International Journal of Electronics Communication and Computer Engineering
Volume 2, Issue 2, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

A Novel Approach for Implementation of Robust Watermarking for Images

Prof. Yash Kshirsagar
Professor, Department of ECE
TIT, Bhopal

Anup. V. Kalaskar
M.Tech, Department of ECE
TIT, Bhopal

Shilpa. R. Jadhav
M.Tech, Department of ECE
TIT, Bhopal

Abstract – In this paper we introduce approach for implementation of robust watermarking for images.It is to be expected that digital photographs, videos, and sound tracks will gradually replace their analog counterparts in the near future. Digital representation of signals brings many advantages when compared to analog representations, such as lossless recording and copying, convenient distribution over networks, easy editing and modification, and durable, cheaper, easily reachable archival. Unfortunately, these advantages also present serious problems including wide spread copyright violation, illegal copying and distribution, problematic authentication, and easy forging. Piracy of digital photographs is already a common phenomenon on the Internet. Information hiding in digital documents provides a means for overcoming those problems. Depending on what information in which form is hidden in the image, one can distinguish at least two types of data hiding schemes: non-robust, undetectable data hiding, and robust image watermarking.

The objective is to implement robust image watermarking by embedding 32 bits of information into a single image in such a way that it is robust to JPEG compression and cropping.

Keywords - Robust watermarking, Digital photographs, Authentication, Information hiding, JPEG compression and cropping, Peak signal to noise Ratio, Discrete cosine transform (DCT), spread spectrum (SS) watermark.

1. INTRODUCTION

Depending on what information in which form is hidden in the image, one can distinguish at least two types of data hiding schemes: non-robust, undetectable data hiding, and robust image watermarking. In the first case, a digital image serves as a container for a secret message. Suppose, a spy in foreign country wants to send messages abroad. He needs to use local communication channels in order to send the messages. He should assume that the communication channel is monitored. Sending encrypted messages would raise suspicion and could result in cutting the access to the communication infrastructure. It is therefore in his best interest to hide the presence of communication at all. This could be solved using a clever stenographic protocol.

In the second application, robust image watermarking, a short message (a watermark) is embedded in the image in a robust manner. By robustness we mean the ability to survive common image processing operations, such as loss compression, filtering, noise adding, geometrical transformations, etc. Such robust watermark can be obviously used for copyright protection, fraud detection (verification of image integrity), authentication, etc. At this point we emphasize that cryptographic authentication protocols cannot solve all the issues related to authentication. Cryptographic authentication deals with authenticating the sender of the message over insecure channels. However, once the message (image) is decrypted, the image is unprotected and can be copied and further distributed. Unlike classical paintings that can be studied for authenticity using sophisticated experimental techniques, a digital artwork is just a collection of bits. A visible signature in the corner of the image can be easily replaced or removed with advanced image processing software packages, such as Photo Shop. Additional information in the image header can be erased or changed as well. In other words, any attempt to authenticate the digital image by appending information will fail. Digital watermarking provides an appealing alternative by embedding rather than appending information directly into the image itself. The embedded information will be transparent to the human eye, but it should be detectable using a sophisticated algorithm provided a secret key is available.Note that we do not impose any security requirements for the watermarking technology[4].

The developed watermarking technology embeds two watermarks, a strong direct-sequence spread spectrum (SS) watermark tiled over the image in the lapped bi-orthogonal transform (LBT) domain [3].

2. AIM

The aim is to Implement Robust Watermarking by developing encoding technique, which can find out the possibility to hide maximum amount of data in an image without degrading its quality. Second issue is to make the hidden data robust enough to withstand image processing which do not change the appearance of image. So this technique can also be used for digital watermarking. And also, this technique should be computationally less intensive.

3. PRINCIPLE OF MODEL

The term “watermark” has been known long before the age of computing: watermarks were found on bank notes to make falsification difficult or on writing paper to add an individual taste or corporate identity. On computers, such applications are possible, too: in 1994, the German software company Star Division distributed free copies of their word processor Star Writer to visitors on the Hanover CeBitfair; the copies were fully functional,

only that when printing documents from within the application, a watermark would be printed as the background of the document's pages. Other common applications for watermarks on computers include proof of rightful ownership and authentication for multimedia objects like images.

Since multimedia objects are digital representations of analogue data (like sound, photos, movies) they tolerate some amount of manipulation as long as some rules are obeyed. If some pixels' intensities in an image are changed subtly, the human eye is unlikely to notice this, yet these changes can carry information visible to the respective detection software.

Figure 3.1 shows a digital image watermarking system's principle setup. In many cases there is an additional data item necessary for embedding or detection, like a secret key. Also, the kind of detection result obviously depends on the watermarking system's purpose and design in some cases the presence of a known watermark pattern is detected, in others a message of some kind (text, or even multimedia contents like images, audio etc.) is read.

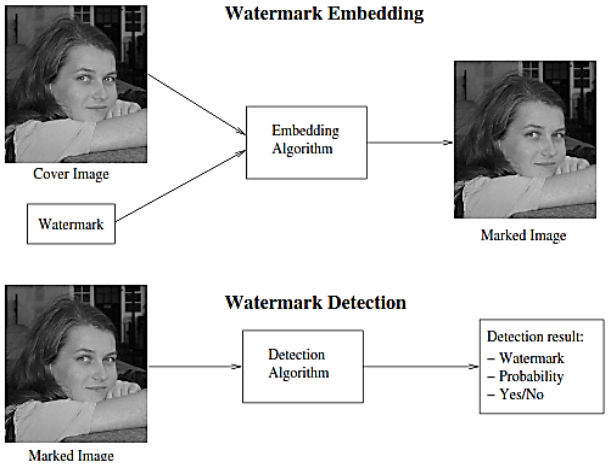


Figure 3.1: Principle Image Watermarking Framework

In general, watermarks can be either visible or invisible. Visible watermarks , also known as masks are often used to mark demonstration images to avoid commercial exploitation; also public libraries sometimes add visible watermarks to copies made from books, papers etc. However their relevance for fragile or robust watermarking is usually rather low most applications deal with original images that need to be of high quality. Therefore most such applications apply invisible watermarks.

4. CONTRIBUTED WORK

In the course of the research project presented in this thesis various aspects involved in robust image watermarking were investigated:

• Different filters were compared to establish their suitability for marking under consideration of image quality and robustness against a simple attack based on lossy compression.

This included implementing embedding technique. Since the various filters have different properties affecting both image quality and robustness, the optimal choice of filter can help optimizing direct-sequence spread-spectrum (SS) watermark watermarking schemes. The results from this research were published in International journal of electronics communication & computer engineering.

• A method to compare the detected watermark to the original (both binary images) was developed and implemented.

• Besides already mentioned surveys, image assessment work has been reviewed and benchmarked in [8]. Standard techniques such as MSE and PSNR have not been matched well to perceived visual quality [10]. Some of the main trends in the field are at the intersection between cognitive sciences [9], understanding the workings of the visual cortex, and ad-hoc heuristics. For example, one class of algorithms separates images into sub-bands (i.e., channels) that are selective for spatial and temporal frequency and orientation. Sophisticated channel decompositions analyze the neural responses in the primary visual cortex [1], [11], [12]. Alternatively, many metrics use simpler transforms such as the DCT [13] or separable wavelet transforms [14], [15] to achieve the same goal. Channel decompositions based upon temporal frequencies have also been used for video quality assessment [16].Thus, visual masking models have been proposed to account for the interdependence of image coefficients [1].Finally, within the realm of watermarking, a related focus to high quality imaging has appeared in [7].

5. ATTACK TOLERANCE OF MODEL

The aim of attacking a robust watermarking system is usually to prevent the watermark embedded (usually owner or copyright holder) from using the watermark to support his claims. This can be accomplished in two ways: either by rendering the watermark unreadable or by successfully disputing the claim based on the watermark detection result. We denote these categories as image processing attacks and protocol attacks in the above order, even though there are other ways to make a watermark undetectable than through classic image processing.

In general, image processing attacks have to fulfill two rather conflicting requirements: the image quality must not suffer, and the attack must make it impossible for the watermark embedded to successfully detect the mark. The second point leads to the conclusion that the attack does not actually have to remove the mark. Specifically, we choose two filters: one that computes the differential standard derivation and another that calculates the entropy of a local region centered at the pixel-of-interest. Given an image $I \in \{Z^*\}^{m \times n}$, for each of its pixels $k(x, y) \in I$ where x and y denote pixel coordinates, we examine its r-by-r neighborhood[1] $\Pi(k)$ centered at k and define the following metrics:

$$S(k,r)=\sqrt{\frac{1}{r^2-1}\sum_{i \in \pi(k)}\left(i-\frac{1}{r^2}\sum_{j \in \pi(k)} j\right)^2} \quad (1)$$

$$E(k,r) = -\sum_{i=1}^{256} p(k,i)\log\left[p(k,i)\right] \quad (2)$$

$$p(k, i) = Pr[k = i|k \in \Pi(k)]. \quad (3)$$

International Journal of Electronics Communication and Computer Engineering
Volume 2, Issue 2, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

The entropy map E (k, r) indicates the complexity of the neighborhood for a given pixel. This is a simple heuristic to identify pixels that are perceptually less tolerant to noise. Empirically, this claim usually holds true for pixels with low E (k, r), i.e., regions with smoothly changing luminosity.

6. IMPLEMENTATION & EMBEDDING OF ROBUST WATERMARK

We built the system in two steps: first, we embed a soft, spread-spectrum watermark whose objective is to signal metadata presence. If this watermark is detected, the decoder proceeds with the message extraction by analyzing localized statistics of the image.

The objective is to embed 32 bits of meta-data as a hard watermark into an image so that their detection is as robust as possible to JPEG compression and cropping. Image watermarking schemes that pertain to this goal, can use the developed visual model to achieve visual transparency as well.

Here we overview the two techniques.The soft watermark (SW) serves two purposes: To detect the existence of the meta-data &To enable image registration at the detector side due to potential cropping or other type of misalignment.

We design the Soft Watermark (SW) to be a random i.i.d. sequence taking value from {-1, 1} or drawn from a standard normal distribution N(0, 1). The SW is spread over a continuous image region of size L.

We denote this region the basic SW block. We create a full image watermark by tiling the same basic SW block. Consequently, the smallest image that can be augmented with meta-data is the size of the basic SW block. In order to reduce blocking effects, we propose to embed the SW in the Lapped Biorthogonal Transform (LBT) domain [3]. In the LBT domain, we choose to leave the DC and high frequency components untouched for better visual quality and robustness to lossy compression,respectively. We introduce a mask for each 4-by-4 block of the LBT image:

$$t = \begin{vmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{vmatrix} \quad (4)$$

where ones indicate the LBT coefficients used for SW embedding. Next, we use f(I) to adjust the energy of the SW according to the content of the image. Since the complexity map is in the pixel domain, we take the inverse LBT transformation of the watermarked image and re-weight the watermark in the pixel domain using f(I). With the above considerations, the SW embedding can be expressed as:

$$Y = I+\alpha f(I)\{LBT^{-1}[LBT(I)+wt]-I\} \quad (5)$$

where wt denotes the masked SW, and Y represents the watermarked image. Parameter a adjusts the watermark energy to achieve the desired trade-off between visual quality and robustness. In our experiments, we used α = 10 in order to create images within 55-50dB PSNR from the original. The SW alone is hardly visible at these noise levels. However, it conveys only one and halfbits of information to the detector.

The hard watermark (HW), which represents the meta-data bits. Here we enter 32 bit wide in formation as hard watermark.

[x y z ...]: [1 0 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 1 1]

Since the detector has no access to the original image, the host signal acts as a strong source of noise during detection. To reduce the interference from the host signal, we deploy quantization of source's first order statistics to embed the HW. Specifically, we partition each part of the image where exactly one basic SW block is augmented into small building blocks. If the size of the basic SW block is L, the number of pixels included in each building block equals $k = \frac{Lr \times Lc}{32}$, where K is denoted as the scaling constant. Typically, we aim at K such that the size of the building block is between 4 ×4 and 8 × 8 pixels. For example, for a basic SW block of size 640 × 480, and K = 48, e.g., a building block of dimensions 8 × 6 pixels, we obtain K = 200. Then, for each meta-data bit, we randomly assign exactly K distinct building blocks within the pixel field of the basic SW block. We denote the set of all coefficients that belong to these building blocks as Ai, I = 1 . . . 32.

We compute the first order statistics of the coefficients in each Ai:

$$\mu i = \frac{1}{kK}\sum_{p \in Ai} Y(p). \quad (6)$$

To embed a bit b1, we quantize µto an even number of Qs if b1has value 0, or to an odd number of Qs ifits value is one. Here, Q is the quantization step size. That's:

$$\mu'I = \left\lfloor \frac{(\mu i+Q)bi}{2Q} \right\rfloor 2Q - Qbi \quad (7)$$

$$\Delta\mu i = \mu'i - \mu i \quad (8)$$

Where µ'iis the mean value after HW embedding and Δµiis the corresponding Ai-wide change. It is straightforward to notice that larger Q results in a more robust HW at the cost of decreased visual quality.

The objective is to allocate the HW to pixels so that the correlation of the watermarked image with SW becomes higher. This can be done by choosing only the pixels whose corresponding SW component has the same sign as the Δµifor embedding:

$$\Delta y(p) = \begin{cases} \Delta\mu i k K \frac{f(p)}{\sum_{p \in A'i} f(p)} & p \in A'i \\ 0 & \text{otherwise} \end{cases} \quad (9)$$

A'I = {p|sign(SW(p)) = sign(Δµi), p∈ Ai}.

In our experiments on a database of over 41 large images,after embedding both the soft and hard watermark, we have observed a resulting PSNR in the range from 49-40dB.

7. WATERMARK EXPOSURE

The detection process consists of two steps. First, we determine whether the test image contains a SW. If yes, we move on to extract the embedded meta-data.

Given a test image z, we first transform it into the LBTdomain to get z. Because the received image may have been cropped, we first align the test image by detecting the SWs. This is done by sliding the basic SW block w over z' and examining the normalized cross-correlation (NCC) values:

International Journal of Electronics Communication and Computer Engineering
Volume 2, Issue 2, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

$$c(zi, w) = \frac{(w-w\prime)(zi-zi\prime)}{||w|| \cdot ||Zi||} \quad (10)$$

for each sub-block zi z'. Operator ā denotes the mean of the argument a. Fast NCC for image registration can be computed via the FFT. Image z is declared tainted with w if max [c(z, w)] > T , where T is the detection threshold that identifies the probability of a false positive or negative according to the gaussian error function.

The extraction of the meta-data is rather simple. First, thedetector identifies the building blocks corresponding to each bit. Then, the mean pixel value ˆμ'iover each set of building blocks is calculated. The bit is extracted by quantizing ˆμ'iusing Q, and examining whether the quantized value is odd or even.

$$\hat{bi} = mod\{\lfloor \frac{\hat{\mu}}{Q} \rfloor, 2\} \quad (11)$$

Wherebiis the extracted bit, In case when there exists more than one SW, the detector uses a soft decoding technique. For simplicity, we use a repetition code to encode each metadata bit, i.e., we augment each bit in each basic SW block separately. We denote asthe bitb(r, i) the i-th extracted copy offrom the r-th basic SW block. For each bit, we record the distance d(r, i) of the statistic μ'ito nearest reconstruction point. This value quantifies the confidence level of the detection for each raw bit. We collect this soft information for all extracted bits & estimate the final metadata bit Bibased on the confidence scores S0and S1:

$$Bi = \begin{cases} 0 & S0 \geq S1 \\ 1 & otherwise \end{cases}, \quad (12)$$

$$Sx = \sum_{\{ r | \hat{b}(r,i)=x \}} \exp\left\lfloor \frac{-10|d(r,i)|}{Q} \right\rfloor$$

8. RESULTS

8.1 Analysis of Results

We have done maximum possible experiments to prove our proposed method and finally we got effective results for efficient image annotation in which we hide 32 bit meta-data in any high fidelity image with medical or any precious value for which used HW and SW.

After embedding the given 32 bit wide hard watermark there is shifting in the first order & Second Order statistics from which we calculate Complexity Vector 1.0e+005 * Which Gives the value representing the noise can introduce for specific block at specific column by embedding soft and hard watermark which is given in the following table.

Complexity Vector 1.0e+005 * is:

Table 1

32 bit Embedded Original Watermark (Information)			
Columns 1 To 8	Columns 9 To 16	Columns 17 To24	Columns 25 To 32
0	0	0	0
3.3645	0	0	0
2.2004	2.6423	2.6536	1.6888
1.7656	2.7912	2.6665	1.8641
0	0	0	0
0	0	0	0
1.7582	2.3262	2.0662	0
1.3999	2.4764	1.5271	0

32 bit wide hard watermark which is nothing but the information which is embedded in the given image is distributed randomly in the image through 1 to 32 columns which is given below in the given table.

Table 2

32 bit Embedded Original Watermark (Information)			
Columns 1 To 8	Columns 9 To 16	Columns 17 To24	Columns 25 To 32
1	1	1	1
0	1	1	1
0	0	0	0
0	0	0	0
1	1	1	1
1	1	1	1
0	0	0	1
0	0	0	1

We detect the original embedded watermark which is nothing but hard watermark (An Information) at the receiver end with the help of decoding algorithm which make the use of soft watermark for detection of hard watermark but this algorithm is known to only exact receiver.

The decoded 32 bit wide hard watermark (An Information) is given as similar it is embedded in 32 different columns as given in the following table.

Table 3

Detected Watermark (Information)			
Columns 1 To 8	Columns 9 To 16	Columns 17 To24	Columns 25 To 32
1	1	1	1
0	1	1	1
0	0	0	0
0	0	0	0
1	1	1	1
1	1	1	1
0	0	0	1
0	0	0	1

For the final result we compare both the embedded Watermark Result in **Table 3** and detected watermark Result in **Table 4** from our experimental result which will clarify the result is as discussed above which shows there is no difference between the embedded and detected watermarks.

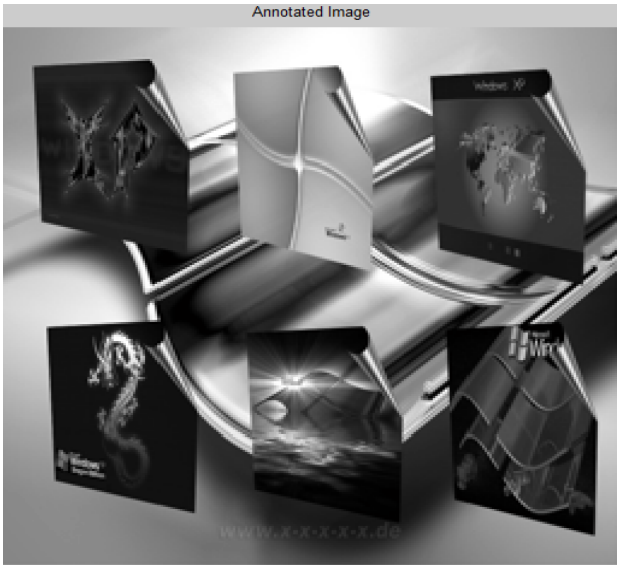
Which shows that the experimental results are accurate and satisfactory which satisfy our aim of this research which will be very useful for Hi speed, highly secured, Hi-Fidelity Image Annotation for data embedding.

8.2 Visual Demonstration of Results

Visual Demonstration of the visual differences between the original image with no watermark Fig(b), and annotated image with both soft and hard watermarks augmented Fig(c). The annotated image illustrates the actual pixel value alterations after embedding the both the watermarks:

(a)

(b)



(c)

Figure: (a) Original Input RGB Image (b) original image converted in Gray scale with no watermarks (c) Output Annotated image with both soft and hard watermarks augmented.

9. CONCLUSION AND FURTHER RESEARCH

9.1 Conclusions

The number of bits of data that can be stored depends upon the number of range blocks that have match in domain region. Bigger the range region more is the data that can be stored. But, since range region cannot overlap the domain region, on increasing the range region, domain region is reduced which may lead to worse quality of image. So, there is a trade-o between the amount of data and quality of image produced.

Increase in tolerance level would allow using all range blocks so that more data can be stored. However low tolerance is desirable in order to give an image that is visually close to the original.

We have conducted several experiments to evaluate our proposed method on a database of 41 challenging images. Figure 1 shows a small portion of one of the original test images with a large smooth region. Most of the semantic content of the image is expressed as an edge. This is an example of an image which is relatively hard to watermark in-perceptively. The same figure illustrates the output of an existing hi-fidelity watermarking scheme compared to our result.

9.2 Further Research

Further research should go towards improving the watermarking program and adding extra functionality. One of these is looking at having multiple watermarks for a single image, so that di erent parts of the image have a di erent watermark. There is also the need to further develop the robustness of existing watermarking techniques to combat the ever-increasing attacks on watermarks.

We used fixed partitioning scheme. Instead of this, adaptive partitioning scheme can be used, which would yield better results if used as the basis for the data hiding method.

In this thesis, we explored the Image Annotation method for 32-Bit Meta data using Soft and Hard Watermarks but they have their own limitations. There is a big scope to explore the more developed watermarking techniques to combat the ever-increasing attacks on watermarks.

REFERENCES

[1] P.C. Teo and D.J. Heeger, “Perceptual image distortion,’ ’ SPIE, vol.2179, pp.127-141, 1994.

[2] Shan He; Kirovski, D. Min Wu; Thomson Corp. Res., Princeton, NJ, “A Novel Visual Perceptual Model with AnApplication to Hi-Fidelity Image Annotation, IEEE Trans. on Image Processing, vol.18, pp.429–434, 2009

[3] H.S.Malvar, “Biorthogonal and Nonuniform Lapped Transforms for Transform Coding with Reduced Blocking and Ringing Artifacts,” IEEE Trans. on Signal Processing, pp.1043–1053, 1998.

[4] I.J. Cox, et al., “A secure, robust watermark for multimedia,” Info Hiding Workshop, pp.183–206, 1996.
[5] Z. Wang, et al., “Why is image quality assessment so difficult,” IEEE ICASSP, vol.4, pp.3313-3316, 2002.
[6] D.A. Silverstein and J.E. Farrell, “The relationship between image fidelity and image quality,” IEEE ICIP, pp.881-884, 1996.
[7] C.I. Podilchuk and W. Zeng, “Image-Adaptive Watermarking Using Visual Models,” IEEE Journal on Selected Areas in Communications, vol.16, no.4, 1998.
[8] Z. Wang, et al., “Objective video quality assessment,” in Handbook of Video Databases, pp.1041-1078, CRC Press, 2003.
[9] W.F. Good, et al., “Joint photographic experts group (JPEG) compatible data compression of mammograms,” Journal on Digital Imaging, vol.17, no.3, pp.123-132, 1994.
[10] B. Girod, “Whats wrong with mean-squared error,” in Digital Images and Human Vision, MIT Press, pp.207-220, 1993.
[11] J. Lubin, “A visual discrimination model for imaging system design and evaluation,” in Visual Models for Target Detection and Recognition, World Scientific, pp.245-283, 1995.
[12] S. Daly, “The visible differences predictor: An algorithm for the assessment of image fidelity,” in Digital Images and Human Vision, pp.179206, MIT Press, 1993.
[13] A.B. Watson, “DCT quantization matrices visually optimized for individual images,” SPIE, vol.1913, 1993.
[14] A.B. Watson, et al., “Visibility of wavelet quantization noise,” IEEE Trans. on Image Processing, vol.6, pp.1164-1175, 1997.
[15] A.P. Bradley, “A wavelet visible difference predictor,” IEEE Trans. on Image Processing, vol.5, pp.717-730, 1999.
[16] C.J. van den BrandenLambrecht and O. Verscheure, “Perceptual quality measure using a spatio-temporal model of the human visual system,” SPIE, vol.2668, pp.450-461, 1996.