Global Journal of Enterprise Information System

DOI: 10.15595/gjeis/2014/v6i2/51851

DCT based Fuzzy Image Watermarking

Durgansh Sharma[1*], Manish Prateek[2] and Tanushyam Chattopadhyay[3]

[1]*Jaipuria Institute of Management, Noida, India; durgansh.sharma@jaipuria.ac.in*

[2]*Centre for Information Technology, College of Engineering Studies, UPES, Dehradun, India; mprateek@ddn.upes.ac.in*

[3]*R&D, Innovation Lab, Tata Consultancy Services, Kolkata, India; t.chattopadhyay@tcs.com*

Abstract

Image watermarking implants an ownership parameter in a digital image or video. This paper works on authentication of the image file. Robust image watermarking technique is used to model the Human Visual System (HVS) using Fuzzy Logic. The proposed Fuzzy Logic System is trained using inference rules considering three sensitivities of HVS as Brightness, Contrast and Edge Sensitivity. The Fuzzy network uses the image captured in realtime and computes block wise for producing a single output weighting factor used to embed unique identification numbers generated from the confidential data as watermark, which is for authorization and verification of the original image. The robustness of the watermark embedded is checked by Stirmark image processing attacks. Recovered watermark's computed value using SIM(X, X*) parameter for the image verified it as good watermark recovery process.

Keywords: Fuzzy Logic, Fuzzy Inference System, Human Visual System (HVS), Robust Image Watermarking,

1. Introduction

Current trends are about posting and sharing the captured images almost instantly, it has raised the amount of data repository in web-servers saved in the form of images, photos and videos. Across the globe it has been observed a trend of exponential growth in the generation of images and video due to the provision of handy mobile devices with a built-in camera. The current way of distributing data, is leading towards unauthorized distribution in terms of copying the digital content. This technology offers advantage intelligently as compared to the old analog counterpart. Some of these advantages are data transmission, easy data editing of digital content, improved capability of lossless copying of the digital content. Digitization of image enhances its prospects almost in every domain from medical imaging to architecture, satellite imaging, and space exploration etc. at the same time the protection of the originality is most important. The digitization of the content has reduced the efforts to connect and collaborate amongst various users across the globe. But, at the other hand it has also increased the scope of vulnerable attacks on these contents specially images and videos.

Digital image watermarking is a method to authenticate the content through its ownership.

Many optimization algorithms based on Transform-ations (DCT-DWT)[1], Encryption Techniques[2], Neuro-Fuzzy (Fuzzy-BP)[3], Fuzzy Logic[4], Artificial Neural Network[5], Genetic Algorithm[7] are used to embed and extract the authorization code for validation from the given image and is perceived as the key application area of image processing. The objective is to develop a Optimized Robust Image Watermarking algorithm for embedding and extracting the unique ownership key as watermark in an image.

Motwani et al.[4] has implemented a MAMDANI type FIS, its input parameters are derived from HVS like sensitivity towards brightness, edge and texture or contrast of the image. Charu et al.[3] extended the work further by including the three layered Fuzzy-BPN with a 3-3-1 layer configuration for learning mechanism system using 50 iterations.

Charu et al.[3] have also implemented the HVS model using Fuzzy-BP in the context of digital image watermarking. They divided the image into blocks and compute its sensitivity, on the basis of the variance computed using Fuzzy-BP, they filtered the blocks and embed the random sequence of numbers as watermark. The adopted procedure generated a good quality watermarked image which is imperceptible in its property.

In the paper, we propose to embed a robust label of text strings of ownership identification in the image for its validation.

* *Author for correspondence*

We consider a 256x256 pixel image of 'Lena' for this presented work. The characteristics are modeled using Zhao and Koch[10,11] emphasized that the multimedia data must contain a label or code, which identifies it uniquely as property of the copyright holder. He described the technique of embedding robust labels in the images for copyright protection.

The watermark extracted from the signed image using algorithm proposed by Cox et al.[9]. It will be compared for the similarity correlation using SIM(X,X*), this parameter is determined for recovered watermark. Computed values show a good significance level of optimization in the process of embedding and extraction of watermark.

The output of proposed inference system in this paper is used to embed the watermark in the host image in the DCT domain. This FIS uses a set of 27 inference rules based on SIGMOID way of interpreting the logical inputs, which are primarily based on the facts of HVS behavior of sensitive to noise in the image with respect to brightness, texture or contrast, edges. All the mentioned ways are better inferred in a SIGMOID format as there are overlaps of brightness, contrast and edge sensitivity in HVS.

2. Experimental Details

The classification of present experimental work is as follows:

(i) Preprocessing of Host Image, Computing its HVS Characteristics and Evolving Fuzzy Inference System (FIS)

The host image of 'Lena' in spatial domain having the size of 256x256 pixel is divided into the 1024 blocks of 8x8 pixel each. Discrete Cosine Transformation (DCT) is used for the transformation of these blocks in the frequency domain. All the three HVS characteristics mentioned formerly are computed over these blocks as follows:

The Luminance Sensitivity: It is derived from the DC coefficients from the DCT blocks of the host image according to following formula[3]:

$$Li = \frac{X_{DC,i}}{X_{DCM}} \quad (1)$$

where, $X_{DC,i}$ denotes the DC coefficient of the i^{th} block and X_{DCM} is the mean value of the DC coefficients of all the blocks put together.

The Contrast Sensitivity: The contrast sensitivity is derived from the texture content of a region of 8x8 blocks in an image. The value of variance computed of an image block is provided to the direct metric for the quantification of the texture as a parameter. A routine proposed by Gonzalez et al.[6] is used through MATLAB. The execution of this routine is given by (2).

t = statxture(f) (2)

where, f is the input image or the sub-image (block) and t is the 7 – element row vector, one of which is the variance of the block in question.

The Edge Sensitivity: The edge could be detected in an image using the threshold operation; edge sensitivity can be quantified as a natural effect to the calculation of the block threshold T. The Matlab image processing toolbox implements graythresh( ) routine which computes the block threshold using histogram – based Otsu's method[9]. The implementation of this routine is given by (3)

T = graythresh(f) (3)

where, f is the host sub-image (block) in question and T is the computed threshold value.

These three parameters are fed into the proposed FIS as shown in Figure 1.

Fuzzy Input Variables for Luminance sensitivity of the eye: The brightness can be categorized as dark, medium or bright. The Figure 2 below plots the fuzzy input variable with less, moderate and high brightness values.

Contrast or Texture sensitivity of the eye: The eye's response to texture is classified into 3 categories - low, medium, and high. Figure 3, illustrate smooth, medium and rough texture values for this fuzzy input variable.

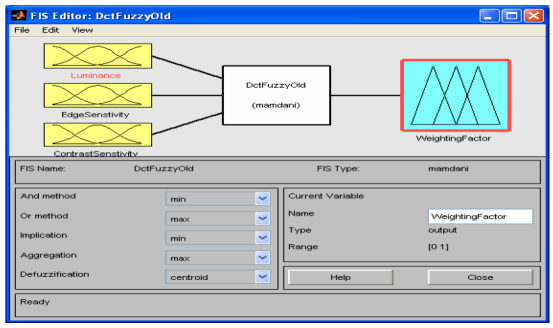

Figure 1. Fuzzy Model for HVS.

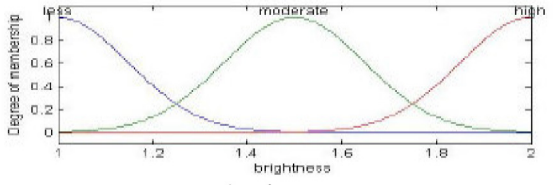

Figure 2. Fuzzy Values for Luminance Sensitivity.

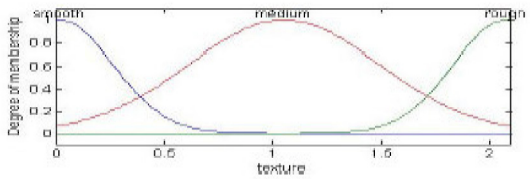

Figure 3. Fuzzy Values for Contrast Sensitivity.

Edge Sensitivity: The Edge Sensitivity can be small, medium, or large as shown in the plots below in Figure 4.

Fuzzy output variable is Weighting factor (W) that can take the following values - least, less, average, higher, and highest. Plots for the values are shown in Figure 5.

Sharma et al.[13] proposed Fuzzy Rules: The fuzzy rules are derived are based on the following facts:

a) Human Eye is highly sensitive to noise in those areas of the image where brightness is average.
b) Human Eye is highly sensitive to noise in low textured areas and towards the edges in high textured area as well
c) Human Eye is highly sensitive in the regions with low brightness and changes in less dark regions.

A total of 27 such rules are developed and are listed in Table 1.

A set of most frequently fired rules in the fuzzy rule engine are shown in the Figure 6.

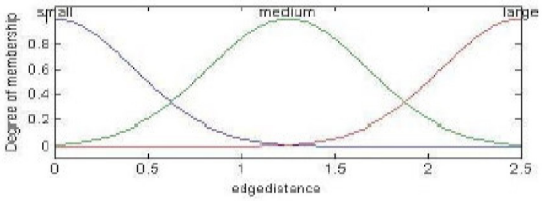

Figure 4. Fuzzy values for edge sensitivity.

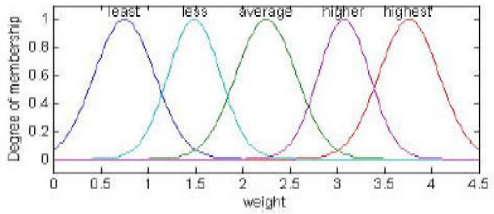

Figure 5. Fuzzy values for Weighting Factor (W).

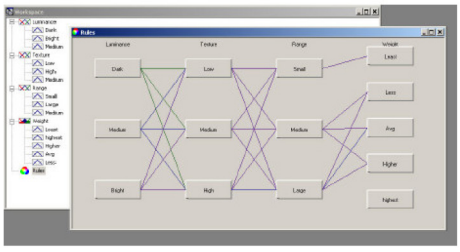

Figure 6. Most frequently fired rules in the fuzzy rule engine.

Table 1. HVS based 27 rules for fuzzy inference system

Rule No.	Luminance Sensitivity	Contrast Sensitivity	Edge Sensitivity	Weighting Factor
1	DARK	LOW	SMALL	LEAST
2	DARK	MEDIUM	SMALL	LEAST
3	DARK	HIGH	SMALL	LEAST
4	MEDIUM	LOW	SMALL	LEAST
5	MEDIUM	MEDIUM	SMALL	LEAST
6	MEDIUM	HIGH	SMALL	LEAST
7	BRIGHT	LOW	SMALL	LEAST
8	BRIGHT	MEDIUM	SMALL	LEAST
9	BRIGHT	HIGH	SMALL	LEAST
10	DARK	LOW	MEDIUM	LESS
11	DARK	MEDIUM	MEDIUM	HIGH
12	DARK	HIGH	MEDIUM	HIGHER
13	MEDIUM	LOW	MEDIUM	LESS
14	MEDIUM	MEDIUM	MEDIUM	AVERAGE
15	MEDIUM	HIGH	MEDIUM	AVERAGE
16	BRIGHT	LOW	MEDIUM	LESS
17	BRIGHT	MEDIUM	MEDIUM	AVERAGE
18	BRIGHT	HIGH	MEDIUM	HIGHER
19	DARK	LOW	LARGE	LESS
20	DARK	MEDIUM	LARGE	HIGHER
21	DARK	HIGH	LARGE	HIGHEST
22	MEDIUM	LOW	LARGE	LESS
23	MEDIUM	MEDIUM	LARGE	AVERAGE
24	MEDIUM	HIGH	LARGE	HIGHER
25	BRIGHT	LOW	LARGE	LESS
26	BRIGHT	MEDIUM	LARGE	HIGHER
27	BRIGHT	HIGH	LARGE	HIGHEST

(ii) Embedding the Watermark for Validation

Any computational device has certain identification numbers like MAC address for a computer, IMEI no. of a mobile phone.

Once the FIS is trained with given set of 27 inference rules. We propose the following process for embedding unique identification numbers as watermark for authorization and verification of the original image

Jian et al.[10] suggested the following algorithm which could be further extended for the usage in current computational devices. The first step generates a pseudo random position sequence using the outcome of FIS for selecting the 8x8 sub-blocks, where the code is embedded. This step is denoted as a function $Ts(y, U_K)$ where y is the image data to be labelled,

GJEIS | Print ISSN: 0975-153X | Online ISSN: 0975-1432

and U_K is the user-supplied secret key. The second step simply embeds or retrieves the code into or from the blocks specified in the position sequence.

The function Ts(y, U_K) initially extracts the required features from the image data, for its further usage with the unique identification numbers provided by user as secret key to be used as seeds for position sequence generation[12]. The featured must be robust against simple image processing that does not affect the visual quality of the image, and they must be image-dependent, i.e. the image can be recognized, distinctively in an ideal case, by these features extracted from the data provided by image under consideration[14].

Let D be the embedded code generated from the unique secret key, represented by binary bit stream {d_0,d_1,..,d_n}. Let, i be the index of current bit in this stream. Let B be the block set in which each block can be randomly selected. Initialize i to 0 and B to {}. The framework for writing and reading robust labels is described below:

In Figures (7,8) following legends will be used:

Image Data as (y), User defined Key (U_K), Label Code and Embedded Code as (D), Position Sequence as (PS), Labeled image as (y'), Position Sequence Generator as [T_s(y, U_k)], Label Embedding System as (LES), Label Retrieval System (LRS).

Algorithm 1(a): Framework (write)

(1) If i ≥ n, return.
(2) Randomly select a block *b*, using the position sequence generation function Ts(U_K, y) in Figure 7.
(3) If *b* exists already in B, goto (2), otherwise add *b* to B.
(4) Call check_write(*b*, d_i) to check wether *b* is a valid block: if this function returns False (i.e. the block *b* is an invalid block), go to (2).
(5) Call write(*b*, d_i) to embed a bit di to the block *b*.
(6) Increment i, go to (1).

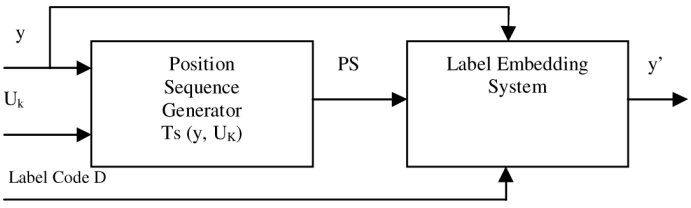

Figure 7. Write Label.

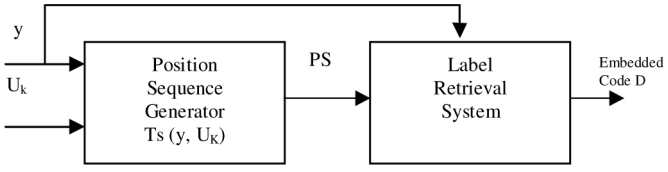

Figure 8. Read Label.

Algorithm 1(b): Framework (read)

(1) If i ≥ n, return.
(2) Randomly select a distributed or a contiguous 8x8 block b, using the position sequence generation function Ts(U_K, y) in Figure 8.
(3) If b exists already in B, then go to (2), otherwise add b to B.
(4) Call check_read(b,di) to check whether b is a valid block: if this function returns False (i.e. the block b is an invalid block), go to (2).
(5) Call read(b) to retrieve a bit from the block b.
(6) Increment i, and go to (1).

Once the label is embedded then Quality assessment of the signed image is done by computing Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR).

Executing StirMark Attacks: The watermarked image is further subjected to seven image processing attacks as prescribed by StirMark standard proposed by Petitcolas[8].

(1) Counterclockwise rotation of 90°.
(2) Dithering of color levels from 256 to 16-color
(3) Gaussian Blur (Radius = 1.0 units)
(4) Brightness and Contrast operation (each 15%)
(5) Median Filtering (Filtering aperture = 3 units)
(6) 10% Gaussian Noise addition
(7) Jpeg compression (QF=90).

Quality assessment is done using Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) before and after execution of attacks on the signed image.

Extracting Watermark from Signed Image and Computing SIM(X, X*) Parameter: Firstly, the DCT of both host and signed images are computed block wise. Thereafter, the computed coefficients are subtracted from each other and the watermark is recovered. Let the original and recovered watermarks be denoted as X and X* respectively. A comparison check is performed between X and X* using the similarity correlation parameter given by eq. (5).

$$SIM(X, X^*) = \frac{\sum_{i=1}^{n} (X, X^*)}{\sum_{i=1}^{n} \sqrt{(X, X^*)}} \quad (5)$$

3. Results

Figure 9 depicts both the host and signed images. The detectable quality of the signed image is very good as indicated by the computed MSE and PSNR values mentioned above it.

Figure 9(a-g) represent attacked images obtained after executing StirMark prescribed image processing attacks over the

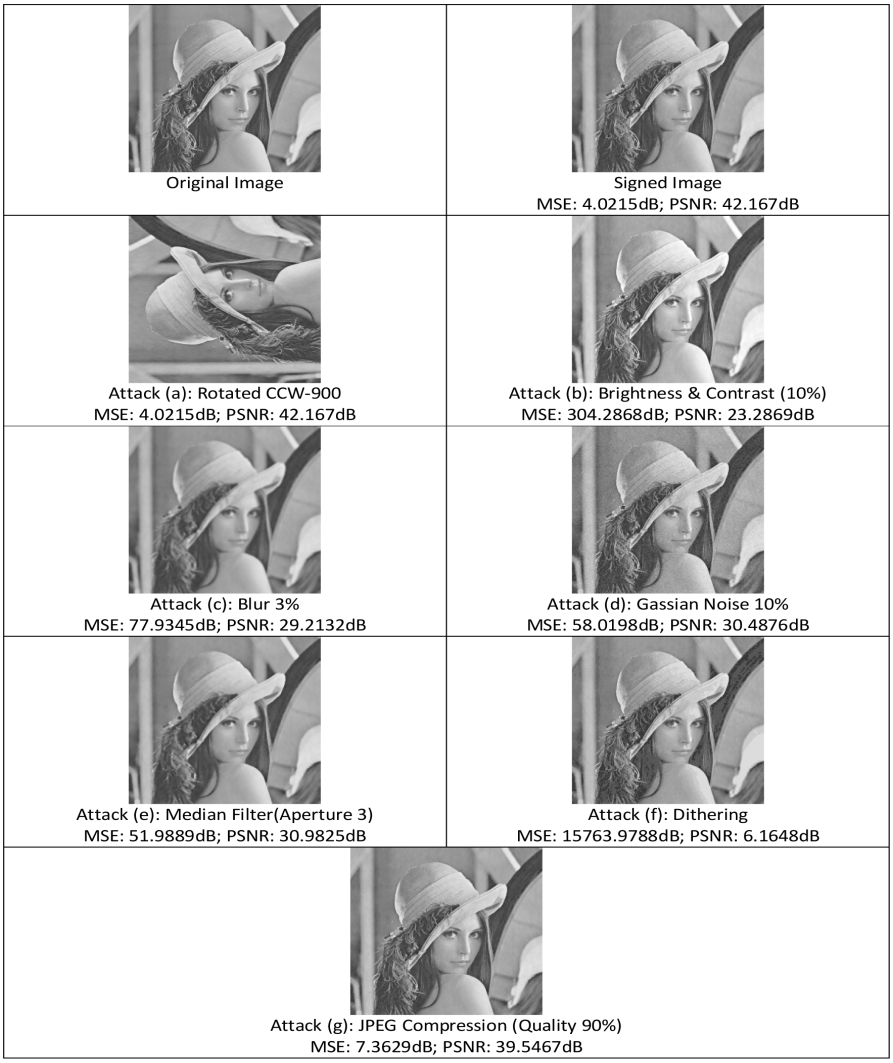

Figure 9. MSE and PSNR calculation of attacked images.

image shown in Figure 9 (Signed image). The respective MSE and PSNR values are mentioned above these images. These computed values are within the expected range for these attacks.

4. Conclusions

Computed value of SIM(X, X*) parameter for the image depicted in Figure 9 (Singed Image) is 18.6348 which indicates a good watermark recovery process.

5. Acknowledgement

The author Durgansh Sharma is a student of Ph.D. under the guidance of Dr. Manish Prateek and Dr. Tanushyam Chattopadhyay wish to thank his guides for providing their valuable support in pursuing his research work.

6. References

1. Idrissi N, Roukh A, Masmoudi L, Radouane M, Messoussi R. A robust digital watermarking technique using DWT-DCT and Statics blocks. International Journal of Computer Science Issues (IJCSI). 2013; 10(2).
2. Jawad LM, Sulong GB. A review of color image encryption techniques. International Journal of Computer Science Issues (IJCSI). 2013; 10(6).
3. Agarwal C, Mishra A. A Novel Image Watermarking Technique using Fuzzy-BP Network. 2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP); 2010; IEEE. p. 102–5.
4. Motwani MC, Harris FC Jr. Fuzzy perceptual watermarking for ownership verification. 2009; IPCV. p. 321–25.
5. Lou, D-C, Hu M-C, Liu J-L. Healthcare image watermarking scheme based on human visual model and back-propagation network. Journal of CCIT. 2008; 37(1):151-62.

6. Gonzalez RC, Woods RE, Eddins SL. Digital image processing using MATLAB; 2005; Pearson Education. p. 406 and 467.
7. Shieh, C-S, Huang H-C, Wang F-H, Pan J-S. Genetic watermarking based on transform-domain techniques. Pattern Recogn. 2004; 37(3):555–65.
8. Petitcolas FAP. Watermarking schemes evaluation. IEEE Signal Process Mag. 2000 Sep; 58–64.
9. Cox IJ, Kilian J, Leighton FT, Shamoon T. Secure spread spectrum watermarking for multimedia. IEEE Trans Image Process.1997; 6(12):1673–87.
10. Zhao J, Koch E. Embedding robust labels into images for copyright protection. KnowRight. 1995; 242–51.
11. Koch E, Zhao J. Towards robust and hidden image copyright labeling. IEEE Workshop on Nonlinear Signal and Image Processing; 1995; Neos Marmaras, Greece. p. 452–55.
12. Diffie W, Hellman M. New directions in cryptography. IEEE Transactions on Information Theory. 1976; IT-22:644–54.
13. Sharma D, Prateek M, Chattopadhyay T. Optimized robust image watermarking. Proceedings of 4th International Conference on Emerging Trends in Engineering & Technology; 2013 Oct 25–27. p. 99–106.