International Journal of Computing and Business Research (IJCBR)

ISSN (Online) : 2229-6166

Volume 4 Issue 2 May 2013

THE PRAGMATIC REVIEW ON WATERMARKING TECHNIQUES IN DIGITAL IMAGE PROCESSING

Neha Garg

M. Tech. (CSE)

University College of Engineering

Punjabi University, Patiala, Punjab, India

Brahmaleen K. Sidhu

Assistant Professor

University College of Engineering

Punjabi University, Patiala, Punjab, India

ABSTRACT

International Journal of Computing and Business Research (IJCBR)

ISSN (Online) : 2229-6166

Volume 4 Issue 2 May 2013

A digital watermark is a digital signal or pattern inserted into a digital image. Since this signal or pattern is present in each unaltered copy of the original image, the digital watermark may also serve as a digital signature for the copies. A given watermark may be unique to each copy (e.g. to identify the intended recipient), or be common to multiple copies (e.g. to identify the document source). In either case, the watermarking of the document involves the transformation of the original into another form. This distinguishes digital watermarking from digital fingerprinting, where the original file remains intact and a new created file 'describes' the original file's content. Digital watermarking is also to be contrasted with public-key encryption, which also transform original files into another form. It is a common practice nowadays to encrypt digital documents so that they become un-viewable without the decryption key. Unlike encryption, however, digital watermarking leaves the original image (or file) basically intact and recognizable. In addition, digital watermarks, as signatures, may not be validated without special software. Further, decrypted documents are free of any residual effects of encryption, whereas digital watermarks are designed to be persistent in viewing, printing, or subsequent re-transmission or dissemination.

Keywords – Digital Image Processing, Watermarking, Image Watermarking

INTRODUCTION

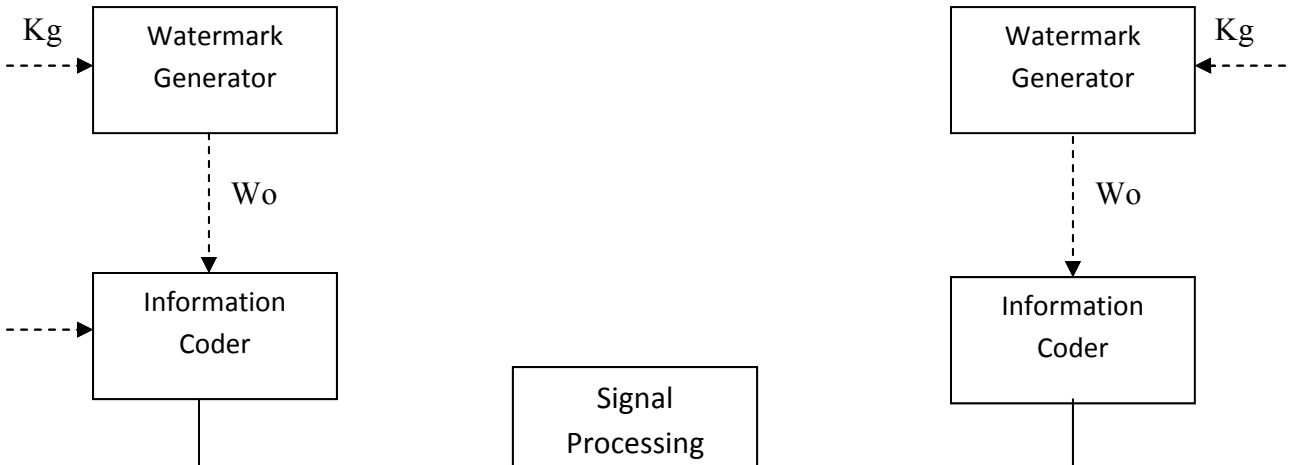
A watermarking system can be viewed as a communication system consisting of three main elements: an embedder, a communication channel and a detector. Watermark information is embedded into the signal itself, instead of being placed in the header of a file or using encryption like in other security techniques, in such a way that it is extractable by the detector. To be more specific, the watermark information is embedded within the host signal before the watermarked

signal is transmitted over the communication channel, so that the watermark can be detected at the receiving end, that is, at the detector.

A general watermarking system is illustrated in Fig. 1. The dotted lines represent the optional components, which may or may not be required according to the application. First of all, a watermark Wo is generated by the watermark generator possibly with a secret watermark generation key Kg. The watermark Wo can be a logo, or be a pseudo-random signal.

Instead of directly embedding it into the host signal, the watermark Wo can be pre-coded to optimize the embedding process, i.e. to increase robustness against possible signal processing operations or imperceptibility of the watermark. This is done by an information coder which may require the original signal So.

The outcome of the information coding component is denoted by symbol W that, together with the original signal So and possibly a secret key K, are taken as input of the embedder. The secret key K is intended to differentiate between authorized users and unauthorized users at the detector in the absence of Kg. The embedder takes in W, So and K, so as to hide W within So in a most imperceptible way with the help of K, and produce the watermarked signal Sw. Afterwards, Sw enters into the communication channel where a series of unknown signal processing operations and attacks may take place. The outcome of the communication channel is denoted by the symbol S´w.



International Journal of Computing and Business Research (IJCBR)

ISSN (Online) : 2229-6166

Volume 4 Issue 2 May 2013

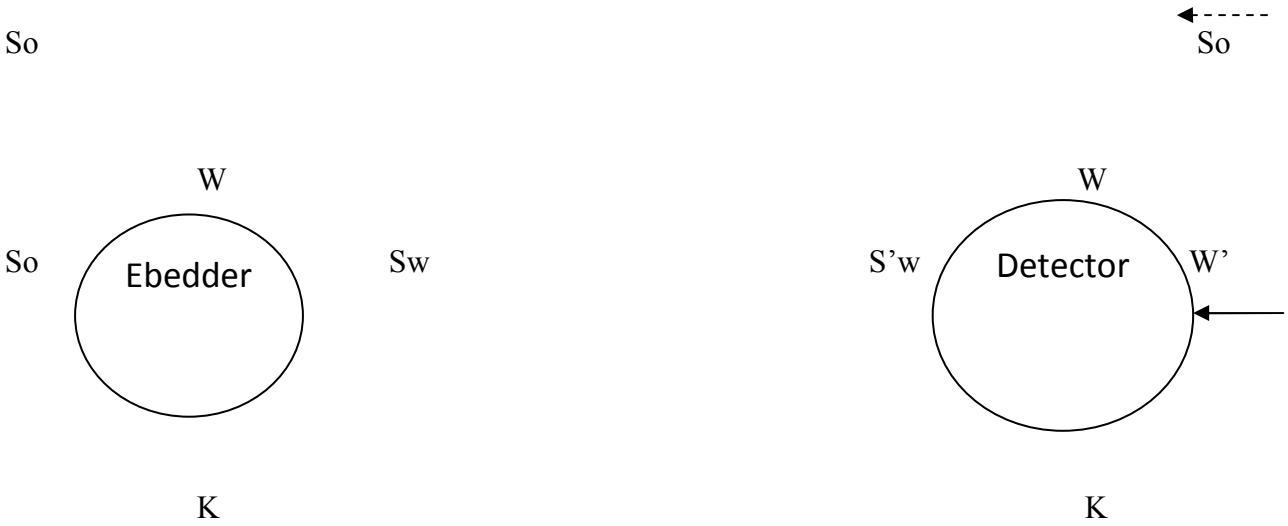


Figure 1 A general watermarking system

At the receiving end, the detector works in an inversely similar way as the embedder, and it may require the secret key Kg, K, and the original signal So. Then the detector reads S´w and decides if the received signal has the legal watermark.

TYPES OF DIGITAL WATERMARKS

Watermarks and watermarking techniques can be divided into various categories in various ways. Watermarking techniques can be divided into four categories according to the type of document to be watermarked as follows: [1]

- Text Watermarking
- Image Watermarking

- Audio Watermarking
- Video Watermarking

In other way, the digital watermarks can be divided into three different types as follows: [1,2]

- Visible watermark
- Invisible-Robust watermark
- Invisible-Fragile watermark

Visible watermark is a secondary translucent overlaid into the primary image. The watermark appears visible to a casual viewer on a careful inspection. The invisible-robust watermark is embedded in such a way that alternations made to the pixel value are perceptually not noticed and it can be recovered only with appropriate decoding mechanism. The invisible-fragile watermark is embedded in such a way that any manipulation or modification of the image would alter or destroy the watermark.

Also, the digital watermarks can be divided into two different types according to the necessary data for extraction:

- Informed (or private Watermarking): in which the original unwatermarked cover is required to perform the extraction process.
- Blind (or public Watermarking): in which the original unwatermarked cover is not required to perform the extraction process.

WATERMARKING IN THE FREQUENCY DOMAIN

In order to understand the advantages of a frequency-based method, it is instructive to examine the processing stages that an image (or sound) may undergo in the process of copying, and to study the effect that these stages could have on the data. Transmission refers to the application of

any source or channel code, and/or standard encryption technique to the data. While most of these steps are information lossless, many compression schemes (JPEG, MPEG etc.) are lossy, and can potentially degrade the data's quality, through irretrievable loss of information. In general, a watermarking scheme should be resilient to the distortions introduced by such algorithms.

Lossy compression is an operation that usually eliminates perceptually non-salient components of an image or sound. Most processing of this sort takes place in the frequency domain. In fact, data loss usually occurs among the high frequency components.

After receipt, an image may endure many common transformations that are broadly categorized as geometric distortions or signal distortions. Geometric distortions are specific to images and video, and include such operations as rotation, translation, scaling and cropping. By manually determining a minimum of four or nine corresponding points between the original and the distorted watermark, it is possible to remove any two or three dimensional affine transformation [Fau93]. However, an affine scaling (shrinking) of the image leads to a loss of data in the high frequency spectral regions of the image. Cropping, or the cutting out and removal of portions of an image, leads to irretrievable loss of image data, which may seriously degrade any spatially based watermark such as [Car95]. However, a frequency-based scheme spreads the watermark over the whole spatial extent of the image, and is therefore less likely to be affecected by cropping.

Common signal distortions include digital-to-analog and analog-to-digital conversion, resampling, re-quantization, including dithering and recompression, and common signal enhancements to image contrast and/or color, and audio frequency equalization. Many of these distortions are non-linear, and it is difficult to analyze their effect in either a spatial or frequency based method. However, the fact that the original image is known allows many signal transformations to be undone, at least approximately. For example, histogram equalization, a

common non-linear contrast enhancement method, may be removed substantially by histogram specication [GW93] or dynamic histogram warping [CRH95] techniques.

Finally, the copied image may not remain in digital form. Instead, it is likely to be printed, or an analog recording made (for instance, onto analog audio or video tape). These reproductions introduce additional degradation into the image that a watermarking scheme must be robust to.

The watermark must not only be resistant to the inadvertent application of the aforementioned distortions. It must also be immune to intentional manipulation by malicious parties. These manipulations can include combinations of the above distortions, and can also include collusion and forgery attacks.

SPREAD SPECTRUM CODING OF A WATERMARK

The above discussion illustrates that the watermark should not be placed in perceptually insignificant regions of the image (or its spectrum) since many common signal and geometric processes affect these components. For example, a watermark placed in the high frequency spectrum of an image can be easily eliminated with little degradation to the image by any process that directly or indirectly performs low pass filtering.

The problem then becomes how to insert a watermark into the most perceptually significant regions of the spectrum in a fidelity preserving fashion. Clearly, any spectral coefficient may be altered, provided such modification is small. However, very small changes are very susceptible to noise.

To solve this problem, the frequency domain of the image or sound at hand is viewed as a communication channel, and correspondingly, the watermark is viewed as a signal that is transmitted through it. Attacks and unintentional signal distortions are thus treated as noise that

the immersed signal must be immune to. While we use this methodology to hide watermarks in data, the same rationale can be applied to sending any type of message through media data.

We originally conceived our approach by analogy to spread spectrum communications [PSM82]. In spread spectrum communications, one transmits a narrowband signal over a much larger bandwidth such that the signal energy present in any single frequency is undetectable. Similarly, the watermark is spread over very many frequency bins so that the energy in any one bin is very small and certainly undetectable. Nevertheless, because the watermark verification process knows the location and content of the watermark, it is possible to concentrate these many weak signals into a single output with high signal-to-noise ratio. However, to destroy such a watermark would require noise of high amplitude to be added to all frequency bins.

Spreading the watermark throughout the spectrum of an image ensures a large measure of security against unintentional or intentional attack: First, the location of the watermark is not obvious. Furthermore, frequency regions should be selected in a fashion that ensures severe degradation of the original data following any attack on the watermark.

A watermark that is well placed in the frequency domain of an image or a sound track will be practically impossible to see or hear. This will always be the case if the energy in the watermark is sufficiently small in any single frequency coefficient. Moreover, it is possible to increase the energy present in particular frequencies by exploiting knowledge of masking phenomena in the human auditory and visual systems. Perceptual masking refers to any situation where information in certain regions of an image or a sound is occluded by perceptually more prominent information in another part of the scene. In digital waveform coding, this frequency domain (and, in some cases, time/pixel domain) masking is exploited extensively to achieve low bit rate encoding of data [JJS93, GG92]. It is known that both the auditory and visual systems attach more resolution to the high energy, low frequency, spectral regions of an auditory or

visual scene [JJS93]. Further, spectrum analysis of images and sounds reveals that most of the information in such data is located in the low frequency regions.

Upon applying a frequency transformation to the data, a perceptual mask is computed that highlights perceptually significant regions in the spectrum that can support the watermark without affecting perceptual fidelity. The precise magnitude of each modification is only known to the owner. By contrast, an attacker may only have knowledge of the possible range of modification. To be confident of eliminating a watermark, an attacker must assume that each modification was at the limit of this range, despite the fact that few such modifications are typically this large. As a result, an attack creates visible (or audible) defects in the data. Similarly, unintentional signal distortions due to compression or image manipulation, must leave the perceptually significant spectral components intact, otherwise the resulting image will be severely degraded. This is why the watermark is robust.

In practice, in order to place a length n watermark into an N xN image, we computed the N xN DCT of the image and placed the watermark into the *n* highest magnitude coefficients of the transform matrix, excluding the DC component.[4] For most images, these coefficients will be the ones corresponding to the low frequencies.

STRUCTURE OF THE WATERMARK

We now give a high-level overview of our a basic watermarking scheme; many variations are possible. In its most basic implementation, a watermark consists of a sequence of real numbers X = x_1; : : : ; x_n. In practice, we create a watermark where each value xi is chosen independently according to N(0; 1) (where N(μ; σ^2) denotes a normal distribution with mean μ and variance

International Journal of Computing and Business Research (IJCBR)

ISSN (Online) : 2229-6166

Volume 4 Issue 2 May 2013

σ^2). We assume that numbers are represented by a reasonable but finite precision and ignore these insignificant roundoff errors. This procedure exploits the fact that each component of the watermark is chosen from a normal distribution. Alternative distributions are possible, including choosing xi uniformly from {1;-1}, {0; 1} or [0; 1].

DESCRIPTION OF THE WATERMARKING PROCEDURE

We extract from each document D a sequence of values V = v_1…..v_n, into which we insert a watermark X = x1; : : : ; xn to obtain an adjusted sequence of values V` = v`$_{1.....}$ v`$_n$. V` is then inserted back into the document in place of V to obtain a watermarked document D`. One or more attackers may then alter D`, producing a new document D*. Given D and D*, a possibly corrupted watermark X$^{\perp}$ is extracted and is compared to X for statistical significance. We extract X* by first extracting a set of values V* = v*$_{1.....}$ v*$_n$ from D* (using information about D) and then generating X* from V * and V.

INSERTING AND EXTRACTING THE WATERMARK

When we insert X into V to obtain V` we specify a scaling parameter which determines the extent to which X alters V . Three natural formulae for computing V` are:

$v` = v_i + ax_i$ *(i)*

$v` = v_i (1 + ax_i)$ *(ii)*

$v`_I = v_i(e^{axi})$ *(iii)*

Equation 1 is always invertible, and Equations 2 and 3 are invertible if v_i 6 ≠ 0, which holds in all of our experiments. Given *V** we can therefore compute the inverse function to derive X$^{\perp}$ from *V** and *V*.

International Journal of Computing and Business Research (IJCBR)

ISSN (Online) : 2229-6166

Volume 4 Issue 2 May 2013

Equation 1 may not be appropriate when the v_i values vary widely. If v_i = 106 then adding 100 may be insufficient for establishing a mark, but if v_i = 10 adding 100 will distort this value unacceptably. Insertion based on Equations 2 or 3 are more robust against such differences in scale. We note that Equations 2 and 3 give similar results when xi is small. Also, when v_i is positive then Equation 3 is equivalent to $\lg(v`_i) = \lg(v_i) + x_i$, and may be viewed as an application of Equation 1 to the case where the logarithms of the original values are used.

DETERMINING MULTIPLE SCALING PARAMETERS

A single scaling parameter may not be applicable for perturbing all of the values vi, since different spectral components may exhibit more or less tolerance to modification. More generally one can have multiple scaling parameters $\alpha_1 \ldots\ldots \alpha_n$ and use update rules such as $v`_I = v_i(1+\alpha_i x_i)$. We can view *i* as a relative measure of how much one must alter vi to alter the perceptual quality of the document. A large *i* means that one can perceptually \get away" with altering vi by a large factor without degrading the document. There remains the problem of selecting the multiple scaling values. In some cases, the choice of i may be based on some general assumption. For example, Equation 2 is a special case of the generalized Equation 1($v`_i = v_i + \alpha_i x_i$), for $\alpha_i = \alpha v_i$. Essentially, Equation 2 makes the reasonable assumption that a large value is less sensitive to additive alterations than a small value.

In general, one may have little idea of how sensitive the image is to various values. One way of empirically estimating these sensitivities is to determine the distortion caused by a number of attacks on the original image. For example, one might compute a degraded image $D^{\llcorner}$ from D, extract the corresponding values $v^*_1 \ldots\ldots\ldots v^*_n$ and choose i to be proportional to the deviation $|v^*_I - v_i|$. For greater robustness, one should try many forms of distortion and make i proportional to the average value of $|v^*_i - v_{ij}|$. As alternatives to taking the average deviation one might also take the median or maximum deviation.

International Journal of Computing and Business Research (IJCBR)

ISSN (Online) : 2229-6166

Volume 4 Issue 2 May 2013

One may combine this empirical approach with general global assumptions about the sensitivity of the values. For example, one might require that $\alpha_i \geq \alpha_j$ whenever $v_i \geq v_j$. One way to combine this constraint with the empirical approach would be to set *i* according to

$\alpha_i \sim \max |v^*_j - v_j|$.

A still more sophisticated approach would be to weaken the monotonicity constraint to be robust against occasional outliers.

In all our experiments we simply use Equation 2 with a single parameter $\alpha = 0{:}1$. When we computed JPEG-based distortions of the original image we observed that the higher energy frequency components were not altered proportional to their magnitude (the implicit assumption of Equation 2). We suspect that we could make a less obtrusive mark of equal strength by attenuating our alterations of the high-energy components and amplifying our alterations of the lower-energy components. However, we have not yet performed this experiment.

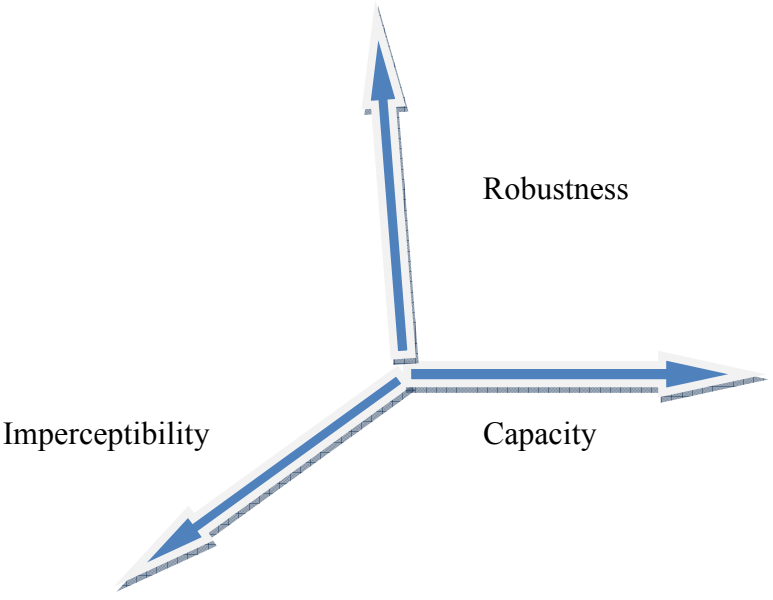
PURPOSE OF WATERMARKING

Security: The security requirement of a watermarking system can differ slightly depending on the application. Watermarking security implies that the watermark should be difficult to remove or alter without damaging the host signal. As all watermarking systems seek to protect watermark information, without loss of generality, watermarking security can be regarded as the ability to assure secrecy and integrity of the watermark information, and resist malicious attacks [4].

- **Imperceptibility:** The imperceptibility refers to the perceptual transparency of the watermark. Ideally, no perceptible difference between the watermarked and original signal should exist [5]. A straightforward way to reduce distortion during watermarking process is embedding the watermark into the perceptually insignificant portion of the host

signal [6]. However, this makes it easy for an attacker to alter the watermark information without being noticed.

- **Capacity:** Watermarking capacity normally refers to the amount of information that can be embedded into a host signal. Generally speaking, capacity requirement always struggle against two other important requirements, that is, imperceptibility and robustness (Fig. 6). A higher capacity is usually obtained at the expense of either robustness strength or imperceptibility, or both.



International Journal of Computing and Business Research (IJCBR)

ISSN (Online) : 2229-6166

Volume 4 Issue 2 May 2013

Figure 2 : The tradeoffs among imperceptibility, Robustness, and capacity

- **Robustness:** Watermark robustness accounts for the capability of the watermark to survive signal manipulations. Apart from malicious attacks, common signal processing operations can pose a threat to the detection of watermark, thus making it desirable to design a watermark that can survive those operations. For example, a good strategy to robustly embed a watermark into an image is to insert it into perceptually significant parts of the image. Therefore, robustness is guaranteed when we consider the case of lossy compression which usually discards perceptually insignificant data, thus data hidden in perceptual significant portions is likely to survive lossy compression operation. However, as this portion of the host signal is more sensitive to alterations, watermarking may produce visible distortions in the host signal. The exact level of robustness an algorithm must possess cannot be specified without considering the application scenario [7]. Not all watermarking applications require a watermark to be robust enough to survive all attacks and signal processing operations. Indeed, a watermark needs only to survive the attacks and those signal processing operations that are likely to occur during the period when the watermarked signal is in communication channel. In an extreme case, robustness may be completely irrelevant in some case where fragility is desirable.

WATERMARKING TECHNIQUES

Several different methods enable watermarking in the spatial domain. The simplest (too simple for many applications) is just to flip the lowest-order bit of chosen pixels. This works well only if the image is not subject to any modification. A more robust watermark can be embedded by superimposing a symbol over an area of the picture. The resulting mark may be visible or not,

depending upon the intensity value. Picture cropping, e.g., (a common operation of image editors), can be used to eliminate the watermark.

Spatial watermarking can also be applied using color separation. In this way, the watermark appears in only one of the color bands. This renders the watermark visibly subtle such that it is difficult to detect under regular viewing. However, the mark appears immediately when the colors are separated for printing. This renders the document useless for the printer unless the watermark can be removed from the color band. This approach is used commercially for journalists to inspect digital pictures from a photo-stockhouse before buying unmarked versions.

Watermarking can be applied in the **frequency domain** (and other transform domains) by first applying a transform like the Fast Fourier Transform (FFT). In a similar manner to spatial domain watermarking, the values of chosen frequencies can be altered from the original. Since high frequencies will be lost by compression or scaling, the watermark signal is applied to lower frequencies, or better yet, applied adaptively to frequencies that contain important information of the original picture. Since watermarks applied to the frequency domain will be dispersed over the entirety of the spatial image upon inverse transformation, this method is not as susceptible to defeat by cropping as the spatial technique. However, there is more a tradeoff here between invisibility and decodability, since the watermark is in effect applied indiscriminately across the spatial image. Table 1. shows a small comparison between the two different techniques.

International Journal of Computing and Business Research (IJCBR)

ISSN (Online) : 2229-6166

Volume 4 Issue 2 May 2013

	Spatial Domain	Frequency Domain
Computation Cost	Low	High
Robustness	Fragile	Most Robust
Perceptual Quality	High Control	Low Control
Capacity	High(Depend on the size of image)	Low
Example of Applications	Mainly Authentication	Copy Rights

Table 1 : Comparison between Watermarking Techniques

CONCLUSION AND FUTURE WORK

The work described here is concerned with the design of robust digital image watermarking algorithms for copyright protection. Various types and application of watermarks were introduced and an overview of existing watermarking algorithms and attacks are given.

In the field of watermarking, the feature points can be used as the reference locations for the both the watermark embedding and detection processes. The feature points are detected with feature point detectors and these detectors should extract the feature points that are robust on various distortions (compression, filtering, geometric distortions, etc.).

In the case of filtering and compressions (JPEG and JPEG 2000), both detectors showed excellent performances. However, in experiments presented, only the feature points with the largest characteristic scale were observed.

The resistance of watermarking schemes against geometrical distortions is one of the still opened and challenging problems in the field of watermarking. One possibility to recover the watermark synchronization is to implement the image registration technique before the watermark detection procedure. An image registration technique, based on establishing point-by-point correspondence

between the original image and image possibly altered by unknown geometrical transformation (received image) is demonstrated. The feature points are extracted with the SIFT detector, where as the SIFT descriptors were calculated for every feature point. The correspondences between the points were established by measuring the correlation coefficient between the SIFT descriptors. When the correspondence between two images is determined, the parameters of the undergone geometrical transformation are estimated and an inverse geometrical transformation is calculated and applied to the received image. This technique effectively estimates the parameters of undergone affine transformation.

Another possibility to recover the watermark synchronization is to implement the synchronization technique. One important feature of this technique is that it does not require the presence of original, or watermarked image. This technique combines the template based and content based approach. The main idea of this technique is to extract the robust feature points with SIFT detector and to embed in the neighborhood of every feature point two information, which can be later used to detect the parameters of undergone geometrical transformations. These two information are embedded robustly using DFT and they represent information about the reference angle and the information about the characteristic scale of the feature point. When the affine transformation, consisted of image rotation, scaling, cropping or combination of them, occurs, it is enough correctly to detect at least from one feature point neighborhood these two information. After that, the parameters of rotation and scaling can be easily calculated. This was demonstrated in experiments presented, and it is shown that compressions (JPEG and JPEG2000) have no influence on the extraction of these two information, as well.

The watermarking presented here is essentially a classical non-blind additive watermarking algorithm in wavelet domain, just like many of the existing algorithms. Using this algorithm the impact of different error correction codes on the watermark robustness was investigated. From this point of view, it is shown that the Read-Solomon error correction code delivers the best

results. The same watermark is embedded in all detail subbands of a two-level DWT. Further, it is tested which subband of DWT decomposition shows the best performances for watermark embedding. The robustness of the watermark was tested on different filtering and compression attacks. It was concluded that the best results are obtained if the watermark is embedded in the subbands 2 LH and 2 HL. The robustness on geometric attacks of this algorithm is additionally improved by using the aforementioned image registration technique.

The second watermarking algorithm developed in the wavelet domain belongs to a class of blind additive algorithms. The watermark embedding is performed in the central part of the image. In this way the cropping of the certain percentage of the image size (in our case, we set to 25 %) has no influence on the watermark detection. The watermark sequence is encoded with Read-Solomon error correction code and embedded in the largest coefficients of the LH and HL DWT subbands. In order to increase the robustness on cropping attacks, a new position vector of the modified DWT coefficients is calculated redundantly and relative to the location of the feature points in the subband. In a classical additive approach, the modified DWT coefficient depends on the original DWT coefficient and the watermark. Here this coefficient depends additionally on the mean value of all DTW coefficients selected for watermark embedding. In this way the stronger watermark was embedded into the image which enables later blind watermark detection. Here, the robustness of different watermarks on attacks is tested. The watermark was embedded in the LH and HL subbands of second, third and fourth levels of the DWT decomposition. The best results were obtained for the watermark embedded in the LH and HL subbands of third level of decomposition. The robustness of this algorithm on geometrical attacks is additionally improved by using the aforementioned proposed synchronization technique.

REFERENCES

International Journal of Computing and Business Research (IJCBR)

ISSN (Online) : 2229-6166

Volume 4 Issue 2 May 2013

1. Hal Berghel, "Watermarking Cyberspace", Comm. of the ACM, Nov.1997, Vol.40, No.11, pp.19-24.

2. G. W. Braudaway, et. al., "Protecting Publicly Available Images with a Visible Image Watermark", Proc. SPIE Conf. Optical Security and Counterfeit Deterrence Technique, Vol. SPIE- 2659, pp.126-132, Feb. 1996.

3. E. H. Adelson. Digital signal encoding and decoding apparatus. Technical Report 4,939,515, United States Patent, 1990.

4.C.-T. Li and F.M. Yang. One-dimensional Neighborhood Forming Strategy for Fragile Watermarking. In Journal of Electronic Imaging, vol. 12, no. 2, pp. 284-291, 2003.

5.C. Podilchuk and W. Zeng. Image-adaptive Watermarking Using Visual Models. In IEEE Journal Selected. Areas of Communications, vol. 16, pp. 525-539, May 1998.

6. C. Podilchuk and E. Delp. Digital Watermarking Algorithms and Applications. In IEEE Signal Processing Magazine, vol. 18, no. 4, July 2001.

7.I. J. Cox, M.L. Miller and J.A. Bloom. Digital Watermarking. Morgan Kaufmann, San Francisco, USA, 2002.

8.Y. Yuan and C.T. Li. Fragile Watermarking Scheme Exploiting Non-deterministic Block-wise Dependency. In Proc. of the IAPR Int. Conf. on Pattern Recognition, vol. IV, pp. 849-852, Cambridge, UK, 2004.

9.G. Qu, J.L. Wong, and M. Potkonjak. Optimization- IntensiveWatermarking Techniques for Decision Problems. 36th Design Automation Conference Proceedings, pp. 33-36, 1999.

10.J. Brassil, S. Low, N. Maxemchuk, and L. O'Gorman, "Electronic marking and identification techniques to discourage document copying," IEEE J. Select. Areas Commun., vol. 13, pp. 1495–1504, Oct. 1995.

11.A. Bors and I. Pitas, "Embedding parametric digital signatures in images," in EUSIPCO-96, Trieste, Italy, Sept. 1996.

12."Image watermarking using DCT domain constraints," in Proc. Int. Conf. Image Processing (ICIP), Lausanne, Switzerland, Sept. 1996.

13.S. Low, N. Maxemchuk, J. Brassil, and L. O'Gorman, "Document marking and identification using both line and word shifting," in Proc. Infocom '95, Boston, MA, Apr. 1995.

14."Secure spread spectrum watermarking for images, audio, and video," NEC Res. Inst., Princeton, NJ, Tech. Rep. 95-10, 1995.

15.Digital watermarking using multiresolution wavelet decomposition," in Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing 1998 (ICASSP 98), vol. 5, Seattle, WA, May 1998, pp. 2969–2972.

16.H. D. L¨uke, Korrelationssignale (in German). Berlin, Germany: Springer, 1992.

17."An information-theoretic approach to the design of robust digital watermarking systems," in Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing 1999 (ICASSP '99), Phoenix, AZ, Mar. 1999.

18.M. J. J. J. B. Maes and C. W. A. M. Overveld, "Digital watermarking by geometric warping," in Proc. Int. Conf. Image Processing (ICIP), vol. 1, Chicago, IL, 1998.

19.I. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for images, audio and video," in Proc. IEEE Int. Conf. Image Processing (ICIP 96), Lausanne,

Switzerland, Sept. 1996.

20.F. Hartung and B. Girod, "Digital watermarking of raw and compressed video," in Proc. SPIE Digital Compression Technologies and Systems for Video Commun., vol. 2952, Oct. 1996,

pp. 205–213.

21.V. Darmstaedter, J.-F. Delaigle, D. Nicholson, and B. Macq, "A block based watermarking technique for MPEG-2 signals: Optimization and validation on real digital TV distribution links," in Proc. European Conf. Multimedia Applications, Services, and Techniques—ECMAST '98, Berlin, Germany, May 1998.

22.R. Ohbuchi, H. Masuda, and M. Aono, "Embedding data in three-dimensional polygonal models," in Proc. ACM Multimedia '97, Seattle, WA, Nov. 1997.

23."Watermarking three-dimensional polygonal models through geometric and topological modifications," IEEE J. Select. Areas Commun. (Special Issue on Copyright and Privacy Protection), vol. 16, pp. 551–560, May 1998.