International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-4 Issue-4, September 2014

Comparison of Robustness in Watermarking Techniques

Mohamad Owais Raja, Tazeem A. Khan, Junaid Geelani

Abstract: ***A methodology for comparing robustness of spatial domain and transform domain watermarking techniques is proposed. The techniques used in the spatial domain are the least significant bit method and the transform domain technique used is the discrete cosine transforms based method. The techniques are compared on the basis of their susceptibilities to various types of noises which a work of digital media undergoes during intentional or unintentional modification in the real world. The recovery of watermarks in such simulated conditions as addition of Gaussian noise , salt & pepper noise, JPEG compression leads us to draw conclusions about how these techniques fare in the actual world. Moreover, the noise levels have been varied so as to elicit the threshold where even an otherwise robust technique fails.***

Keywords: Digital watermarking, robustness, perceptual distortion measures, spatial and transform techniques..

I. INTRODUCTION

Digital watermark is a perceptually transparent pattern inserted in an image using an embedding algorithm and a secret key. The purpose of the watermark is to supply some additional information about the image to identify the image owner or a particular customer, to verify image integrity, or to achieve control over the copy process of a particular digital media [1][2]. The information carried by the watermark can be can be accessed using a detection algorithm provided the secret key is known. An important property of a watermark is its robustness with respect to image distortions. This means that the watermark should be readable from images that underwent common image processing operations, such as filtering, lossy compression, noise adding, histogram manipulation, and various geometrical transformations. Watermarks designed for copyright protection, fingerprinting, or access control must also be embedded in a secure form. This means that an attacker who knows all details of the embedding algorithm except the secret key should not be able to disrupt the watermark beyond detection. In other applications, such as adding additional captions to images or subtitles in several languages to movies, there is little motivation for intentional removal of the watermark, and the embedding/detecting key can be made public. The number of bits carried by the watermark could be as low as one bit or several hundred bits. Obviously, there is a trade-off between the robustness and the capacity of the watermark.

Manuscript published on 30 September 2014.
***Correspondence Author(s)
Mohamad Owais Raja, M. Tech Scholar, Department of ECE, AFSET, Faridabad, India.
Tazeem A Khan, Asst. Prof., Department of ECE, AFSET, Faridabad, India.
Junaid Geelani, Head, Electronics and Communication Government Women's Polytechnic Srinagar, India.

Another important attribute of watermarking is the computational complexity of the embedding and extracting process. In some applications, it is important that the embedding process be as fast and simple as possible (watermarking images in digital cameras for tamper detection) while the extraction can be more time consuming. In other applications, the speed of extraction is absolutely crucial (e.g., extracting captions from digital video). The idea of comparing watermarking techniques is fruitful. The choice of test images could be fixed, as well as a set of stego images or copyright information. Each watermarking technique could be put into standard forms to embed a bit pattern or a repetition of bit pattern. The watermark strength (or visibility) can be adjusted using a model of the human visual system so that the number of pixels with visible changes is less than a specified fraction. Each watermarking scheme would also have to be adjusted so that the probability of false detections and missed detections is below certain specified limit. Watermarking techniques standardized in this manner could probably be meaningfully compared. The robustness of different techniques can be measured by finding the value of the distortion parameter (e.g., quality factor for JPEG compression) at which the watermark is lost. For techniques that embed multiple-bit watermarks, one can use the bit error rate as the discriminating parameter. This way, we may be able to compare robustness of different techniques to specific image distortions. The results of the comparison can actually be used for finding the most useful application for a particular technique. Pointing out the strong points of different schemes will lead to better applications, composite schemes, and new schemes. A good methodology for comparing would also give us a useful tool for identifying what schemes have good potential and should be further developed and which are weak. Assuming that a methodology for comparing schemes is available, there are several possible ways how to approach the comparison study. The first possibility is that one researcher implements all typical representatives available in the literature and performs all the tests. This, however, has a serious drawback because for some techniques the implementation issues are critical and are not always adequately described in papers. In some cases, the inventors may not even be willing to share their experience. Thus, our researcher could end up comparing bad implementation of one technique with a fine-tuned implementation of another technique. It seems that a better way of achieving a truly fair comparison would be to get the authors of the techniques involved in the whole process.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

The second possibility is to ask every participant to send a source code for his/her technique, and one person would run all standard tests. However, this again may not be a practical solution because distributing the source code may not be acceptable for everybody, especially for private companies or industrial research centers. It appears that the best choice would be to make the testing methodology and guidelines together with associated routines publicly available for download and challenge every participant to perform the tests. One researcher would gather the data, evaluate, and publish the results. The purpose of this paper is to describe such a methodology and guidelines and initiate the process of comparing watermarking schemes. In next sections, we describe a methodology for comparing watermarking schemes. We also present a family of image deformations with a parameter with respect to which the robustness will be evaluated. We use one spatial domain technique which is the least significant bit method and one frequency domain technique called the discrete cosine transform based method of watermarking. The results of tests are summarized and discussed . Finally, we conclude the paper and outline some directions towards a formal definition of robustness.

II. TESTING METHODOLOGY

The robustness is usually tested using typical image processing operations that can be divided into two groups: gray scale manipulations (filtering, noise adding, lossy compression, gamma correction, color quantization, color truncation to a finite palette, etc.) and geometric transformations (scaling, cropping, rotation, affine transforms, general rubber sheet deformations of Stir Mark type[4]. It is significantly easier to achieve robustness with respect to gray scale transformations than to geometrical transformations. Vast majority of watermarking schemes embeds the watermark by modifying the gray scales while leaving the image geometry untouched (one exception is the watermarking method based on geometric warping due to Maes[5]. One can say that geometric transformations do not erase watermarks but make the detection difficult if not entirely impossible. In theory, for any combination of rotation, shift, and scale an extensive search could be applied and the watermark recovered. However, this is not a practical solution due to extensive computational complexity of the search. Those schemes that are robust with respect to geometrical transformations usually utilize a separate synchronization pattern or transformation invariants for detecting the geometrical transformations applied to the watermarked image [6][7][8][9][10]. Once the geometric transformation is estimated, an inverse transform is applied and the actual watermark is read from the transformed image (it is likely the image will be resample and/or cropped). Since the synchronization pattern can be combined with different watermarking schemes, we did not include the tests of robustness with respect to geometric deformations in our methodology. Instead, we used three different types of manipulations i.e., the salt and pepper noise, the Gaussian noise and the JPEG compression to understand the reliability of recovering a watermark once embedded. The level of noise was progressively increased to find the threshold at which the watermark recovery becomes impossible to compare visually with the original watermark.

III. SPATIAL AND FREQUENCY DOMAIN TECHNIQUES

We chose two techniques that embed the watermark: one spatial domain using LSB substitution method and other transform domain technique by modulating the DCT coefficients. These two techniques have contrasting robustness properties. The first technique is considered to be least robust but has exceptional property of capacity which means that a large number of bits can be embedded. The second technique is based on modulating the middle band of frequencies of disjoint image blocks by a random Gaussian signal. The most straight-forward method of watermark embedding would be to embed the watermark into the least-significant-bits of the cover object [11]. Given the extraordinarily high channel capacity of using the entire cover for transmission in this method, a smaller object may be embedded multiple times. Even if most of these are lost due to attacks, a single surviving watermark would be considered a success. An advantage of the spatial techniques can be easily applied to any image, regardless of subsequent processing (whether they survive this processing however is a different matter entirely). A possible disadvantage of spatial techniques is they do not allow for the exploitation of this subsequent processing in order to increase the robustness of the watermark. In addition to this, adaptive watermarking techniques are a bit more difficult in the spatial domain. Both the robustness and quality of the watermark could be improved if the properties of the cover image could similarly be exploited. For instance, it is generally preferable to hide watermarking information in noisy regions and edges of images, rather then in smoother regions. The benefit is two-fold; Degradation in smoother regions of an image is more noticeable to the HVS, and becomes a prime target for lossy compression schemes. Taking these aspects into consideration, working in a frequency domain of some sort becomes very attractive. The classic and still most popular domain for image processing is that of the Discrete-Cosine-Transform, or DCT. The DCT allows an image to be broken up into different frequency bands, making it much easier to embed watermarking information into the middle frequency bands of an image. The middle frequency bands are chosen such that they have minimize they avoid the most visual important parts of the image (low frequencies) without over-exposing themselves to removal through compression and noise attacks (high frequencies) [13]. One such technique utilizes the comparison of middle-band DCT coefficients to encode a single bit into a DCT block. To begin, we define the middle-band frequencies (FM) of an 8x8 DCT block. Rather than arbitrarily choosing these locations, extra robustness to compression can be achieved if we base the choice of coefficients on the recommended JPEG quantization table. If two locations are chosen such that they have identical quantization values, we can feel confident that any scaling of one coefficient will scale the other by the same factor preserving their relative size.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

The swapping of such coefficients should not alter the watermarked image significantly, as it is generally believed that DCT coefficients of middle frequencies have similar magnitudes. To begin, we define the middle-band frequencies (FM) of an 8x8 DCT block as shown below in figure 1.

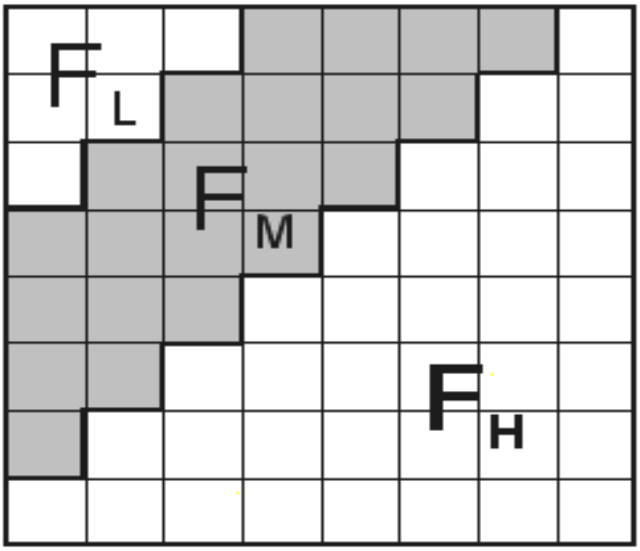

Figure 1 Definition of DCT Regions

FL is used to denote the lowest frequency components of the block, while FH is used to denote the higher frequency components. FM is chosen as the embedding region as to provide additional resistance to lossy compression techniques, while avoiding significant modification of the cover image [5].

IV. RESULTS OF COMPARISON

In order to evaluate different algorithms especially with regards to their robustness we wrote different programs in MATLAB 7.0 , using in particular the MATLAB editor to create M-files. We successfully performed digital watermarking on real images taken from the USC-SIPI database [14]. The USC-SIPI image database is a collection of digitized images which are free of copyrights if used in image processing research. The miscellaneous sub-set consists of 40 images like baboon, Lena and peppers, of various sizes such as 256x256 pixels, 512x512 pixels, or 1024x1024 pixels. The details of results having successfully embedded, detected and verified different parameters of various algorithms are elucidated below. The processing time of various algorithms was also calculated. In general, algorithms were implemented in the most straightforward way, not the most computationally optimal. Furthermore, the software may handle certain programming constructs differently from other languages, thus the best performing algorithm may vary for each language and implementation. In spite of these limitations we obtained pretty decent results. Next, robustness evaluations were limited to testing against JPEG compression, the addition of guassian and salt & pepper noise. We also calculated the PSNR of each watermarked image. Even though, PSNR does not take aspects of the HVS into effect so that images with higher PSNRs may not necessarily look better than those with a low PSNR. Still use of PSNR is a good indicator of the perceptibility of an image when compared to the original un-watermarked image.

4.1 Comparison of Mid-Band DCT Coefficients

The following results were obtained for mid-band DCT coefficients based watermarking

Figure 2 Watermarked Image PSNR = 67.6 dB

Figure 3 Recovered Watermark

Comparison-of-mid-band-DCT-Coefficients recovered watermarks under different attacks.

Figure 4(a) - 5% Gaussian Noise

Figure 4(b) - 15% Gaussian Noise

Figure 4(c) – JPEG Compression Q=50

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Figure 4 (d) – JPEG Compression Q=20

Here we include results for comparison-based correlation in the DCT mid-band Comparison-based Correlation in the DCT mid-band K = 15

Figure 5 (a) - Watermarked Image PSNR = 65.7 dB

Figure 5(b) - Recovered Watermark

Comparison-of-correlation based mid-band-DCT-Coefficients recovered watermarks under different attacks. K=15

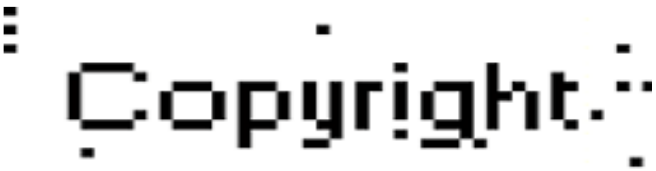

Figure 6(a) - 5% Gaussian Noise

Figure 6 (b) - 15% Gaussian Noise

Figure 6 (c) – JPEG Compression Q=50

Figure 6 (d) – JPEG Compression Q=20

4.2CDMA Spread-Spectrum in the wavelet domain

The following results were obtained for CDMA Spread-Spectrum in the wavelet domain based watermarking.
K = 2 with small watermark.

Figure 7 (a) - Watermarked Image PSNR = 68.1 dB

Figure7 (b) - Recovered Watermark

Comparison-of- CDMA Spread-Spectrum in the Wavelet Domain: recovered watermarks under different attacks.

Figure8 (a) - 15% Gaussian Noise

Figure 8 (b) - 50% Gaussian Noise

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

Figure 8 (c) – JPEG Compression Q=50

Figure 8 (d) JPEG Compression Q=20

4.3 Interpretation of Results

Mid-band DCT Coefficients

Results of the comparison of mid-band DCT coefficients were encouraging. We can observe that the technique works perfectly for unaltered images, with good visual quality of the watermarked image. The block size for each of the DCT-based techniques was kept constant at 8 x 8, in anticipation of JPEG compression. Better results could be obtained using larger block sizes at the expense of message capacity. The comparison DCT-coefficients method proved to be both moderately robust against Gaussian noise, and extremely robust against JPEG compression. Good recovery results were still possible with a watermarked image that had been compressed with a JPEG quality factor of 20. The watermarked image at this point was showing heavy JPEG artifacts, reducing quality of the attacked image beyond usability. By predicting which DCT coefficients would be altered using JPEG, an extremely high level of JPEG robustness can be achieved.

CDMA Spread-Spectrum in the Wavelet Domain

Due to its computationally efficient modeling of the HVS, the wavelet domain offers perhaps the most promising environment for robust watermarking. CDMA in the wavelet domain was first tested using the smaller message size, and then next using the normal message as per most of the other implementations. The algorithm seemed to have no problem retrieving the small watermark from the watermarked image with only minimal degradation of the cover image during embedding. Even with a minimal gain of k=2, the algorithm was still able to provide moderate robustness to Gaussian noise and JPEG compression. The recovered watermark was even recognizable under heavy degradation of the cover such as 50% Gaussian noise or JPEG compression with quality factor 20. While CDMA in the spatial domain degraded with increased image size, CDMA in the wavelet domain was able to encode the normal watermark, still with good results Robustness results using the normal message size were also positive. The watermark was able to survive moderate levels of Gaussian noise, while still be recognizable at detection. JPEG robustness faired even better, with the watermark still be recognizable after JPEG compression with quality factor 20. CDMA in the wavelet domain appears to show the most promise of the tested watermarking techniques. The algorithm described here is one of the most simplistic available in the wavelet domain, and yet the results are still excellent. These results tend to reinforce the common belief in wavelet domain as the most promising domain for digital watermarking [9].

Comparison of Computational Complexity

The algorithms were implemented in the most straightforward method possible and not the most computationally efficient. Furthermore, the results will not necessarily scale linearly over systems of varying architecture and speed. That being said, CDMA in the spatial domain was clearly the most computationally intensive, requiring twice the processing time of its closest competitor and an order of magnitude above the average. CDMA in the wavelet domain is an improvement over the spatial domain; however the processing requirements are still quite high. Also note the highly non-linear behavior of the two CDMA sequences with increasing message sizes. In the next few pages, a graphic illustration of the comparison of results amongst different watermarking techniques is made.

V.CONCLUSIONS

In this paper presented number of techniques for the watermarking of digital images, as well as touching on the limitations and possibilities of each. Although only the very surface of the field was scratched, it was still enough to draw several conclusions about digital watermarking. As per performance, transform domains are typically better candidates for watermarking then spatial domain, for both reasons of robustness as well as visual impact. Embedding in the DCT domain proved to be highly resistant to JPEG compression as well as significant amounts of random noise. CDMA in the wavelet domain is an improvement over the spatial domain; however the processing requirements are still quite high.

REFERENCES

1. M. D. Swanson, M. Kobayashi, and A. H. Tewfik, “Multimedia Data Embedding and Watermarking Technologies”, IEEE Proc. 86, (6), pp. 1064□1087, 1998.
2. F. Mintzer, W. Braudaway, and M. M. Yeung, “Effective and Ineffective Digital watermarks”, Proc. ICIP'97, Santa Barbara, CA, pp. 9□12, 1997.
3. A. Piva, M. Barni, F. Bartolini, V. Cappellini, “Threshold Selection for Correlation-Based Watermark Detection”, Proceedings of COST 254 Workshop on Intelligent Communications, L'Aquila, Italy, June 4-6, 1998.
4. M. G. Kuhn, “Stirmark”, available at http://www.cl.cam.ac.uk/~mgk25/stirmark/, Security Group, Computer Lab, Cambridge University, UK (E-mail: mkuhn@acm.org), 1997.
5. M. J. J. Maes and C. W. A. M. van Overveld, “Digital watermarking by geometric warping”, Proc. of the ICIP'98, Chicago, Illinois, 1998.
6. J. J. K. Ó Ruanaidh and T. Pun, “Rotation, scale and translation invariant digital image watermarking”, Proc. of the ICIP'97, vol. 1, pp. 536–539, Santa Barbara, California, 1997.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

7. J. J. K. Ó Ruanaidh, W. J. Dowling, and F. M. Boland, "Watermarking digital images for copyright protection", IEE Proc. Vision, Image and Signal Processing, 143(4), pp. 250–256, 1996.
8. A. Herrigel, J. Ó Ruanaidh, H. Petersen, S. Pereira, T. Pun, "Secure copyright protection techniques for digital images," Proc. of the 2nd Int. Information Hiding Workshop, Portland, Oregon, 1998.
9. H. Choi, H. Kim, and T. Kim, "Robust Watermarks for Images in the Subband Domain", Proc. of The 6th IEEE International Workshop on Intelligent Signal Processing and Communication Systems (ISPACS'98), Melbourne, Australia, pp. 168□172, 1998.
10. D. J. Fleet and D. J. Heeger, "Embedding Invisible Information in Color Images", ICIP '97, pp.523□535, Santa Barbara, California, 1997.
11. N.F. Johnson, S.C. Katezenbeisser, "A Survey of Steganographic Techniques" in Information Techniques for Steganography and Digital Watermarking, S.C. Katzenbeisser et al., Eds. Northwood, MA: Artec House, Dec. 1999, pp 43-75.
12. Kamran Ahsan, Deepa Kundur. Workshop Multimedia and Security at ACM Multimedia'02, December 6, 2002.
13. Emil Frank Hembrooke. Identification of sound and like signals. United States Patent, 3,004,104, 1961
14. ,quoted in" The first 50 years of electronic watermarking ".Ingemar J. Cox, Matt L. Miller, published in the Journal of Applied Signal Processing,IEEE, 2002.
15. 14. "USC-SIPI image database," available at http://sipi.usc.edu/services/database/Database.html.
16. Dr. M. A. Dorairangaswamy, "A Robust Blind Image Watermarking Scheme in Spatial Domain for Copyright Protection", International Journal of Engineering and Technology Vol. 1, No.3, August, 2009.
17. [A. Al-Haj, "Combined DWT-DCT Digital Image Watermarking", Journal of Computer Science3 (9): 740-746, 2007. [15] M. Calagna, H. Guo, L. V. Mancini and S. Jajodia, "A Robust Watermarking System Based on SVDCompression", Proceedings of ACM Symposium on Applied Computing (SAC2006),Dijon, France, pp. 1341-1347, 2006.
18. F. Cayre, C. Fontaine and T. Furon, "Watermarking security: theory and practice", Signal Processing, IEEE Transactions on, vol. 53, no. 10, pp. 3976–3987, Oct. 2005.
19. P. Taoaand and A. M. Eskicioglu, "A robust multiple watermarking scheme in the Discrete Wavelet Transform domain", Internet Multimedia Management Systems Proceedings of the SPIE, Volume 5601, pp. 133-144 (2004).
20. Pradhan, C., Rath, S., Bisoic, and A. K., "Non Blind Digital Watermarking Technique Using DWT and Cross Chaos", Journal of Procedia Technology, vol. 6, pp. 897- 904, 2012.
21. Keyvanpour, M., Bayat, F. M., "Robust Dynamic Block-Based Image Watermarking in DWT Domain", Journal of Procedia Computer Science, vol. 3, pp. 238-242, 2011.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)