International Journal of Research and Development in Applied Science and Engineering (IJRDASE)
ISSN: 2454-6844

Genetic Algorithm based High Quality Image Watermarking using Multi Resolution Wavelet Transform

Smriti Upadhyay
Computer Science & Engg. (S/W Engg.),
BBD University, Lucknow, India
smriti.neetu@gmail.com

Kiran Jain
Computer Science & Engg.
BBD University, Lucknow, India
kiranc1975@gmail.com

***Abstract*- In the modern world, multimedia applications are becoming increasingly significant . The tremendous growth of multimedia data of these applications, particularly over the web has increased the demand for protection of copyright. Digital watermarking is much more acceptable as a solution to the problem of copyright protection and authentication of multimedia data while working in a networked environment. In this work a DWT based watermarking scheme is proposed. Wavelet transform is used because it has a number of advantages over other transforms, such as DCT. It has multi-resolution hierarchical characteristics, and lower resolution embedding and detection which are computationally inexpensive. The presentation of the image because of the hierarchical multi-resolution properties of the transformation is well-suited for applications where the multimedia data is transmitted regularly, as such in the application of video systems, or applications in real time. In this research work, we have used genetic algorithm, to optimize the watermark embedding inside original image. The fitness function used is the function of PSNR values. The perpetual aspect of the watermark is found to be relatively satisfactory. A number of images are taken and the algorithm is tested on these images.**

Keywords*-- *DCT, DWT, Genetic Algorithm, PSNR, Watermark.

1. Introduction:

Data Hiding or Steganography offers an essential alternative to image integrity and authenticity problem. It is a kind of data hiding technique that provides another way of security protection for digital image data. Unlike utilizing a particular cipher algorithm to protect secret data from illicit access, the purpose of steganography is to embed secret data in preselected meaningful images, called cover images, without creating visually perceptible changes to keep an invader unaware of the existence of the secret.

Digital data hiding is a multidisciplinary research area involving theory of communications, signal processing, multimedia coding, information theory, cryptography and computer science etc .Soft computing is one sub branch of computer science which may be used to achieve tractable, robust, low cost, optimal and adaptive solutions in data hiding problems. Fuzzy Logic (FL), Rough Sets (RS), Artificial Neural Networks (ANN), Genetic Algorithms (GA) and Support Vector Machine (SVM) etc. are the various components of soft computing and each one offers specific attributes . In data hiding problem, GA may be used for optimizing the fundamentally conflicting requirements of imperceptibility, security and robustness. Neural network may be used to design robust watermarking for images to take advantages of relatively easy algorithmic specification, pattern mapping and classification. The feasibility of Support Vector Machine (SVM) may be explored to determine automatically where the significant blocks are and to what extent the intensities of the block pixels can be modified.

Research of data hiding in digital media reports that there exists different trade off relations. Hiding a secret message in any cover media this method is called Steganography. Cover media can be a text, or an image or an audio or video etc. It is an art of hiding information in ways a message is hidden in cover media so that will not arouse an unintended observer. A covert channel can be defined as a communications channel that transfers secret information. Observers are unfamiliar that a covert message is being connected. Only the sender and receiver of the message notice it.

Data Hiding or Steganography represents an important paradigm in software engineering. Several kinds of steganography methods exist for images but they are not intelligent to differentiate between redundant and non-redundant information in the data.

The work presented in this paper is about the perceptual shaping of watermark for digital images. The watermark shaped perceptually is then embedded to the digital images in wavelet domain. Digital watermarking has become an emerging area recently firstly because of the accessibility of powerful editing software, lossless copying and broadcast of multimedia data. Secondly the adversaries are continuously busy in developing sophisticated attacks. To counteract these new attacks as stated above there must be some intelligent and adaptive watermarking techniques. For effective watermarking, there should be an optimum tradeoff between robustness and imperceptibility. But unfortunately both of these properties are conflicting properties that make the problem of watermarking interesting and more challenging. For optimum tradeoff the watermark should be concealed in an imperceptible manner. A perceptual model is used to perceptually shape the watermark. So for the optimum tradeoff between the two conflicting properties of watermarking as stated above, some adaptive and global

search techniques like Genetic Algorithm (GA)[1], Ant Colony Optimization (ACO)[3,4], Genetic Programming (GP)[2] or Particle Swarm Organization (PSO)[5] should be used along with a suitable perceptual model. In this Thesis Work, an attempt has been made to implement a perceptual watermarking scheme using genetic algorithm.

2. Watermarking Concept:

Digital watermarking is the act of hiding a message related to a digital signal (i.e. an image, song, video) within the signal itself. It is a concept closely related to steganography, in that they both hide a message inside a digital signal. However, what separates them is their goal. Watermarking tries to hide a message related to the actual content of the digital signal, while in steganography the digital signal has no relation to the message, and it is merely used as a cover to hide its existence. Watermarking has been around for several centuries, in the form of watermarks found initially in plain paper and subsequently in paper bills. However, the field of digital watermarking was only developed during the last 15 years and it is now being used for many different applications. In the following sections are present some of the most important applications of digital watermarking, explain some key properties that are desirable in a watermarking system, and give an overview of the most common models of watermarking as presented in the book by Ingemar Cox, Matthew Miller, Jeffrey Bloom, Jessica Friedrich and Ton Kalker [11]. These basic models will be further illustrated by the use of example watermarking systems that were developed in MATLAB. All images used in this essay, except those used to present the results of the example watermarking systems are taken from this book [10].

2.1 Watermarking applications

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. It is often crucially important that we are able to track when a specific video is being broadcast by a TV station. This is important to advertising agencies that want to ensure that their commercials are getting the air time they paid for. Watermarking can be used for this purpose. Information used to identify individual videos could be embedded in the videos themselves using watermarking, making broadcast monitoring easier.

Another very important application is owner identification. Being able to identify the owner of a specific digital work of art, such as a video or image can be quite difficult. Nevertheless, it is a very important task, especially in cases related to copyright infringement. So, instead of including copyright notices with every image or song, we could use watermarking to embed the copyright in the image or the song itself. Transaction tracking is another interesting application of watermarking. In this case the watermark embedded in a digital work can be used to record one or more transactions taking place in the history of a copy of this work. For example, watermarking could be used to record the recipient of every legal copy of a movie by embedding a different watermark in each copy. If the movie is then leaked to the Internet, the movie producers could identify which recipient of the movie was the source of the leak. Finally, copy control is a very promising application for watermarking. In this application, watermarking can be used to prevent the illegal copying of songs, images of movies, by embedding a watermark in them that would instruct a watermarking-compatible DVD or CD writer to not write the song or movie because it is an illegal copy.

Although the major application of digital watermarking is to protect the copyright, but its applications are not that limited. It has a wide range of applications. Some important applications are:

2.1.1 Broadcast Monitoring

We can use digital watermarking to monitor that how many times a particular advertisement has been broadcasted [11]. In broadcast monitoring the system receives the broadcast. Then the system searches for the detection of watermarks and identifies when, where and how many times this work advertisement is broadcasted. Television is an example where news contains watermarked videos from broadcasters.

2.1.2 Owner Identification

In this application watermarking is used to confirm the owner. The creator of art work such as songs, book, and painting hold the copyright as soon as it is published/printed. Textural copyright notices have been used but they have some limitation. It can be easily removed from a document and then be copied even by those who don't have any wrong intentions. As the watermark can be concealed imperceptibly in to the work, it can identify the owner of watermark better then the textual form of owner identification.

2.1.3 Medical Applications

Watermarking is used to identify the medical x-ray images and other records of patients thereby reducing the chances of tampering of the medical records.

2.1.4 Content Authentication

Content authentication is another application of digital watermarking. Signature information are embedded into the content. Later it is verified whether the content information has been changed/modified. If a small change made to the cover, the same distortion will also be reflected on the watermark and hence the authentication work becomes invalid. Such types of watermark are called fragile watermark.

2.1.5 Transaction Tracking

In this application, watermark is used to recognize the procurer of digital commodities like audios, images and videos etc. manufacturer of such products conceal a fingerprint for the unique identification of each customer. In this way legal/illegal customers and illegal distribution can be easily identified.

2.2 Watermarking Properties:

Every watermarking system has some very important desirable properties. Some of these properties are often conflicting and we are often forced to accept some trade-offs between these properties depending on the application of the watermarking system.

The first and perhaps most important property is effectiveness. This is the probability that the message in a watermarked image will be correctly detected. We ideally need this probability to be 1.

Another important property is the image fidelity. Watermarking is a process that alters an original image to add a message to it, therefore it inevitably affects the image's quality. We want to keep this degradation of the image's quality to a minimum, so no obvious difference in the image's fidelity can be noticed.

The third property is the payload size. Every watermarked work is used to carry a message. The size of this message is often important as many systems require a relatively big payload to be embedded in a cover work. There are of course applications that only need a single bit to be embedded.

The false positive rate is also very important to watermarking systems. This is the number of digital works that are identified to have a watermark embedded when in fact they have no watermark embedded. This should be kept very low for watermarking systems.

Lastly, robustness is crucial for most watermarking systems. There are many cases in which a watermarked work is altered during its lifetime, either by transmission over a lossy channel or several malicious attacks that try to remove the watermark or make it undetectable. A robust watermark should be able to withstand additive Gaussian noise, compression, printing and scanning, rotation, scaling, cropping and many other operations.

3. Methodology:

To develop a watermarking scheme to shape the watermark perceptually according to the contents of the cover image requires incorporating the Human Vision to understand the contents of the cover image. In spatial domain, this phenomenon refers to the knowledge of differentiating between the flatter and edges/textured regions in a cover media.

In transform domain, this refers to know about the distribution of frequency in the cover image i.e. low, mid and high frequency components. Thus to conceal the watermark in an efficient manner the watermark is shaped perceptually by using perceptual models. These models explore sensitivities/insensitivities of human vision. A better a perceptual model will result in providing a better perceptual shaping and hence high imperceptibility will be achieved for watermarking applications. Perceptual models provide maximum distortion to a pixel (or DWT coefficient) and hence will not be visible to a human eye. These perceptual models make use of the frequency sensitivity, contrast masking, luminance sensitivity etc. Frequency sensitivity refers to the sensitivity of human vision to sinusoidal waves at different frequencies. It depends on the surroundings only. Luminance sensitivity is a threshold where a point becomes visible on a constant back ground. This threshold depends luminance of the target and on the mean luminance of the background. The third property of human vision which is important is the contrast masking. The effect of a signal on the detection of a different signal is known as contrast masking. In this work, DWT method is used to obtain the various coefficients of the image and to optimally watermark the image in one of the portions of this coefficients. The use of Genetic algorithm for optimizing the embedding process using the PSNR values of the image with respect to the original cover image, in determining the fitness function is the key aspect in this research work. The below write up summarizes the key aspects of this research work.

3.1 Genetic Algorithm:

Idea of evolutionary computing was introduced in the 1960s by I. Rechenberg in his work "Evolution strategies" (Evolutions strategie in original). His idea was then developed by other researchers. Genetic Algorithms (GAs) were invented by John Holland and developed by him and his students and colleagues. This lead to Holland's book "Adaption in Natural and Artificial Systems" published in 1975.

In 1992 John Koza has used genetic algorithm to evolve programs to perform certain tasks. He called his method "genetic programming" (GP). LISP programs were used, because programs in this language can expressed in the form of a "parse tree", which is the object the GA works on.

The concept of GP derives its existence from the concepts of natural selection and genetics. Accordingly, GP can be considered as to be inspired by biological evolution process. In GP, we develop a class of candidate solutions for the given problems and evolve them again and again by using stochastic operators. A fitness function is designed against which each candidate solution is evaluated. Fitter solutions after evaluation have high probability of generating offspring. The cycle of iterations continue until either an optimal solution is reached or predefined set of iterations is executed.

3.2 Watermarking Using Genetic Algorithm:

In this section a novel watermarking scheme has been proposed. The technique is based on genetic algorithm which utilizes the spatial to wavelet transform to shape the watermark perceptually according to the contents of the cover image in DWT domain. DWT is used because the compression standard of JPEG2000 is also based on DWT. It is used also because of its multi-resolution hierarchical characteristics, and lower resolution embedding and detection which are computationally inexpensive. The optimization for perceptual shaping of a watermark according to the cover image using genetic algorithm have led us to obtain excellent results which are convincingly better than previously established results. Genetic Algorithm belongs to probabilistic optimized search algorithms. The concept derives its existence from the concepts of natural selection and genetics. Accordingly, genetic algorithm can be considered as to be inspired by biological evolution process. In genetic algorithm, we develop a class of candidate solutions for the given problems and evolve them again and again by using stochastic operators. A fitness function is designed against which each candidate solution is

evaluated. Fitter solutions after evaluation have high probability of generating offspring. The cycle of iterations continue until either an optimal solution is reached or predefined set of iterations is executed.

Proposed Algorithm:

- Read the image
- Convert it into grayscale.
- Generate the key image to be embedded.
- Compute the wavwlet coefficients using 2-D DWT algorithm and db1 filters.
- Perform Watermark Embedding:

$$Y = cv + c*abs(cv).* N \quad (1)$$

where cv is the DWT coefficient in which the embedding is done, c is the watermark weight, N is the size of hidden image

- This generates new coefficients with the embedded information of the hidden image.
- Perform Inverse DWT to form the image.
- Calculate the Mean Square Error (MSE) and Peak Signal to Noise ratio (PSNR) values.
- Initialize the genetic algorithm by defining the fitness function using the PSNR values.

Fitness Function:

$$F=PSNR(1)+PSNR(2)+PSNR(3)+PSNR(4); \quad (2)$$

where PSNR is Peak Signal to Noise Ratio and 1,2,3,4 are the indexes of four quadrants of DWT.

- Convert to image form.
- **Watermark Extraction**:

Read in the watermarked image.
Perform DWT.
Obtain Coefficients of Hidden message, using below equation:

$$cc=abs(cv1./N); \quad (3)$$

where cc is hidden message, cv1 is the coefficients of DWT and N is watermark size.

Thus the Watermarking and De-Watermarking (Extraction) is performed using this approach. The following chapter shows a detailed description of the implementation part and various results are obtained using a number of test images.

4. Result and Discussion:

Extensive experiments have been performed on a number of images to analyse the working of the algorithm. Several standard test images such as boat, baboon, Lena, peppers, couple, cameramen etc are referred to in the present paper for watermark embedding and watermark detection. The technique is not limited to the use these cover images but we have used them as they are standard images widely used by other researchers working on watermarking. They all are gray scale images with size 256x256. All the images are watermarked using the best evolved expression.
The below portion shows the obtained results on Baboon image:

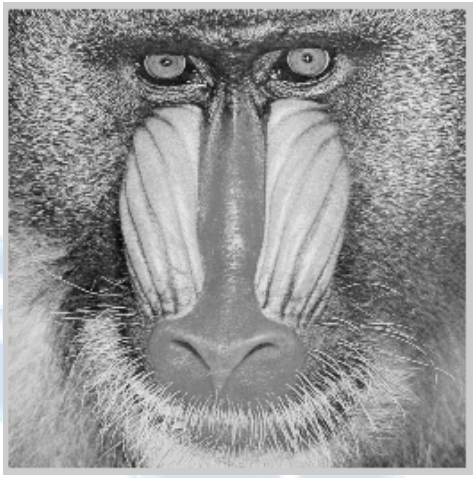

Fig. 1. Original Image

Fig 2. Key Image (Hidden Image)

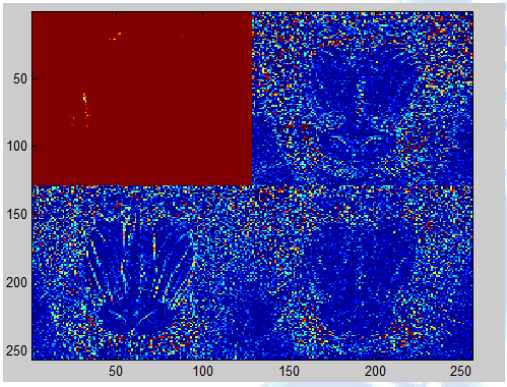

Fig. 3. Image after 2D-DWT

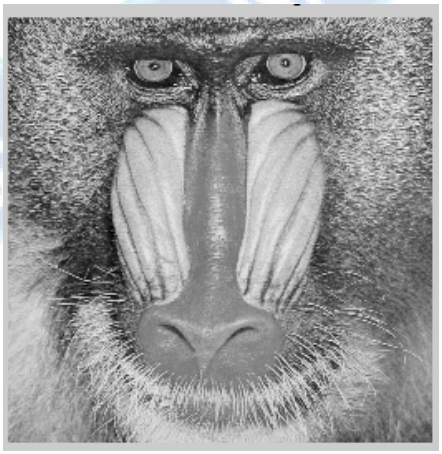

Fig. 4. Watermarked Image

Fig. 5. Retrieved Watermark

The above figure shows the various parts of the implementation. Figure 1 shows the original image of baboon. Figure 2 shows the key image. Figure 3 shows the watermarked image which is watermarked using the best evolved expression. There is no perceptual distortion in the watermarked image which shows the high imperceptibility of the proposed technique. Figure 5 shows the retrieved watermark under no attacks, which proves that the proposed method is able to learn the spatial distribution of the Lena image.

The below table shows the PSNR values at the time of testing for propose work and a comparison of PSNR values from two References [1] and [2] and proposed work.

Table 1: PSNR values Comparison

	Host Image PSNR Value [1]	Host Image PSNR Value [2]	PSNR Values for Proposed
Boat	44.860226	29.75	64.82
Leena	44.783592	30.34	74.12
Mandrill	44.9216	26.46	45.17
Pepper	44.8291	30.65	67.34

5. Conclusion:

This research work was focused at study and analysis of various data hiding techniques and using the genetic algorithms for the purpose of digital watermarking. As discussed earlier, in the case of images invisible digital watermarking makes the suppression of a watermark more interesting. In order to attain imperceptibility, and at the same time the quality of image the choice would be to conceal the watermark in those coefficients which are insignificant perceptually. The DWT transform domain provides a detailed analysis of various components of an image data which can be chosen to hide the message in one of the components of the DWT transform. The PSNR values of the images obtained after watermarking in DWT domain was used as the fitness function, to evaluate the optimal coefficient in which to hide the hidden message. The program was implemented on MATLAB software tool and the various results were shown. The algorithm shows a significant increase in the PSNR values as compared to the other methods discussed in Literature review especially the GADSCT method. The algorithm was tested on a number of standard test images available on the internet. All these images are grayscale and standard size of 256x256. The retrieved watermark in almost all test cases was clearly perceptible after extraction algorithm was implemented which shows the efficiency of the method.

References:

[1] K.B. Raja, C.R. Chowdary, K.R. Venugopal and L. M. Patnaik, “A Secure Image Steganography using LSB, DCT and Compression Techniques on Raw Images”, Proceeding of 3rd IEEE International conference on Intelligent Sensing and Information Processing (ICISIP), (2005) December 14-17, Bangalore, India.

[2] A. Cheddad, J. Condell, K. Curran, and P. M. Kevitt, “Digital image steganography: survey and analysis of current methods”, Signal Processing, vol. 90, no. 3, (2010).

[3] H. Yang, X. Sun, and G. Sun, “A High-Capacity Image Data Hiding Scheme using Adaptive LSB Substitution” , Radio Engineering, vol. 18, no. 4, (2009).

[4] Z. H. Wang, C. C. Chang, and M. C. Li, “Optimizing Least Significant Bit Substitution using Cat Swarm Optimization Strategy”, Information Sciences, vol. 192, no. 1, (2012).

[5] S. Wang, B. Yang, and X. Niu, “A secure steganography method based on genetic algorithm”, Journal of Information Hiding and Multimedia Signal Processing”, vol. 1, no. 1 (2010).

[6] Z. Zhao, H. Luo, Z. M. Lu, and J. S. Pan, “Reversible Data Hiding Based on Multilevel Histogram Modification and Sequential Recovery”, International Journal of Electronics and Communication, vol. 65, no. 10, (2011).

[7] C. C. Lin, W. L. Tai, and C. C. Chang, “Multilevel Reversible Data Hiding Based on Histogram Modification of Difference Images”, Pattern Recognition, vol. 41, no. 12, (2008).

[8] D. Wu, and W.H. Tsai, “A Steganographic Method for Images by Pixel Value Differencing”, Pattern Recognition, vol. 24, no. 9-10, (2003).

[9] V. M. Potdar, and E. Chang,“Gray Level Modification Steganography for Secret Communication”, Proceeding of 2nd IEEE International Conference on Industrial Informatics (INDIN), (2004) June 26-26, Berlin, Germany.