ISSN No. 0976-5697

Volume 3, No. 3, May-June 2012

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A Comparision and Survey of Invisible and Visible Watermarking with Correctness Measures of Various Attacks

Y. Arockia Raj
Assistant Proffessor, Department of Computer Science and Engineering,
PSNA College of Engineering and Technology,
Dindigul, Tamil Nadu, India.
y.arockiaraj@gmail.com

Abstract: The major growth of information technology is based on the growth of computer networks. The computer network diminished the entire global in a nutshell, via the internet and the intranet capabilities. In the recent year, communicating information within authenticated groups in the text, image and video formats are highly unavoidable one. And in the same manner, there are more possibility that the communicated information to be hacked by the anonymous hacker. The hacker may be passive or active; it is highly risk for many engineering applications like military network. Hence, digital watermarking is merged to rectify the above pitfalls. Watermarking techniques developed for images are mainly classified into visible and invisible approaches. The study further analyses the modern digital watermarking system.

***Key words*:** Providing additional information, Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Discrete Fourier Transform (DFT), Peak Signal to Noise Ratio (PSNR), sliding square window containing

I. INTRODUCTION

Electronic watermarking is a new research area, combining aspects of digital signal processing, cryptography, statistical communication theory and human perception[1]. It aims to embedding an additional data into the original content in a way that is difficult to remove and to identify. Principal applications of electronic watermarks are in copyright enforcement, automatic metering and monitoring of asset usage in multi-media applications, piracy tracing and in providing additional information, such as image captions.

A watermark is a perceptually non-obstructive mark embedded in an image, audio or video clip or other multimedia asset[3]. A watermark can carry additional information, for instance about the source and copyright status of a document or its intended recipient, its rights and restrictions.

Many research efforts over the past decade have enabled digital watermarking to establish itself as a potential solution for the protection of ownership rights and policing information piracy of multimedia elements like images, audio and video[4]. Digital watermarking is defined as a process of embedding data (watermark) into a multimedia object to help to protect the owner's right to that object. The embedded data (watermark) may be either visible or invisible. While the visible methods provide means for overt assertion of ownership with logos, the invisible methods provide covert protection of these rights.

In visible watermarking of images, a secondary image (the watermark) is embedded in a primary (host) image such that watermark is intentionally perceptible to a human observer whereas in the case of invisible watermarking the embedded data is not perceptible, but may be extracted/detected by a computer program. The Fig. 1 shows the visible and invisible watermarking in Lena image with watermark logo.

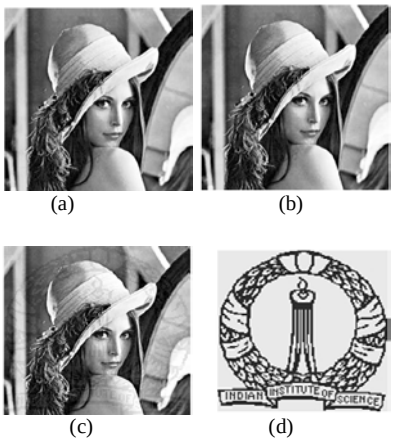


Figure 1: Visible and Invisible watermarking Original Imageinvible watermarkVisible Watermarking Watermarking logo

The requirements for watermarking methods include:

a. Erasing the watermark should be technically difficult. Methods should be robust against attackers knowing the watermarking algorithm but not the key[5]
b. Replacing the watermark by another watermark should be a difficult task[6]
c. The watermarking scheme should be robust to transmission and storage imperfections such as compression, noise addition, format conversion, bit errors; signal processing objectives such as noise reduction, filtering
d. It should be robust against typical attacks
e. It should also be robust against colluding pirates who combine multiple versions of the same content that are stamped with different watermarks
f. The watermark should be non-obstructive and not annoying to authenticated users

II. MATERIALS AND METHODS

For example, there is a trend to move from conventional libraries to digital libraries. In the digital libraries images and texts are made available through the internet for scholarly research. At the same time care is taken to prevent

the unauthorized use of the images commercially[7]. In some cases the observer is encouraged to patronize the institution that owns the material. To satisfy both these needs simultaneously the owner needs to use visible watermarking. Visible watermarking is a type of digital watermarking used for protection of publicly available images. In visible watermarking, IBM's Vatican Library project (Mintzer, 1996) is a significant contribution. Some of the desired characteristics of visible watermarks are:

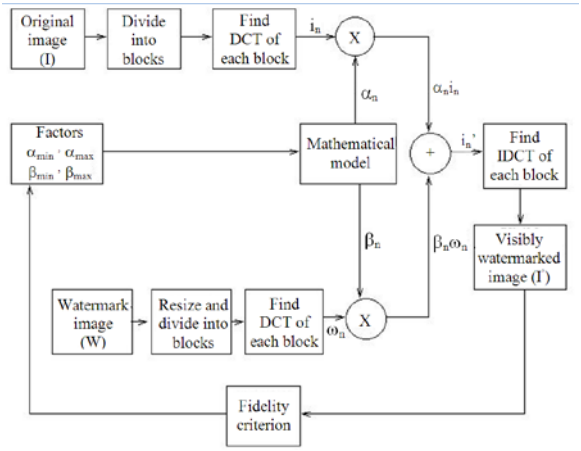


Figure 2: Visible watermarking process using DCT

a. A visible watermark should be obvious in both color and monochrome images[8]
b. The watermark should be spread in a large or important area of the image in order to prevent its deletion by clipping
c. The watermark should be visible yet must not significantly obscure the image details beneath it
d. The watermark must be difficult to remove; removing a watermark should be more costly and labor intensive than purchasing the image from the owner
e. The watermark should be applied automatically with little human intervention and labor[8]

Most of the recent studys are using different types of transformation methods for embedding the watermarks. The transformation techniques are inspired by methods of information coding and image compression[9]. The watermark is embedded into the cover image using the Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Discrete Fourier Transform (DFT). The process of visible watermarking using DCT is shown in the Fig. 2. The effective and efficient watermarking process consists of the following two distinct phases:

a. A statistical image is synthesized from a perceptually important sub image of the host image and
b. A compound image is created by fusing the input logo and synthetic statistical image[10]

A. Invisible Watermarking: Invisible watermarks have an advantage over visible watermarks, in that their location may be unknown. A common practice is to distribute the watermark (or watermarks) across the entire image. This provides some protection against cropping attacks.

However, the less perceptible a watermark is, it may be more vulnerable to manipulation. Assume an image (I) is composed two types of data based on the human visible threshold. These types are visible data (v) and invisible data (w)[11]. Thus, an image can be defined as I = v + w. To further define these types, any manipulation to (v) will result is noticeable distortion in the image. Modifying (w) will not be noticeable. The size of (w) is available to both the owner and attacker.

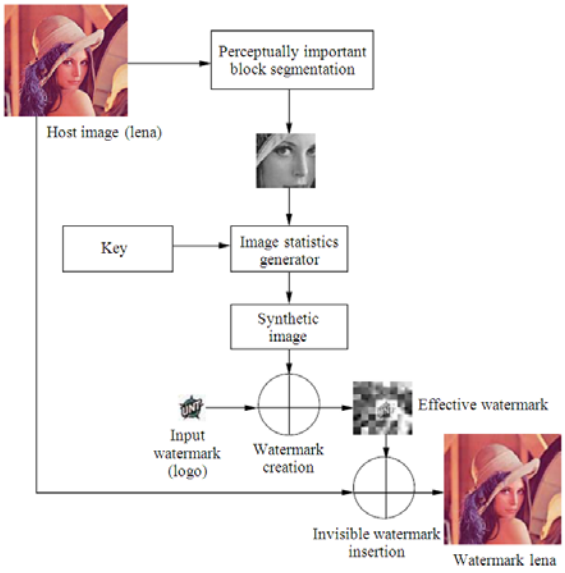


Figure 3: Invisible watermarking process

Since (w) remains imperceptible, there exist some (w') such that I' = v + w' and there is no perceptible difference between I and I'. An attack may be to replace, remove, or distort (w). One such attack described in (Petitcolas *et al*., 1998) discusses adding illicit watermarks as means to counterfeit valid watermarks. If information is added to some media such that the added information cannot be detected, then there exists some amount of additional information that may be added or removed within the same threshold, which will overwrite or disable the embedded information. If the attacker is intent on disabling the watermark, this can be easily done (Johnson and Jajodia, 1998).

Invisible watermarking was initiated by the research teams of (Craver *et al*., 1998; Cox *et al*., 1996). Though invisible watermarking techniques helped in making the watermark imperceptible to human eye and less prone to attacks, serious challenges to protect the embedded watermark against different types of attacks still persist. The invisible watermarking process is shown in the Fig. 3. The invisible watermark algorithm is described below:

a. Divide the host image into an integral number of M ×N blocks (after necessary image extensions.)
b. Choose the blocks in perceptually the most important region of the host for the generation of the synthetic image[11]
c. Obtain DCT coefficients for the individual blocks of the host and compute the standard deviations of the significant DCT coefficients over the sample space of the host image blocks
d. Synthesize a statistical image (in DCT space) of the same size as the above said sensitive area of the image
e. Choose an input logo of smaller size by scaling down for superposition on the synthetic image (ws) so generated. Divide it into M × N pixel size blocks and obtain its block-wise DCT coefficients (wc's)
f. Fuse this in a less sensitive area of the synthetic image using any DCT based visible watermarking algorithm. This actually involves determination of two block-specific parameters αk and βk indicating the proportions

of the synthetic image and the input watermark required for effective fusion. The position key determining the selection of DCT coefficients for the synthetic image generation and the seed used by the random variates during the statistics generation are saved for the use during authentication. To create a compound watermark from a user given color logo, each band of the color logo is treated as of the gray scale logo and finally stitched together to generate a color compound watermark. The DCT is suit well in the VLSI design, therefore optimal VLSI design also proposed in many studys. One such study is a dual voltage design for DCT proposed by saraju *et al.* (2006)

III. RESULTS

A. Contrast: A block which has high level of contrast with respect to the surrounding blocks attracts the human eye's attention and hence is perceptually more important.

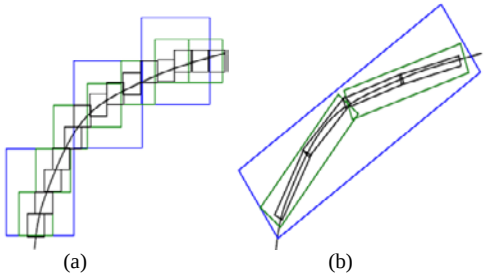
B. Location: According to the center-quarter of an image is perceptually more important than other areas of the image. So, we concentrate our focus at the central-quarter of the image.

C. Edginess: A block which contains prominent edges captures the attention of the human eye.

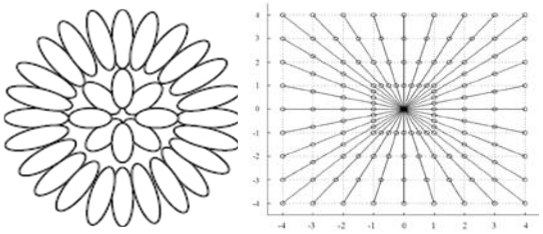
D. Texture: A highly textured block is less sensitive to noise. Modification inside a highly textured block is unnoticeable to human eye[12]. In order to determine the sub-image of interest, the host image is divided into M × N blocks and a sliding square window containing NB number of such blocks in both the horizontal and vertical directions (a tentative sub-image) is considered. The sliding window slides across the image and computes a quantitative Measure (M) for each one of the influencing factors at every location.

The effectiveness of the watermarking is measured in terms of probability. The probabilities of incorrect detections are expressed in terms of the watermark-to-image power ratio, showing a significant similarity in the problem of detecting watermarks and that of receiving weak spread-spectrum signals over a radio channel with strong interference. The Peak Signal to Noise Ratio (PSNR) is used to evaluate the image quality. Various attack types in watermarking with its PSNR are discussed in the Table 1.

The wavelet transforms, which is applied widely in various tasks of image processing, has some pitfalls such as it fails to represent objects that contains randomly oriented edges and curves. The wavelet transform is optimal only for line singularities[13]. The Gabor filters are found to perform better than wavelet transform in representing textures and retrieving images due to its multiple orientation approach. However, due to the loss of spectral information in Gabor filters they cannot effectively represent images.



(a) (b)



(c) (d)

Figure 4: Wavelet, Ridgelet and Curvelet Wavelet Ridgelet curvelet with scale 2 Curvelet with polar representation

Table 1: Attack type and correctness measure

Attack type	Restored Image Probability (%)	Extracted Watermark	Correctness (PSNR)
No Attack	Infinity	38.02	99.6
JPEG Compression	39.98	24.44	75.7
Gaussian Blurred	43.22	29.50	98.8
White noise	42.95	27.10	91.8

Therefore, the Curvelet transform is developed to overcome the limitations of wavelet and Gabor filters to achieve a complete coverage of the spectral domain and to capture more orientation information. Curvelets are band-limited complex-valued functions, few examples of curvelet transform was shown in the Fig. 4. In order to achieve higher level of efficiency, the curvelet transform is implemented in the frequency domain.

The curvelet and the image are transformed and multiplied in the Fourier frequency domain. Then the product is applied with inverse Fourier transform to obtain the curvelet coefficients[15].

The process can be described as:

Curvelet transform = IFFT

[FFT(Curvelet) × FFT(Image)]

where, the FFT means for Fast Fourier Transform and the IFFT means for Inverse FFT.

IV. DISCUSSION

Jean-Luc *et al*. (2002) proposed curvelet for image de-noising, in which the author proposes curvelet using ridgelet transform as one of the components. In this study, the author applied digital transforms for de-noising of images which is embedded in white noise. The author applied various techniques like wavelet, threshold methods, tree based Bayesian posterior mean methods and curvelet. The performance of curvelet is proven result than the other methods. In addition to these watermarking techniques, genetic algorithms also proposed. Chin-Chin (2011) proposes a tiny genetic algorithm with singular value decomposition for digital watermarking to achieve robustness and Vellasques *et al*. (2011) proposed particle swarm optimization technique for watermarking. In chandramohan et al (2008, 2010, 2011) ant colony optimization is proposed and reviewed, the ACO is an optimization technique which is also applied for digital image processing.

Security is also important aspect for digital watermarking. The research in security and authentication receives higher focus in the recent years. Sanjay *et al.* (2011) proposed a tamper protection for digital watermarking using chaotic system.

V. CONCLUSION

In this study, the visible and invisible watermarking techniques are explained and the research on various watermarking is analyzed. Then few digital watermarking techniques which are already implemented in different domains are discussed. The application of visible and invisible watermarking are explained with an example. The key terminology regarding the image watermarking is also discussed. The aim of this study is to guide the researcher about the various research opportunities in the watermarking field of study.

VI. REFERENCES

[1]. Chandra Mohan, B. and Baskaran, R. 2010, Improving network performance by optimal load balancing using ACO based Redundant Link Avoidance algorithm, International Journal of Computer Science Issues, 7, 3, : 27-35

[2]. Chandra Mohan, B. and Baskaran, R. 2011, Reliable Transmission for Network Centric Military Networks, European Journal of Scientific Research, 50, 4: 564-574

[3]. Chandra Mohan, B. and Baskaran, R. 2011, Reliable Barrier-free Services in Next Generation Networks, Lecture Notes in Computer Science, Second International Conference on Advances in Power Electronics and Instrumentation Engineering, PEIE 2011, Springer-Verlag Berlin Heidelberg, CCIS 148 : 79-82

[4]. Chandra Mohan, B. and Baskaran, R. 2011, Survey on Recent Research and Implementation of Ant Colony Optimization in Various Engineering Applications, International Journal in Computational Intelligent Systems, 4, 4:566-582

[5]. Chandra Mohan, B. and Baskaran, R. 2011, Energy Aware and Energy Efficient Routing Protocol for Adhoc Network using Restructured Artificial Bee Colony System, HPAGC 2011, Springer-Verlag Berlin Heidelberg, CCIS 169 : 480-491

[6]. Chandra Mohan, B., Sandeep, R. and Sridharan, D. 2008, A Data Mining approach for Predicting Reliable Path for Congestion Free Routing using Self-Motivated Neural Network, Studies in Computational Intelligence, Springer-verlag, 149 : 237-246

[7]. Chih-Chin, L., 2011. A digital watermarking scheme based on singular value decomposition and tiny genetic algorithm. Digital Signal Processing, 21: 522-527.

[8]. Cox, I.J., J. Kilian, T. Shamoon and T. Leighton, 1996. Secure spread spectrum watermarking of images, audio and video. Proceeding of the IEEE International Conference Image Processing, 3: 243-246

[9]. Craver, S., N. Memon, B. Yeo and N.M. Yeung, 1998. Resolving rightful ownerships with invisible watermarking techniques: Limitations, attacks and implications. IEEE J. Selected Areas Communi., 16: 573-586.

[10]. Jean-Luc, S., J.C. Emmanuel and L.D. David, 2002. The curvelet transform for image denoising. IEEE Trans. Image Proc., 11: 670-684.

[11]. Johnson, N.F. and S. Jajodia, 1998. Steganalysis of images created using current steganography software. Proceeding of the 2nd International Workshop (IH'98), Proceedings. Lecture Notes Comp. Sci., 1525: 273-289.

[12]. Mintzer, F., 1996. Towards online worldwide access to vatican library materials. IBM J. Res. Develop., 40: 139-162.

[13]. Petitcolas, F., R. Anderson and M. Kuhn, 1998. Attacks on copyright marking systems. Proceeding of the 2nd International Workshop (IH'98), Proceedings. Lecture Notes Com. Sci., 1: 218-238.

[14]. Sanjay, R. and R. Balasubramanian, 2011. A chaotic system based fragile watermarking scheme for image tamper detection. Int. J. Electr. Communi., 65: 840-847.

[15]. Saraju, P., N.R. Mohanty and B. Karthikeyan, 2006. A Dual Voltage-Frequency VLSI Chip for Image Watermarking in DCT Domain. IEEE Trans. Circuits Syst. II: Express Briefs, 1-5.

[16]. Vellasques, E., S. Robert and G. Eric, 2011. A high throughput system for intelligent watermarking of bi-tonal images. Soft Comput. J., DOI: 10.1016/j.asoc.2011.05.038.

EXAMPLES OF RELATED PUBLISHED MATERIAL

[17]. Malik F. Alamaireh, 2007. A Main Object-oriented Projective Invariant Image Watermarking Approach. American Journal of Applied Sciences, 4: 405-409. **DOI:** 10.3844/ajassp.2007.405.409.

[18]. Mehemed B. Aliwa, Tarek E. El-Tobely, Mahmood M. Fahmy, Mohamed E.S. Nasr and Mohamed H.A. El-Aziz, 2010. A New Novel Fidelity Digital Watermarking Based on Adaptively Pixel-Most-Significant-Bit-6 in Spatial Domain Gray Scale Images and Robust. American Journal of Applied Sciences, 7: 987-1022. **DOI:** 10.3844/ajassp.2010.987.1022.

[19]. T. Al-Khatib, A. Al-Haj, L. Rajab and H. Mohammed, 2008. A Robust Video Watermarking Algorithm. Journal of Computer Science, 4: 910-915. **DOI:** 10.3844/jcssp.2008.910.915.

[20]. Banshidhar Majhi and Hasan Shalabi, 2005. An Improved Scheme for Digital Watermarking Using Functional Link Artificial Neural Network. Journal of Computer Science, 1: 169-174. **DOI:** 10.3844/jcssp.2005.169.174.

[21]. Kevin Curran, Xuelong Xi and Roisin Clarke, 2005. An Investigation into the Use of the Least Significant Bit Substitution Technique in Digital Watermarking. American Journal of Applied Sciences, 2: 648-654. **DOI:** 10.3844/ajassp.2005.648.654.

[22]. Ababneh M.F. Mohammad and Naseem M. Asad, 2006. An Optimization Approach for Selecting Blocks of Embedding Process in Robust Watermarking System . Journal of Computer Science, 2: 114-117. **DOI:** 10.3844/jcssp.2006.114.117.