coefficients that are used in the embedding patterns. If the radius of a Gaussian blur, for example, is less than the scale of embedded detail, then the blur does not distort the watermark providing extraction is good. However, when the radius is equal or larger than the scale of embedded detail this detail is dissipated in the blur and extraction becomes impossible. A Gaussian blur with a pixel radius up to and including 12 allows for proper watermark extraction but beyond this threshold the blur erases the watermark. However, this effect does not depend on the embedding rate R.

4.3. Robustness to Image Shift

Shift robustness also depends on the specific embedding coefficients. However, if the embedding patterns use the same set of embedding frequencies (which is optimal for noise robustness) then the spatial pattern P^s appears similar to it's counter-pattern shifted in some direction as illustrated in Figure 4. While a 3 pixel shift is easily recovered, a 4 pixel shift, either vertically of horizontally, prevents successful watermark recovery, regardless of the embedding rate.

4.4. Robustness to 'Barrel' and Rotational Distortions

Geometric image distortions such as barrel, pincushion and rotational distortions are tightly connected with image resampling and optical image deformation. These distortions need to be corrected in an image alignment procedure and the results discussed in this section are devoted to illustrating the systems reaction to improper alignment. Watermark

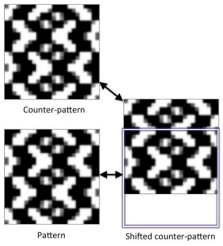

Figure 4: *Illustration of a shifted pattern which can be erroneously recovered as a counter-pattern.*

recovery is not disrupted by re-sampling and a major problem with barrel/rotation distortions is the displacement of edge embedding blocks which appear shifted with regard to the recovery procedure. Neither barrel or rotational distortions depend upon the embedding rate R and a marginal barrel parameter such as $3.0 \cdot 10^{-5}$ and a rotation of less than $\pm 0.85^{\circ}$ does not affect accurate watermark extraction. However, these results depend significantly upon the container image and embedding block sizes.

4.5. Robustness to Partial Removal of Image Data

The partial removal of an entire section of the watermarked image will clearly lead to complete corruption of the watermark data in the same section. However, it is important to evaluated the effect of this on watermark extraction over the rest of the image. Figure 5 clearly illustrates that the effect of removing data from a portion of the image (in this example, the lower left-hand corner of the image) does not affect the remaining portion of the image with regard to watermark extraction whose performance characteristics are the same with regard to the robustness criteria discussed in the previous sections.

Figure 5: *Example of the bit-errors generated in both the Red and Blue channels (right) by the partial removal of a portion of the watermarked image as shown (left). The rest of the image on the right-hand-side is white indicating that there are no bit-errors in the remaining portion of the watermark after extraction from the spoiled image. This is due to the BCH error correcting code that is applied which easily compensates for the data corruption shown, the remainder of the watermark in the image being extracted without bit errors.*

5. Alignment Issues

An error-less extraction of embedded data relies on proper image alignment, and, in this section we discuss a novel method for aligning the image using the same watermark data. The idea is to use the watermark to align the image before final extraction of the watermark itself. If the container image I_c is known, an alignment procedure via the image contents can be performed. However this approach introduces additional limitations on the watermarking system itself. A common solution to this problem lies in the addition of special alignment markers on the image which allow for the automatic alignment. These markers can flag the fact that a watermark maybe present in the image thereby initiating a potentially successful attack. However, using the approach described here, the system does not need any additional markers. This is because the presence of embedding patterns in the image blocks' yields a DCT spectrum that, in effect, provides a set of hidden markers located at the centre of each block. This idea is compounded in the following procedure:

1. The embedding block patterns are extracted in image space. We start with an empty spectrum X^0 given by

$$\mathrm{X}^0 = \left[X^0_{m,n}\right] = 0$$

   The embedding pattern P is added to X^0 and the two dimensional IDCT is performed and repeated for all embedding patterns P_v, $v = 0, 1, ..., V-1$. Although the total number of patterns used in the results reported here is $V = 2$, the system can use a larger number of embedding patterns at the cost of lower robustness but increased capacity. The spatial embedding patterns

$$P^s_v = \mathrm{IDCT}(\mathrm{X}^0 + P_v)$$

   are rectangular image blocks which indicate the presence of spectral patterns P_v in the block spectrum.
2. For each of the colour channels of the input watermarked image C_b and C_r a cross-correlated is performed with each of the embedding patterns P_v where, in the output $\Theta = [\theta_{x,y}]$, negative values are replaced by zeros:

$$(\theta_v)_{x,y} = \begin{cases} (C_r \star\star P^s_v)_{x,y} & \text{if } (C_r \star\star P^s_v)_{x,y} > 0, \\ 0 \text{ otherwise.} \end{cases}$$

   where $\star\star$ denoted the two-dimensional cross-correlation operation. All the results for a particular colour channel are combined additively, i.e.

$$\Theta = \sum_{v=0}^{V-1} \Theta_v$$

3. The correlation results for both colour channels are also added together, i.e. $\Theta = \Theta_b + \Theta_r$. The Θ matrix has the same size as the Container Image and consists of multiple cross-correlations. Each of these results have a pronounced peak in the correlation surface which locates the

centre of each embedding block. A typical example of the output is shown on a Figure 6.

Using this procedure, coupled with some 'intelligent filtering' applied to Θ, the correlation peaks can be used as markers for the automatic image alignment and thus realignment of an image, realignment being undertaken through application of the Radon transform, for example [Bla02].

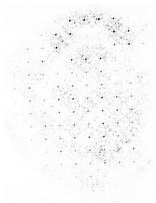

Figure 6: *Example of the peaks (regular points) generated in the correlation surface that identify the blocks associated with the presence of the watermark data.*

5.1. Conclusions

The DCT coefficient embedding algorithm presented in this paper depends (as with all algorithms) on the specific embedding pattern used and other algorithmic parameters. However, in the context of our focus on using a DCT based approach to produce a highly resilient watermarking method, we may conclude with some common conceptual strengths and weaknesses. The strengths/weaknesses listed below are primarily concerned with the watermark robustness characteristics and do not relate to watermark capacity or visibility factors. Strengths: (i) robustness to additive noise (with a proper set of embedded patterns) and robustness to image re-sampling; (ii) flexible visibility and robustness characteristics through choice of different patterns and robustness to scaling (within certain limits). Weaknesses: (i) sensitivity to image shifting; (ii) sensitive to image blur (especially if the patterns include high-frequency coefficients). The sensitivity to shift is one of the principal problems associated with application of the DCT in general. Though patterns can be isolated, that have different spatial frequencies, noise robustness requires that a counter-pattern should be as close as possible to an intensity-inverted initial pattern. But due to the periodic nature of DCT-component patterns, shifted patterns can be easily recovered as counter-patterns, see Figure 4. However, subject to the weakness listed above, the algorithm presented in this paper does provide a DCT based watermarking method that is practically applicable to print/e-display to e-scan detection that is inclusive of (marker-independent) automatic alignment. To the best of the authors knowledge, this is the first DCT-based algorithm of its type that can be used in this way.

References

[AP98] ANDERSON R. J., PETITCOLAS F.: On the limits of steganography. *IEEE: Selected Areas in Communications 16*, 1 (May 1998), 474–481. 2

[BAR11a] BLACKLEDGE J. M., AL-RAWI A. R.: Application of stochastic diffusion for hiding high fidelity encrypted images. *ISAST Trans. On Computing and Intelligent Systems 3*, 1 (2011), 24–33. 4

[BAR11b] BLACKLEDGE J. M., AL-RAWI A. R.: Steganography using stochastic diffusion for the covert communication of digital images. *IANEG International Journal of Applied Mathematics 41*, 4 (2011), 270–298. 4

[BAR13] BLACKLEDGE J. M., AL-RAWI A. R.: Image authentication using stochastic diffusion. In *Proc. UKSIM2013* (2013), vol. 15, pp. 437–442. 4

[BI13] BLACKLEDGE J. M., IAKOVENKO O.: On the application of two-dimensional chirplets for resilient digital image watermarking. In *Proc. ISSC2013* (2013), vol. 24, pp. 1–8. 4

[Bla02] BLACKLLEDGE J. M.: *Cryptography and Steganography: New Algorithms and Applications*. Centre for Advanced Studies Textbooks, Warsaw University of Technology, 2002. 1, 3, 8

[Bla05] BLACKLLEDGE J. M.: *Digital Image Processing: Mathematical and Computational Methods*. Woodhead Publishing Series in Optical and Electronic Materials, 2005. 4

[Bla08] BLACKLEDGE J. M.: Multi-algorithmic cryptography using deterministic chaos with application to mobile communications. *ISAST Trans. on Electronics and Signal Processing 1*, 2 (2008), 23–64. 3

[CMB02] COX I. J., MILLER M., BLOOM J.: *Digital Watermarking*. Morgan-Kaufmann, 2002. 2

[HW99] HSU C. T., WU J. L.: Hidden digital watermarks in images. *Transactions of Image Processing 8*, 1 (1999), 58–68. 2

[LW10] LIU H., WANG X.: Color image encryption based on one-time keys and robust chaotic maps. *Computers and Mathematics with Applications 59*, 10 (2010), 3320–3327. 3

[MM97] MINTZER F. LOTSPIECH J., MORIMOTO N.: Safeguarding digital library contents and users. *D-Lib Magazine* (December 1997). 2

[MS77] MACWILLIAMS F. J., SLOANE N. J. A.: *The Theory of Error-Correcting Codes*. North-Holland Publishing Company, 1977. 6

[PK99] PETITCOLAS F., KUHN M.: Information hiding: A survey. *IEEE Special Issue on the Protection of Multimedia Content 87*, 7 (July 1999), 1062–1077. 2

[She00] SHEN J.: On wavelet fundamental solutions to the heat equation - heatlets. *Journal of Differential Equations 161*, 1 (2000), 403–421. 4

[SZ06] SITU G., ZHANG J.: Double random-phase encoding in the fresnel domain. *Optics Letters 29*, 14 (2006), 1584–1586. 4

[Tsa06] TSAUR G.: Constructing green functions of the schrödinger equation by elementary transforms. *American Journal of Physics 74*, 7 (2006), 600–606. 4

[YK10] YOON J. W., KIM H.: Multi-algorithmic cryptography using deterministic chaos with application to mobile communications. *Communications in Nonlinear Science and Numerical Simulation 15*, 12 (2010), 3998–4006. 3