Analytical Study of Watermarking Techniques

Mohamad Owais Raja, Tazeem A Khan, Junaid Geelani

Abstract: - The increasing amount of research on watermarking over the past decade has been largely driven by its important applications in digital copyrights management and protection. One of the first applications for watermarking was broadcast monitoring. In this paper presented LSB substitution and threshold-based correlation techniques, performance analysis on the basis of their various types of noises. In this analysis, Different image simulated using two watermarks techniques. We used simulation through using Matlab Simulator.

Keywords: Digital watermarking, LSB substitution, threshold based correlation

I. INTRODUCTION

Digital watermarking is the development of inserting a digital signal or blueprint into digital content. The signal, known as a watermark, can be used later to recognize the owner of the work, to authenticate the content, and to trace illegal copies of the work. There are dozens of different watermarking techniques that have been described in the literature during the last decade. In addition to that, each technique can usually be implemented with many modifications. Clearly, it would be an unwieldy task to try to compare all of them. Fortunately, the techniques can be roughly divided into groups depending on the procedure for watermark embedding. Only typical representatives selected from each group would be involved in the comparison study. 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. The results of tests are summarized and discussed.

II. TESTING METHODOLOGY

The performance is directly influenced by the watermark extraction statistics. Majority of watermarking schemes are based on thresholding a correlation between an extracted vector and a pseudo-random sequence. With decreasing threshold the probability of missed detections also decreases and the robustness increases. But at the same time, the rate of false detections will also increase. In this paper, we present to adjust the detection statistics so that the probability of false detections is less than reference value. For some watermarking schemes under simplified conditions one can actually derive the appropriate value of the threshold[3], or a set of numerical experiments can be done to estimate the probability distribution of the correlations. The strength is usually tested using typical image processing operations that can be divided into two groups: gray scale manipulations and geometric transformations [4].

Manuscript Received on August 2014.

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.

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]. 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. WATERMARK 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. LSB substitution however despite its simplicity brings a host of drawbacks. Although it may survive transformations such as cropping, any addition of noise or lossy compression is likely to defeat the watermark. An even better attack would be to simply set the LSB bits of each pixel to one ,fully defeating the watermark with negligible impact on the cover object. Furthermore, once the algorithm is discovered, the embedded watermark could be easily modified by an intermediate party. An improvement on basic LSB substitution would be to use a pseudo-random number generator to determine the pixels to be used for embedding based on a given "seed" or key [12]. Security of the watermark would be improved as the watermark could no longer be easily viewed by intermediate parties. The algorithm however would still be vulnerable to replacing the LSB's with a constant. Even in locations that were not used

Published By:
Blue Eyes Intelligence Engineering & Sciences Publication Pvt. Ltd.

for watermarking bits, the impact of the substitution on the cover image would be negligible. LSB modification proves to be a simple and fairly powerful tool for stenography, however lacks the basic robustness that watermarking applications require.

IV. SIMULATION RESULTS

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. Next, robustness evaluations were limited to testing against JPEG compression, the addition of Gaussian 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 Threshold-Based Correlation

The following results were obtained for threshold based correlation.

K = 5, block- size=16

Figure1 (A) Watermarked Image (PSNR = 94.0 dB)

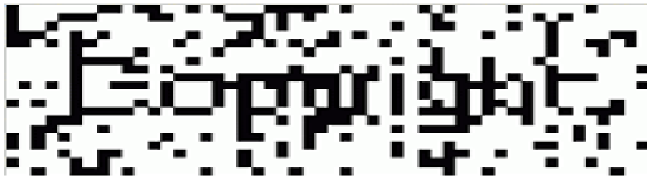

Figure 1(B) - Recovered Watermark

Threshold-Based Correlation K = 40 block size=16

Figure 2 (A) - Heavily Watermarked Image PSNR = 57.9 dB

Figure 2 (B) - Recovered Watermark

Threshold-Based Correlation Recovered watermarks

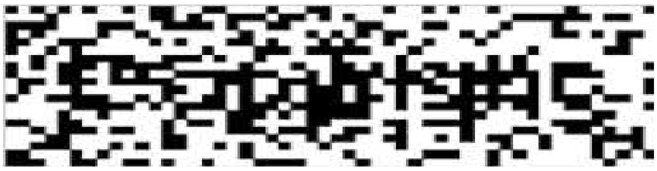

Figure 3 (A) - 5% Gaussian Noise (k = 5)

Figure 3 (B) - 5% Gaussian Noise (k =

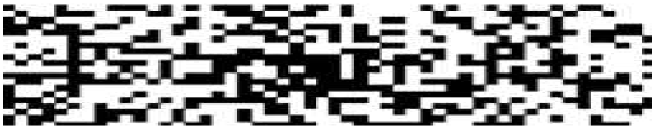

Figure 3 (C) - JPEG Compression Q=75 (k = 5)

Figure 3 (D) - JPEG Compression Q=75 (k = 40)

Comparison-Based Correlation K = 5 blocksize=16

Figure 4 (A) - Watermarked Image PSNR = 72.5 Db

Figure 4 (B) - Recovered Watermark

4.2 LSB substitution

Results from LSB substitution were as expected. The watermarked image shows little noticeable degradation, while the large watermark was recovered perfectly. The watermarked image is shown on next page in figure 14a. Not shown above is the large watermark created for the LSB embedding algorithm, which uses the normal watermark and titles it out to full image size. For our reference image, the boat image is used, as shown below in figure 5.

Published By:
Blue Eyes Intelligence Engineering & Sciences Publication Pvt. Ltd.

Figure 5 – Unwatermarked Boat Image (512 x 512 Pixels)

Figure 6 – Watermarked Boat Image PSNR= 102 dB

Figure 7 Recovered Watermark

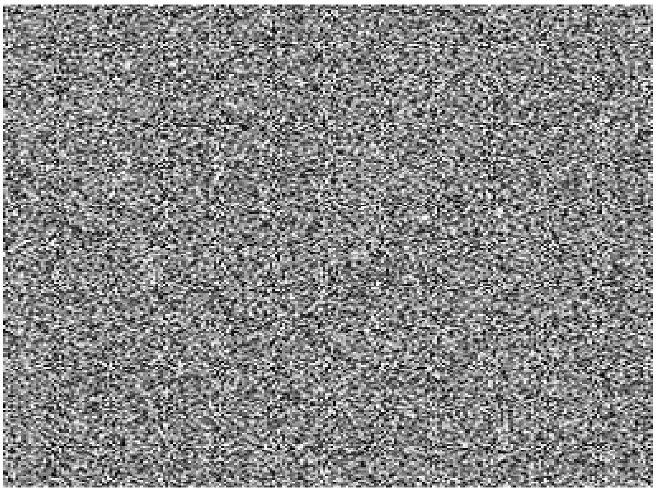

Figure 8 Recovered Watermarkafter Addition of 1% Gaussian Noise

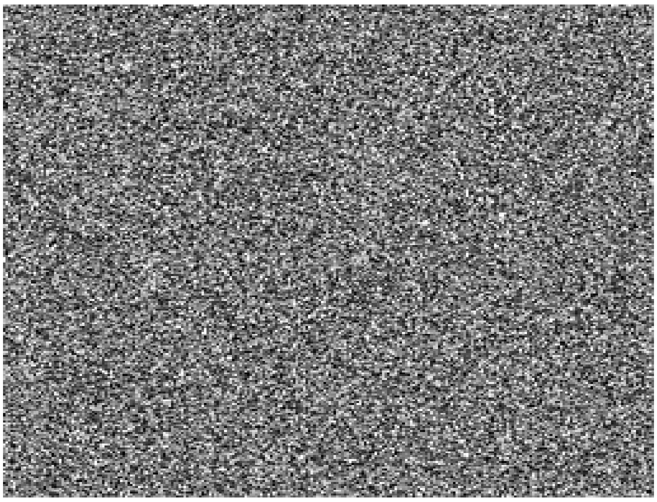

Figure 9 Recovered Watermark after JPEG Compression with Quality 95

4.3 Analysis

LSB Substitution

Results from LSB substitution were as expected. The watermarked image shows little noticeable degradation, while the large watermark was recovered perfectly although the watermark was recovered perfectly in the ideal case, the addition of any amount of noise, or compression of the image using JPEG fully destroys the embedded watermark, leaving nothing but noise. Even worse, the watermark can be removed with no perceivable change to the watermarked image. The message capacity of LSB embedding however is quite good, a 1:1 correlation with the size of the image.

Threshold-Based Correlation

The results of threshold-based correlation showed a vast improvement over LSB substitution in terms of robustness. Several parameters however must be discussed before we move on to results of this technique. A gain factor of k was chosen experimentally, however larger factors might be used for increased robustness at the expense of visual quality. Another issue with threshold-based techniques is the choosing of a suitable threshold for detection. One method is to store the correlation of each PN sequence and then use the mean of all the correlations as the threshold T. For watermarks with relatively equal numbers of zero's and ones, this technique should prove somewhat adaptive to a range of image types, as well as varying levels of noise. A final consideration is the size of the watermark being embedded. Use of a smaller watermark will allow larger blocks to be used, increasing the strength of correlation and thus system robustness. Although the watermark was not perfectly recovered, threshold-based correlation fares much better then LSB in the presence of noise and compression. Using a gain of 5, the watermark is still slightly distinguishable after light levels of noise and compression. As expected, increasing the gain to 40, improves the watermark's robustness significantly. The comparison-based watermark with gain 5 performed marginally better than even the threshold-based with gain 40; with less impact on the cover image. Robustness is improved as well in the comparison-based watermark. Again we see the comparison-based approach at a gain of 5 rivaling or even besting threshold-based with gain 40. Disadvantage of these block-

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

based techniques in relation to LSB embedding is that they are highly fragile to flips, crops and rotations. These transformations alter the coordinate systems of the image, making the task of matching up blocks in embedding and recovery quite difficult. The technique however should prove fairly resistant to contrast, brightness and any other sort of per-pixel transform.

V. CONCLUSIONS

In this paper investigate performance of watermarking techniques for digital images, as well as limitations and possibilities of each. LSB substitution is not a very good candidate for digital watermarking due to its lack of even a minimal level of robustness. LSB embedded watermarks can easily be removed using techniques that do not visually degrade the image to the point of being noticeable. Furthermore if one of the more trivial embedding algorithms is used, the encoded message can be easily recovered and even altered by a third party. It would appear that LSB will remain in the domain of steganography due to its tremendous information capacity. Threshold-based correlation showed an improvement over LSB substitution in terms of robustness.

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.

[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.