Watermarking Algorithm using Genetic Algorithm and HVS

T.Sridevi
Associate Professor
CBIT,Hyderabad
India

S Sameen Fatima,Ph.D
Professor
Osmania University,Hyderabad
India

ABSTRACT
In this work, a watermarking algorithm is proposed using Genetic algorithm and discrete wavelet transformation. The algorithm proposed is to improve both robustness and fidelity of the watermarked image. Fuzzy Inference system is used to determine the embedding strength based on HVS properties of the image. To test the robustness different attacks are performed and the NC (Normalized cross correlation) is computed. The algorithms showed better results and good quality for watermarked image.

General Terms
Genetic Algorithms, Watermarking, Security, Algorithm, Fuzzy logic.

Keywords
Watermarking, DWT (discrete wavelet transformation), robustness, fidelity, Fuzzy Inference system(FIS), HVS (human visual system) NCC (normalized co-relation coefficient).

1. INTRODUCTION
With the increased recognition of the digital media through digital networks on World Wide Web in the early 1990's demonstrated the commercial potential. So, there should be protection of ownership rights .Digital watermarking is one method of accomplishing this.

Generally information could be hidden either by directly modifying the intensity value of pixels or frequency coefficients of an image. The former technique is called spatial domain technique and later is called frequency domain technique. In transform domain casting of watermark can be done in full frequency band of an image or in specific frequency band such as in low frequency band or in high frequency band or in middle frequency band. If perceptually insignificant coefficients are selected for embedding then the watermark may be lost by common signal processing operations.

The watermarks can be of two types, visible and invisible watermarks according human perception. A visible watermark is a secondary translucent image overlaid into the primary image and appears visible to a casual viewer on careful inspection. Invisible watermarking can again be of two types, robust and fragile. A fragile watermark is embedded in such a way that any manipulation or modification of the image would alter or destroy the watermark. A robust watermark is embedded in such a way that modifications made to the pixel value are perceptually not noticed, and it can be recovered only with appropriate decoding mechanism.[4]

In the frequency or transformed domain, one can insert watermark into the coefficients of a transformed image. Some of the transformations are Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT). Watermarking in this domains are difficult to be detected.[4].

HVS was introduced to perform quantization of DWT coefficients for image compression by Lewis et al[2].Quantization steps are adjusted according to noise based on HVS. Barni [5] modified [2] to adjust for image watermarking.

The essential requirements of Digital watermarking are robustness, perceptual transparency. Robustness is ability of watermark for different attacks. Embedding of watermark should not degrade the quality of original image which we call as Perceptual transparency. These requirements diverge with each other. If watermarking strength is increased, robustness can be achieved, but perceptual transparency is lost and vice versa. An efficient solution can be attained with HVS. The watermark strength can be altered with HVS.

This work executes a watermarking algorithm based on characteristics of HVS combined with Fuzzy Inference system. The strength of watermarking is adjusted based on HVS and |FIS.

2. PRELIMINARIES
The Preliminaries used in this work are discussed below.

2.1 Discrete Wavelet Transform (DWT)
In DWT, the signal is split or decomposed into two parts, usually the high frequency and the low frequency part, which is called as decomposition of the signal. The edge components of the signal are largely confined to the high frequencies part. High frequency components of the signal are send through high pass filters and low frequency components through low pass filters.

In DWT, each level of decomposition produces four bands of data denoted by LL, HL, LH, and HH. The LL sub band can further be decomposed to obtain another level of decomposition. This process is continued until the desired number of levels determined by the application is reached.
The adaptive watermarking strength can be adjusted based on the relation between the DWT.

2.2 HVS (Human visual system)

The strength of watermark is modified according to the relation between image DWT coefficients and HVS. Taking into account that when brightness is very high or very low, eye is less sensitive to noise, the equation for eye's sensitivity is given as in Eq (3).

$$L_1(i,j) = \frac{1}{256} \sum_{(x,y)\in\eta} X_3^3 \left(x + \left[\frac{i}{2^{3-l}}\right], y + \left[\frac{j}{2^{3-l}}\right]\right) \qquad (3)$$

Where

$$\eta = \{(x,y)|(x,y) \in (-1,0),(0,-1),(0,0),(1,0),(0,1)\}$$

2.3 Texture sensitivity (T)

One of the methods to calculate texture sensitivity is based on Local Binary Pattern (LBP). This operator was first introduced [9] based on the postulation that texture has locally two paired aspects, a pattern and its strength. Now, LBP became one of the strongest measures of texture analysis in an image. From experimental studies [7], it is found that it got good results.

The LBP is the effect from a description of texture in local neighborhood .It's property is that it is gray-scale invariant texture measure. After combining the neighborhood values, LBP value will range from 0 to 255 for each pixel [8].

2.4 Fuzzy Inference System (FIS)

The Fuzzy inference system, also known as a fuzzy expert system, is supported by fuzzy set theory. The FIS deals with plotting a given set of inputs to a fuzzy set.

A fuzzy inference system is comprised of four blocks:

1. Fuzzifier,
2. Knowledge base,
3. Fuzzy inference engine
4. De-Fuzzifier

The Fuzzifier transforms crisp inputs into fuzzy sets. The knowledge base encompasses a database and a rule base. In this scenario, the database defines the membership functions. The rule base consists of a set of IF-THEN rules .The fuzzy inference engine is a generic control mechanism that exploits the fuzzy rules and the fuzzy sets defined in the knowledge base in order to reach a certain conclusion and de-Fuzzifier in a typical FIS is used to convert fuzzy outputs of the fuzzy rules into crisp output values.

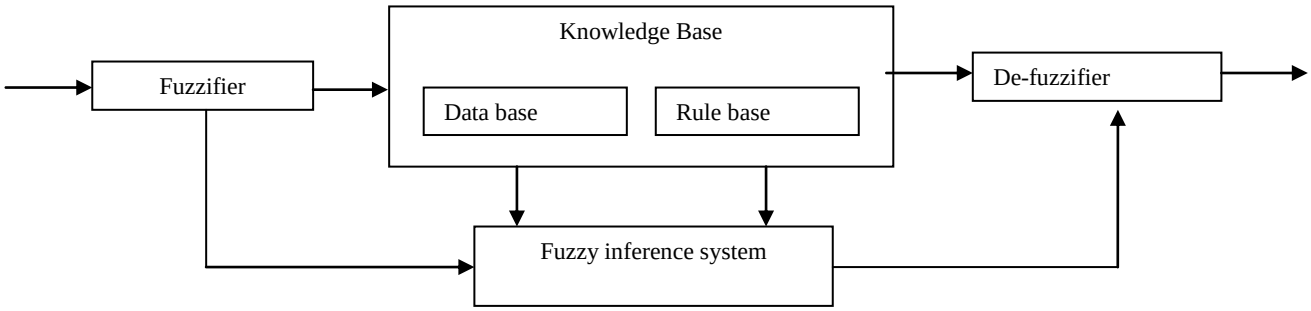

Fig1.Fuzzy inference system

2.5 Genetic Algorithm

Genetic Algorithm is a search's technique that simulates natural process [11, 12] and generates best solution for all possible combinations. In this context GA will find best solution for both perceptual transparency and robustness. As the watermark strength 'α' is increased robustness of the algorithm is increased and vice versa.

The input image is first encoded through a binary string encoding scheme which is called as 'chromosomes'. These binary strings are maximized or minimized for the fitness function. The fitness function will be different for different applications. The main parts of any genetic algorithm [11] are

1. Selection
2. Crossover
3. Mutation

Initially chromosomes are selected randomly. Genetic operators crossover and mutation are performed on the selected parents to produce new offspring from the population to form the next generation. The entire process is repeated for several generations until the best solutions are obtained.

3. Proposed Algorithm

The algorithm is based on fuzzy and genetic methods

3.1 Fuzzy rules

Fuzzy rules are a collection of linguistic statements that describe how the FIS should make a decision regarding classifying an input or controlling an output. A typical fuzzy if-then rule has an antecedent part as well as a consequent part.

1. If (luminance is dark) and (texture is slightly smooth) then (embedding is small)
2. If (luminance is dark) and (texture is rough) then (k is average)
3. If (luminance is lightly dark) and (texture is smooth) then (k is small))
4. If (luminance is lightly dark) and (texture is slightly smooth) then (k is small)

5. If (luminance is lightly dark) and (texture is rough) then (k is large)
6. If (luminance is bright) and (texture is smooth) then (k is small)
7. If (luminance is bright) and (texture is slightly smooth) then (k is average)
8. If (luminance is bright) and (texture is rough) then (k is large)
9. If (luminance is dark) and (texture is smooth) then (k is small)

Mamdani's fuzzy inference method is the most commonly seen fuzzy methodology. Mamdani's method was among the first control systems built using fuzzy set theory. It was proposed in 1975 by Ebrahim Mamdani as an attempt to control a steam engine and boiler combination by synthesizing a set of linguistic control rules obtained from experienced human operators. Mandani's method expects the output membership functions from the fuzzy sets. After the aggregation process, there is a fuzzy set for each output variable that needs de-fuzzification. It is possible, and in many cases much more efficient, to use a single spike as the output membership functions rather than a distributed fuzzy set. This type of output is sometimes known as a singleton output membership function, and it can be thought of as a pre-de-fuzzified fuzzy set. It enhances the efficiency of the de-fuzzification process because it greatly simplifies the computation.

3.2 Steps for genetic Algorithm:

- Watermark amplification factor α is calculated from Fuzzy inference system, initialize the population size, number of iterations, crossover rate, mutation rate.
- Permute watermark image.
- Generate the first generation of GA individuals **based on the parameters specified by performing** the watermark embedding procedure. A different watermarked image is generated for each individual.
- ***For each iteration do***
  - Evaluate the perceptual transparency of each watermarked image by computing the corresponding PSNR value
  - Apply a common attack on the watermarked image.
  - Perform the watermark extraction procedure on each attacked watermark image.
  - Perform inverse permutation on the extracted watermark.
  - Evaluate robustness by computing the correlation(ρ) between the original and extracted watermarks
  - Evaluate the fitness function for the PSNR and ρ values
  - Select the individuals with the best fitness values.
  - Generate new population by performing the crossover and mutation functions on the selected individuals.
- ***End While***

3.3 Watermark Embedding

Choose an image, *I* of size M by N. Before embedding into the image, perform discrete wavelet transform on the image. After performing one-level DWTs, choose one of the bands LL, LH, HL, and HH for embedding the watermark.

Perform permutation on the watermark of size M_wX N_w with a key k_0 for further protection.

$$W_{p=} permute\ (W, k_0) \qquad (2)$$

Where, W_p –number of bits to be embedded into the cover image.

Select population of size M_w by N_w with number of individuals equal to *n*. Set the coefficients of the individuals randomly. The coefficients for embedding W_p is finally achieved with GA. The equation for embedding is given below.

$$W_m = LL + \alpha W_p \qquad (3)$$

Where,

W_m is the watermarked image,

LL is the low band of cover image after DWT and it may replaced with LH, HL *or HH*,

α is the embedding strength calculated based on fuzzy rules.

After embedding perform inverse DWT using the watermarked band.

3.4 Watermark Extraction

The process of extraction is just the inverse process of the embedding process. In this method we do not require the cover image that was used initially. The key k_0 along with the selected coefficients is sent the user via a secret encrypted method. Let the image received by the user be *I'*. Perform DWT on *I'* and choose the same band that was selected while embedding.

Then extract the W'_p from the watermarked image by using the inverse process of embedding.

4. Results

The performance of the proposed watermarking algorithm is explored with number of experiments on different images. MATLAB platform is used. To test the robustness and imperceptivity of the algorithm NC and PSNR values are evaluated between original images and modified images. Some of the test images are shown in fig 3.The equation for NC and PSNR is given as

$$NC = \frac{\sum\sum(W * W')}{\sum\sum W^2} \qquad (4)$$

$$PSNR = 10log_{10}\left(\frac{255^2}{MSE}\right) \qquad (5)$$

Now, the attacks are performed on the watermarked image. The attacks like low pass filtering (LPF), median filtering attack (MF) and the JPEG Compression attack are chosen. Any number of attacks can be included calculate the fitness values using the fitness function which is given by,

$$F=PSNR+\lambda*(NC1+NC2+NC3) \qquad (6)$$

Where λ is selected for ease of calculation, NC1, NC2, NC3 are the NC values obtained by performing the LPF, MF and JPEG attack on the watermarked image.

PSNR plays the role of imperceptibility measure, while NC plays the role of robustness measure. Because the PSNR values are dozens of times larger than the associated NC values in the GA fitness function, magnify the NC values with the weighting factors λ in the fitness function to balance the influences caused by both the imperceptibility and robustness requirements.[3]

The fitness values thus calculated indicate the individual that give best results. Replace the worst fitness individuals with the best ones by cross over and mutation operations. Mutation increases the divergence of individuals in the population. Every iteration will eliminate the worst individuals and replace them by children of the best individuals. Thus, preserving the best and the children while eliminating the worst.

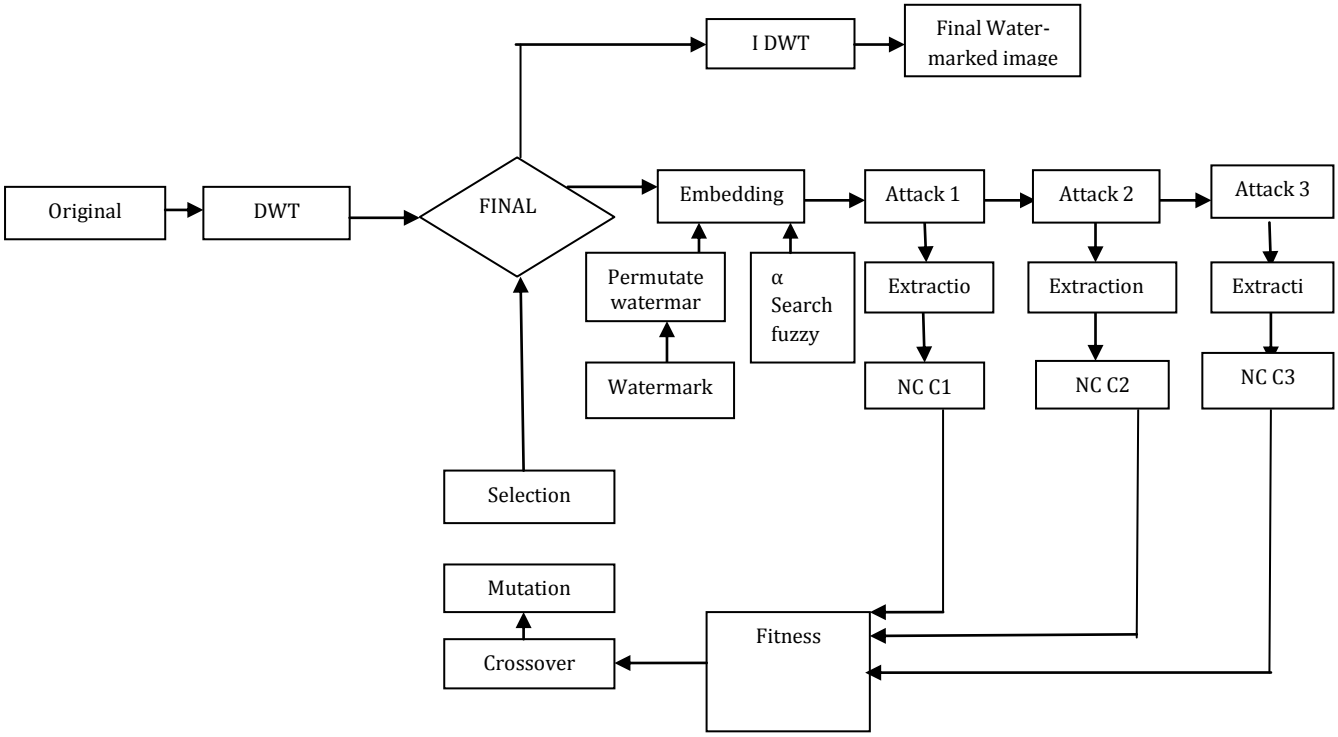

Fig 2: Watermark embedding procedure using GA and fuzzy logic

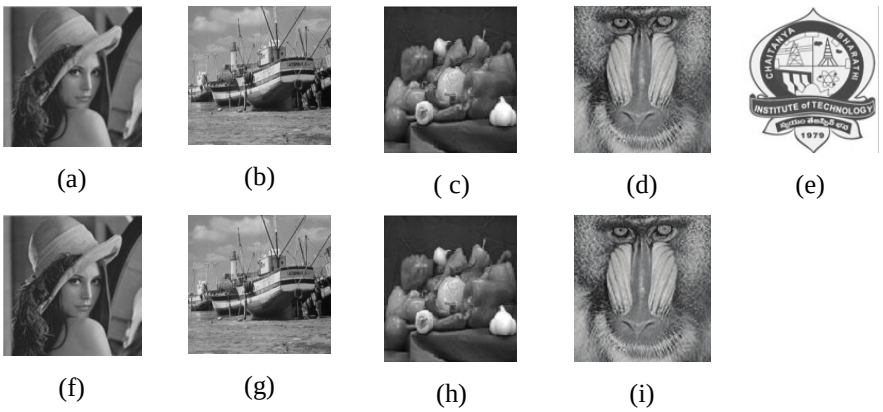

Fig 3: Original images (a) Lena(b) Boat(c))Peppers (d) Baboon(e) binary watermark (f)---(i)watermarked images

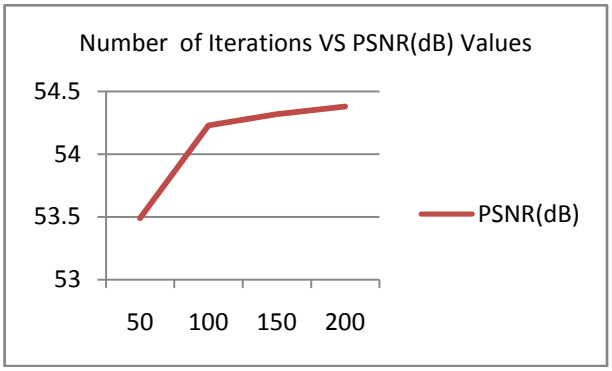

Fig4:PSNR values in LH band for different iterations

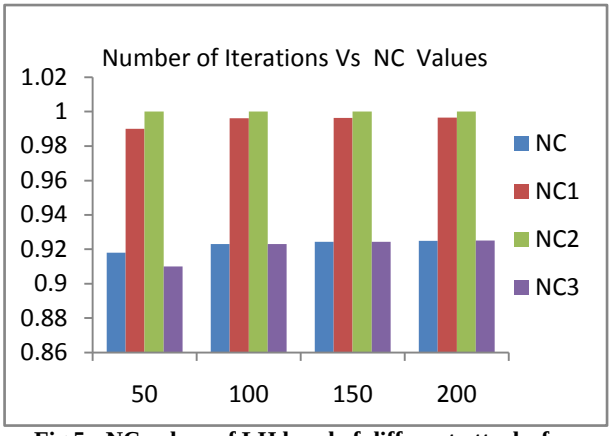

Fig 5 : NC values of LH band of different attacks for different iterations

Table 1 : Optimization performance after 50 iterations

images	NC,PSNR dB(Proposed)	NC,PSNR dB[15]	NC,PSNR dB [13]	NC,PSNR dB [14]
Lena	0.918,53.49	0.84,40.25	0.73,36.23	0.78,37.01
Boat	0.92,53.87	0.85,41.26	0.74,36.16	0.78,36.62
Baboon	0.92,53.69	0.83,39.17	0.74,35.76	0.76,36.94
Peppers	0.92,53.73	0.82,40.96	0.75,35.89	0.77,36.45

5. CONCLUSIONS

In this work, the digital image watermarking in DWT domain based on genetic algorithm proposed. The watermark amplification factor is calculated based on the HVS properties of the image. The values PSNR and NC are increased as the number of iterations increased showing that genetic algorithms improves the image imperceptibility and robustness of watermarked images even after performing attacks.

6. ACKNOWLEDGMENTS

Authors would like to thank to all the reviewers.

7. REFERENCES

[1] A. Reza, "Wavelet Characteristics, What Wavelet Should I use?," White Paper, 1999.

[2] A. S. Lewis and G. Knowles, "Image Compression Using the 2-D Wavelet Transform," IEEE Transactions on Image Processing, Vol. 1,No. 2, pp.244-250, Apr. 1992.

[3] Chin-Shiuh Shieh, Hsiang-Cheh Huang, Feng-Hsing Wang, Jeng-Shyang Pana, "Genetic watermarking based on transform-domain techniques", C.-S. Shieh et al. / Pattern Recognition 37,pp. 555 – 565, 2004.

[4] Dr Cauvery N K,"Water Marking on Digital Image using Genetic Algorithm", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 6, No 2, pp. 323-332, 2011.

[5] M. Barni, F. Bartolini, and A. Piva, "Improved Wavelet-Based Watermarking Through Pixel-Wise Masking," IEEE Transactions on Image Processing,May 2001.

[6] Nizar Sakr, Nicolas Georganas, and Jiying Zhao ,"Copyright Protection of Image Learning Objects using Wavelet-based Watermarking and Fuzzy Logic", 3rd annual e-learning conference on Intelligent Interactive Learning Object Repositories Montreal, Quebec, Canada, 9–11 November, 2006

[7] Pietikäinen, M. "Image Analysis with Local Binary Patterns", 2005, pp 115-118.

[8] Sherin M. Youssef, Ahmed Abouelfarag, and Noha M. Ghatwary ,"Adaptive Digital Watermarking Integrating Fuzzy Inference HVS Perceptual Model", World Academy of Science, Engineering and Technology 72 2012

[9] T. Ojala, M. Pietikäinen, and T. Mäenpää, "Multiresolution gray-scale and rotation invariant texture classification with local binary patterns", IEEE Trans. PAMI, vol. 24, 2002, pp. 971- 987.

[10] Goldberg, D.E , "Genetic Algorithm in Search , Optimization & machine Learning", Addison-Weseley,1989. [12] M.Srinivas and Lalit M.Patnaik, " Genetic Algorithm : A Survey" IEEE,1994.

[11] Lin, T.C., Lin, C.M., 2009. Wavelet-based copyright-protection scheme for digital images based on local features. Information Sciences 179, 3349–3358.

[12] Paquet, A.H., Ward, R.K., Pitas, I., 2003. Wavelet packet-based digital watermarking for image verification and authentication. Signal Processing 83, 2117–2132.

[13] Maity, S.P., et al., Collusion resilient spread spectrum watermarking in M-band wavelets using GA-fuzzy hybridization. J. Syst. Software (2012)