A Study on Spatial and Transform Domain Watermarking Techniques

Pooja Dabas
Computer Science & Engineering Deptt
P.D.M.College Of Engineering for Women

Kavita Khanna
Computer Science & Engineering Deptt
P.D.M.College Of Engineering for Women

ABSTRACT

Digital Image Watermarking is used for copyright protection of digital information. With the widespread of internet, the intellectual properties are accessible and manipulated easily. It demanded to have different ways to protect data. Digital watermarking provides a viable and promising solution. In this paper, we have described about the three different watermarking techniques (LSB, DCT, DWT) along with the various performance parameters required to evaluate the best technique out of them. This can help us to propose and implement new technique to achieve maximum robustness against various attacks.

General Terms

Digital Watermarking, Embedding, Extraction, Spatial Domain Technique, Transform Domain Technique.

Keywords

Digital Image Watermarking, Copyright Protection, LSB, DCT, DWT, Robustness, Performance Parameters, Attacks.

1. INTRODUCTION

Watermarking process is a sub-discipline of information hiding. Internet is the biggest network now days. This demanded maintenance of security [1] and privacy of data available on internet. Watermarking approach is used to make sure of the protection of the data. Watermarking is the pattern of bits inserted into a digital image, audio or video file, specifying the copyright information of data, such as author, owner etc. The actual bits representing watermark are scattered in data file in such a manner they cannot be detected or tampered by unauthorized person. Perceptual transparency, security, capacity, robustness, verifiability and payload of watermark are the important aspects or requirements for design of watermarking systems. Media [2] watermarking research is very active area and digital image watermarking is considered an interesting research area to act on.

Rest of the paper is organized as follows : the 2nd section gives brief introduction about the watermarking process, section 3rd include different types of techniques, section 4th describe about LSB technique, section 5th discusses about the DCT technique and 6th section describes about DWT technique. The 7th section deals about the parameters that can be used to calculate the performance of different watermarking techniques. Later, the conclusion is presented in section 8th.

2. WATERMARKING FRAMEWORK

Digital watermarking is the process of embedding information into a digital signal. It is used to verify the authenticity or identity of its owner [3]. A watermarking system is divided into three distinct steps: Embedding, Attack and Extraction. Figure 1, depicts the general framework of a digital watermarking.

2.1 Embedding

In embedding, an algorithm is used to combine watermark and host data. Watermark is embedded into the host data and a watermarked signal(data) is produced.

2.2 Attack

The output of embedding step, i.e. the watermarked signal is then transmitted, published or stored. Modification can be made to that signal, which is known as an attack [11]. Attack an attempt to remove or modify the watermark which is a threat to copyright protection application. Attacks can be done in different forms like lossy compression (resolution get diminished), cropping, adding noise, rotation etc.

2.3 Extraction

During watermark extraction**,** the watermark is extracted from watermarked image.

3. WATERMARKING TECHNIQUES

Watermarking techniques are broadly categorized into two types on the basis of working aspect i.e. the method used to embed the data. The types are as: Spatial Domain Technique and Transform Domain Technique.

3.1 Spatial Domain Technique

Spatial Domain Technique [13] is less complex with high payload. This type of technique cannot stand low pass filtering and the common attacks of images. Example: LSB (Least Significant Bit), it is implemented by modifying the least significant bit of the image pixel data.

3.2 Transform Domain Technique

In this technique, the transform coefficients are modified rather than the pixel value [4]. To detect watermark, inverse transform is used. Example- DCT (Discrete Cosine Transform), DWT (Discrete Wavelet Transform), DFT (Discrete Fourier Transform) etc. are common transform techniques.

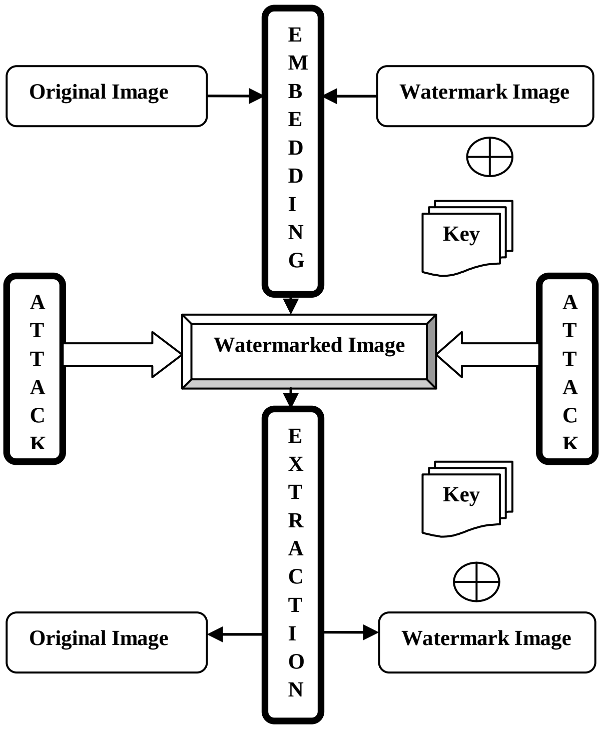

Figure 1: Digital Watermarking Framework

4. LSB

Least Significant Bit [16] is a spatial domain technique which is a very simple and straight forward. It takes less time to embed image (watermark).The watermark is embed into the least significant bits of the original image. This technique has many drawbacks, even simple attacks can remove or destroy watermark but sometime it may survive against some of the transformations. Various improvements on LSB substitution has also been proposed in recent times like embed watermark at single bit rate, multi bit rate or using a pseudo-random number generator. Pixel can also be selected with help of key. Any addition of noise [12] and performing lossy compression can easily degrade the image quality or remove or destroy or disrupt watermark. It lacks the basic robustness. In case, if the algorithm is discovered, it becomes easy for attacker to change or remove watermark.

5. DCT

Discrete Cosine Transform [9] is a very popular transform domain watermarking technique. In this technique, an image is divided into different frequency band as low (F_L), medium (F_M) and high (F_H). It allows selecting the band to embed data or watermark into the image. Figure 2 represents Discrete Cosine Transform Frequency 8X8 block , where low frequency band F_L appears at upper left corner, if modification performed here, the watermark can be caught by human eyes. High frequency band F_H lies at lower and right edges, if modification performed here, it may lead to local distortion along with edges. Medium frequency band F_M is considered best region for modification, it cannot affect the image quality. Thus, a middle frequency band is the best band to embed watermark. DCT is a faster technique [17], with complexity O (n log n). This technique can survive attacks like compression, noising, sharpening and filtering. This technique is considered to be better than spatial domain watermarking technique.

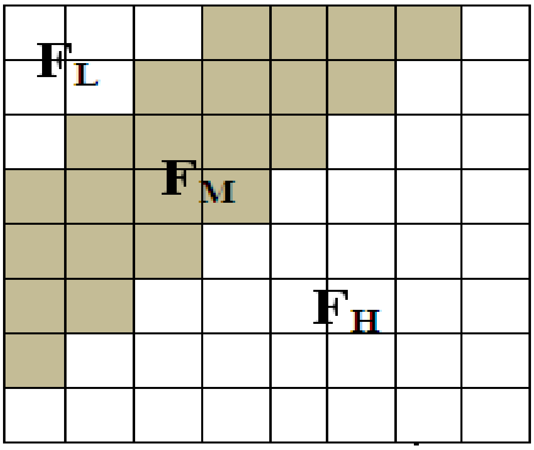

Fig 2: Discrete Cosine Transform Frequency 8X8 block

6. DWT

Discrete Wavelet Transform [5] is also a transform domain watermarking technique. In this technique the host image is divided into four different components as: LL (Lower resolution component), HL (Horizontal component), LH (Vertical component) and HH (Diagonal component). This breaking process can be repeated to have multi-level wavelet components like 2-Level, 3-Level etc. Figure 3, is a 2- Level Discrete Wavelet Transform. DWT needs large computation. The embedding time and extraction time of DWT is greater then LSB and DCT watermarking technique. It has a very little effect on quality of the image. But it is said to be more accurate model aspects of HVS as compared to DCT. Robustness can be increased using DWT watermarking technique. It has great spatial localization and multi-resolution as its characteristics.

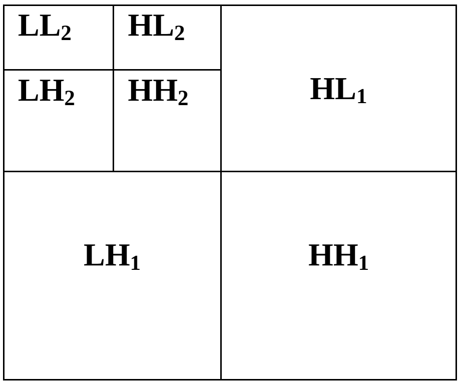

Fig 3 : 2- Level Discrete Wavelet Transform

7. PERFORMANCE ANALYSIS

The performance analysis [7] deals with various parameters to be calculated to check the robustness of the technique. The main goal of watermarking is to resist both geometric distortion and signal processing attacks. Since, no watermarking algorithm resists all the attacks. But, still one can find better technique which will give more robust watermark by performing various calculations. Aim of attack is to impair detection of watermark or destroy the embedded watermark. Attacks can be removal attacks, geometrical attacks, cryptographic attacks and protocol attacks. Robustness against attacks is an important aspect for watermarking schemes.

7.1 Execution Time

It is one of the important parameter to compute the working and performance of the watermarking algorithms in relation with time. It measure the amount of time required in embedding process and extraction process of watermark. To measure of execution time CPU cycles are used. General formulae can be used as:

Start_Time = CPUtime
Time_Taken = CPUtime – Start_Time

7.2 Peak Signal to Noise Ratio

It is used to measure the imperceptibility of a watermarked image, i.e. similarity between the original image and watermarked image. It can also be used to compare original watermark with the extracted watermark. It is expressed as quality measure. Higher the PSNR value higher is the security. It itself uses Mean Square Error (MSE) for its computation. PSNR can be represented as:

$$PSNR = 10 \log_{10} \left(\frac{255^2}{MSE} \right)$$

PSNR is the ratio between maximum possible power of a signal and the power of corrupt noise. Here 255 is maximum possible pixel value (of the cover image). MSE is computed as:

$$MSE = \frac{\sum^{N}_{i=1} \sum^{N}_{j=1} (X(i,j) - X_w(i,j))^2}{N^2}$$

Where, N represents number of rows and columns (here considered same value), X(i,j) is the original image pixel value and X_w (i,j) is the watermarked image pixel value.

7.3 Bit Correct Ratio

The Bit Correct Ratio (BCR) represents the ratio of correct extracted bits to the total number of embedded bits. Some attacks are applied to the watermarked images to check for the robustness of the techniques. After every attack the BCR is computed of the extracted watermark. It is expressed using formula:

$$BCR = \frac{100 \sum^{L-1}_{n=0}}{L} \begin{cases} 1, & W'_n = W_n \\ 0, & W'_n \neq W_n \end{cases}$$

Where, L represents watermark length, W_n represents the nth bit of the original watermark and W'_n represents the nth bit of the recovered watermark.

7.4 Normalized Cross Correlation

It is used to measure the similarity between the cover image and the watermarked image as well as original watermark and recovered watermark. Higher the value of NCC will result in better technique. It is calculated by the formula:

$$NCC = \frac{\sum i \sum j \, [\, I(i,j) - I_w(i,j) \,]}{\sum i \sum j \, [\, I(i,j) + I_w(i,j) \,]}$$

Where, I(i,j) is the original image pixel value and I_w (i,j) is the watermarked image pixel value.

7.5 Similarity Ratio

Similarity Ratio (SR) is the comparison between original watermark and extracted watermark. It is represented as:

$$SR = \frac{S}{S + D}$$

Where S is the number of matching pixels value and D is the number of different pixel values.

7.6 Payload

Payload [21] or capacity is also one the important performance parameter because it has a direct impact on the robustness of the image. It is the amount of information i.e. the amount of watermark that can be hidden in to the original image without deteriorating the quality of the original image. The size or amount of data is termed in bits or pixel value.

7.7 Structural Similarity Index Measure

Structural Similarity Index Measure (SSIM) is the used to measure similarity between original image and watermarked image or original watermark and recovered watermark. It is said to be improved way to check for the robustness of the technique on methods like PSNR and MSE. Its value exit between the decimal values 1 and -1. If SSIM is equal to 1, it means the images are identical sets. It is calculated as:

$$SSIM\ (x.\ y) = \underline{(\, 2\mu_x\, \mu y + C_1 \,)\, (\, 2\sigma_{xy} + C_2 \,)}$$

$$(\mu_x^2 + \mu_y^2 + C_1)(\sigma^2_x + \sigma^2_y + C_2)$$

Where, μ_x is average of x , μ_y is average of y, σ^2_x is the variance of x, σ^2_y is the variance of y, σ_{xy} is the covariance of x & y , C_1 and C_2 are the two variable to stabilize the division with weak denominator.

7.8 Other Parameters

Various other parameters like SNR (Signal to Noise Ratio), BER (Bit Error Ratio), NAE (Normalized Absolute Error), MAE (Mean Average Error), UIQI (Universal Image Quality Index), MAE (Mutual Information) and SC(Structural Content) can also be used to check the robustness.

8. CONCLUSION

The comparison study of different watermarking technique is performed in this paper. A great scope exists for more improvements. By studying these techniques we can conclude that LSB is simplest among all but cannot be considered as a good technique. DCT domain based technique is more robust than LSB and can sustain various types of attacks. Same as DWT domain based technique also proved to be better than LSB. But this technique has more computational requirements. The combination of DCT and DWT domain can be one of the future aspects to have more secured watermarking. Geometric, protocol and various other attacks have great influence on the imperceptibility and robustness of watermarked digital images. Various performance evaluating parameters stated guide us, to know about better robust techniques.

9. REFERENCES

[1] C. S. Lu, Multimedia Security: Steganography and Digital Watermarking for Protection of Intellectual Property, Idea Group Publishing, 2005..

[2] Sin-Joo Lee and Sung-Hwan Jung, "A Survey of Watermarking Techniques Applied to Multimedia", ISIE 2001.

[3] Petitcolas Fabien A., Anderson Ross J., Kuhn Markus G., "Information Hiding – A Survey", Proceedings of IEEE, Special issue on protection of multimedia content, pp 1062-1078,July 1999.

[4] Bijan Fadeena and Nasim Zarei,"Hyprid DCT-CT "Digital Image Adaptive Watermarking", 3rd International Conference on Advances in Database, Knowledge, an data Applications, IARIA 2011.

[5] Tay P., Havlicek J.P., "Image Watermarking using Wavelets". IEEE, pp 258-261, 2002.

[6] H. Inoue, A. Miyazaki and T. Katsura, "An Image Watermarking Method Based on the Wavelet Transform", IEEE Conf. on Image Processing, Vol. 1, pp. 296-300, 1999.

[7] Taha El Areef, Hamdy S. Heniedy, S . Elmougy, and Osama M. Ouda, "Performance Evaluation of Image Watermarking Techniques", Third International Conference on Intelligent Computing and Information Systems, Faculty of Computer & Information Sciences, ICICIS 7002 ,March 15-18, 2007, Cairo.

[8] S. Voloshynovskiy, S. Pereira, T. Pun, University of GenevaJ.J. Eggers and J.K. Su, University of Erlangen-Nuremberg," Attacks on Digital Watermarks: Classification, E(1)stimation-based Attacks and Benchmarks ", 2001.

[9] I. Cox, J. Kilian, T. Leighton, and T. Shamoon, , "Secure spread spectrum watermarking for multi-media," IEEE Trans. on Image Processing 6 (1997), 1673-1687.

[10] Baisa L. Gunjal , R.R. Manthalkar "An Overview Of Transform Domain Robust Digital Image Watermarking Algorithms", Journal of Emerging Trends in Computing and Information Sciences, 2010-11.

[11] Craver, S., N. Memon, B.L. Yeo and M.M. Yeung, "Resolving rightful ownerships with invisible watermarking techniques: Limitations, attacks and implications". IEEE J. Selected Areas Commun, 1998.

[12] J. L., Dugelay, S. Roche, C. Rey, G. Doërr, "Still-image watermarking robust to local geometric distortions," IEEE Trans. on Image Proc., vol. 15, no. 9, pp. 2831-2842, 2006

[13] Mustafa Osman Ali , Elamir Abu Abaida Ali Osman, Rameshwar Row, Electronics & Communication Engineering Dept., Biomedical Engineering Dept., University College of Engineering, Osmania University, "Invisible Digital Image Watermarking in Spatial Domain with Random Localization", International Journal of Engineering and Innovative Technology (IJEIT), Volume 2, Issue 5, November 2012

[14] S Jayaraman, S Esakkirajan, and T Veerakumar: Digital Image Processing. McGraw-Hill, 2009.

[15] Mustafa Osman Ali, and Rameshwar Rao., " Fundamentals of Digital Image Watermarking: an Overview". International Conference on Information and Communication Technology. pp. 64–67, Oct. 2011.

[16] D. Samanta, A. Basu, T. S. Das, V. H. Mankar, Ankush Ghosh, Manish Das and Subir K Sarkar, SET Based Logic Realization of a Robust Spatial Domain Image Watermarking," Proc. in 5th International Conference on Electrical and Computer Engineering-ICECE 2008, Dhaka, Bangladesh, pp. 986-993, Dec. 2008.

[17] J.R. Hemandez, M. Amado, "DCT domain watermarking techniques for still images as detector performance analysis and a new structure," in IEEE Transactions on Image Processing, 2000, vol. 9, pp. 55-68.

[18] Lee, G. J., Yoon, E. J. and Yoo, K. Y. (2008), " A new LSB based Digital Watermarking Scheme with Random Mapping Function", in2008 IEEE DOI 10.1109/UMC.2008.33

[19] S. Z. Yu, "A color image-adptive watermark based on wavelet transform," in Computer Simulation, 2006, vol. 23, pp. 132-134.

[20] C. C. Chang, J. Y. Hsiao, and C. S. Chan, "Finding optimal LSB substitution in image hiding by using dynamic programming strategy", Pattern Recognition, Vol. 36, No.7, 2003, pp.1583–1595.

[21] S. Shefali and S. M. Deshapande, "Mathematical Model for Improved Capacity Estimations for Data Hiding Techniques under Lossy Compression," in Proceedings of the 2nd IMT-GT Regional Conference in Mathematics, Statistics & Applications, Malaysia , 2006.

[22] AI-Gindy , H. AI-Ahmad, R Qahwaj, and A. Tawfik, "A novel blind Image watermarking technique for colour RGB images in the DCT domain using green channel "in Mosharaka International Conference on Communications. Computers and Applications (MIC-eCA 2008). , Amman, Jordan, 2008 .