Watermarking Robustness Evaluation Using Enhanced Performance Metrics.

Sweta .S.Palewar
MTech student,
Computer Science & Engineering,
G.H.R.I.E.T.W,Nagpur.

Ranjana Shende
Lecturer,
Computer Science & Engineering,
G.H.R.I.E.T.W,Nagpur.

Abstract

The main idea of this paper is to propose an innovative benchmarking tool to evaluate robustness of any digital image watermarking technique.Image fidelity metrics such as signal to noise ratio(SNR),peak signal to noise ratio(PSNR), weighted peak signal to noise ratio(WPSNR) are being used. Researchers in the field of image processing use MSE (Mean Square Error) based fidelity metrics to validate their research results.However,when large quantities of data are to be assessed,subjective metrics such as mean opinion score(MOS),signal to noise ratio(SNR),peak signal to noise ratio(PSNR) are not pragmatic since it needs experts and inordinate amount of time.PSNR and WPSNR are independent of human visual system(HVS) parameters and hence they are inappropiriate scales to measure potential research results.This brings out a new image fidelity metric called Enhanced Weighted peak signal to noise ratio(EWPSNR) which is experimentally proven to be better than PSNR and WPSNR.

Keywords*:Genetic algorithm,perceptual quality,digital image watermarking, robustness,benchmark.*

1. Introduction

In the age of information technology, it has become easier and easier to access and redistribute digital multimedia data. Digital Watermarking techniques have been widely developed as an effective instrument against piracy, improper use or illegal alteration of contents.Two main problems seriously darken the future of this technology though.Firstly, the large number of attacks performed against watermarking systems and weaknesses which appear in existing systems have shown that far more research is required to improve the quality of existing watermarking methods. Secondly, the requirements, tools and methodologies to assess the current technologies are almost non existent.Consequently, the role of performance evaluation tools has become far more important[2]. A novel and flexible benchmarking tool based on genetic algorithms has been proposed to assess the robustness of digital watermarking system.The main idea is to evaluate robustness of watermarking scheme in terms of perceptual quality, measured by metrics Signal to noise ratio (SNR),Peak signal to noise ratio(PSNR),Weigted peak signal to noise ratio(WPSNR). The goal is to remove the watermark from a content while maximizing perceptual quality[1]. Here additional enhanced fidelity metric is introduced called Enhanced Weighted peak signal to noise ratio (EWPSNR) considering the limitations of PSNR and WPSNR which are independent of human visual system parameters and hence are inappropriate scales to measure potential research results.

2. Literature Review

In the literature, there are several benchmarking tools, which standardize the process of evaluating a watermarking system on a large set of single attacks.Fabien A. P. Petitcolas ,Ross J.Anderson,Markus G.Kuhn proposed a system called StirMark[3] in the year 1997,which is a generic tool for basic robustness testing of image watermarking algorithms. The first proposed benchmarking tool StirMark , applies a number of attacks (one at each time) to the given watermarked content and performs the detection process to check the presence of the mark.The drawbacks of the system are that it does not take into account the method's false alarm probability(probability to detect watermark in a non watermarked image),embedding and detection time are not evaluated.

Jan C. Vorbruggen,Franois Cayre proposed a system called Certimark[5] in the year 2000. In the system, an image source delivering the multimedia data to be watermarked, is taken. The attack module simulates all sorts of attacks on the watermark (intentional and non-intentional) resulting in possible loss of watermark readability.There is System Under Test(SUT) watermark encoder and System Under Test watermark decoder, performs detection of the watermark and extraction of the payload for monitoring purposes. A comparator module is used to compare payload to the original values. Then all results are taken into account to write a benchmark report, with tables and graphics to ease analysis.At the end , if required, a certificate of compliance is generated[5].This design approach provides several crucial advantages: modules can be exchanged easily; given well-defined interfaces, they can be developed separately; and they can be upgraded when needed.However, the certimark benchmark supports only still images and a limited set of professional quality video clips.

V. Solachidis, A. Tefas, N. Nikolaidis, S. Tsekeridou, A. Nikolaidis,I.Pitas, proposed a system called Optimark[6] in the year 2002.In the benchmarking system,the embedding module embeds a watermark Wj and a message M_k to an image I_i. The watermarked image should satisfy the quality specification Q_l.The above procedure is repeated for the sets of images ,keys, messages ,attacks and a set of watermarked images is generated. Then attacks are performed to distort the watermarked images that have been generated in the watermark embedding stage.First, the detection algorithm detects the watermark W_i that has been indeed embedded in the image I_a in the embedding procedure and the message M' is decoded.The same procedure is repeated for erroneous watermark W_i (i!=j). Thus, for each attacked image two pairs of detector and decoder outputs are extracted.Then detector and decoder outputs are collected for correct key and for erroneous key.During the watermark detection-decoding procedure the execution times are also measured and stored. The relative performance of the algorithm under test or its suitability for a certain application scenario is then checked[6]. The time needed for watermark and message embedding in each image is evaluated.The main drawback of optimark is the lack of possibility to expand the number of attacks.

3. Proposed Algorithm

Visual quality degradation due to the watermark embedding and the removing process is an important but often neglected issue to consider in order to design a fair watermarking benchmark.Given a pattern of possible attacks, the aim of this work is to find a near-optimal combination of them, which removes the mark minimizing the degradation perceived by the Human vision system(HVS). Hence, we need to define a proper quality metric. In general, several metrics can be used to evaluate the artifacts but the most popular one is the peak signal-to-noise ratio (PSNR) metric. The success of this measure is due to its simplicity but several tests show that such a metric is not suitable to measure the quality perceived by HVS.A modified version of PSNR, the so-called WPSNR, is introduced: it takes into account that HVS is less sensitive to changes in highly textured areas and introduces an additional parameter, called the noise visibility function (NVF), which is a texture masking function:

$$\mathrm{WPSNR(dB)} = 10\log_{10} \mathrm{I}^2_{\mathrm{peak/MSE\times NVF^2}} \qquad (1)$$

Where I_{peak} is the peak value of the input image.

The value of NVF ranges from:

$$\mathrm{NVF} = \mathrm{norm} \quad \{ \frac{1}{1+\delta^2_{block}} \} \quad \epsilon\,(0,1) \qquad (2)$$

Where norm is the normalization function and δ^2_{block} is the luminance variance of 8 * 8 block. The main idea of this contribution is to evaluate the robustness of a watermarking system in terms of perceptual quality measured by WPSNR. Namely, fixed a set of admissible image processing operators, the robustness of a method is quatified as:

$$\mathrm{R(q)}=\frac{Q}{M(q)} \qquad (3)$$

Where Q is fixed quality threshold,q is perceptual quality of watermarked image Iw,and M(q) is the maximal perceptual quality of the unmarked image obtained from Iw by applying any combination of the selected attacks. If R(q) is greater than 1, then it is possible to remove the mark from the given image only degrading its maximal perceptual quality M(q) under q. As a consequence, the watermarking algorithm can be declared robust since a large degradation needs to be introduced in the image to remove the mark. On the other hand, the embedded watermark is not robust if M(q) assumes values higher than the threshold Q (i.e.,R(q) is less than 1).

Robustness evaluation metric

Q>=M(q) R(q)>=1 ROBUST

Q<M(q) R(q)<1 NON ROBUST

3.1. Tool Description

In the proposed tool, Genetic algorithm(GA) is applied in the detection procedure of the watermarking scheme. An image previously watermarked by the algorithm to be tested and with perceived quality q is attacked with different combinations of selected image processing operators(attacks such as Rotation,Gray effect,Fixed Resolution) in order to remove the embedded mark. The aim is to find a near-optimal combination of attacks to apply in order to remove the watermark, while granting a perceptual quality of the resulting image as high as possible. The algorithm robustness is then measured via R(q) i.e optimization process is performed by GA and WPSNR is the fitness value to be maximized.

Step 1 Randomly generate combinations of parameters to be applied to processing operators and convert them into chromosomes . This way, an initial population is created.

Step 2 Apply each generated attack to the input image and evaluate the WPSNR of each chromosome in the current population which removes the watermark, i.e. which generates an unmarked image, and then create a new population by repeating the following steps: 1) pick as parents the chromosomes with the higher WPSNR, according to the selection rule; 2) form new children (new patterns of attacks) by applying to parents the stochastic operator of crossover with probability Pc 3) mutate the position in the chromosome with probability Pm. Among all individuals of the current population which allow removing the watermark, the one that provides an image with the higher WPSNR will survive to the next generation. We set to zero the fitness value of those chromosomes which do not succeed in removing the mark.

If in *Step 2* no solutions for the problem are found, i.e., none of the individuals of the population succeeds in removing the watermark, another population is re-initialized and the process is repeated until a termination criterion is met (number of generation exceeded). Consequently, the result of the test is that the analyzed watermarking technique is robust to the selected attacks.

Step 3 A new iteration with the just generated population is processed. This new population provides new attacks parameters,their corresponding fitness values are evaluated, and at every generation the individual with the highest fitness value is kept.

Step 4 The process ends when a given number of generation is exceeded (termination criteria). At that point a near-optimal combination of attacks removing the watermark from the image has been discovered. In particular, given the quality threshold Q ,M(q)<Q means that it is hard to remove the watermark while keeping a high perceptual quality, hence, the watermarking technique is declared to be robust. On the other hand, if M(q)>Q , our robustness measure indicates a serious weakness corresponding to high quality of the unmarked image.

3.2. Why Modify WPSNR?

1) WPSNR does not consider the ROI(Region of interest) of the image. Therefore, the noise on ROI and ROB regions are given equal weightage.

2) Consider a situation where there are two distorted images having same MSE(Mean Square error). In one, distortion is concentrated at one part of the image and hence it is visible. In other, distortion is not visible because the distortion is spread on the whole image with low intensity. If error distortion is localized on an image it will be annoying to the viewer while if it is spreaded on whole image it will be less annoying even though the total MSE is the same.

3)If the distortions are scattered as separate isolated areas,it will be more annoying than it is gathered together at one area. WPSNR metric does not

consider whether the distortions are formed in isolated areas or not.These three aspects discussed above need attention. If the WPSNR is modified to rectify these limitations, a more meaningful metric can be generated.

3.3. Algorithm for EWPSNR

1)Read reference image H(i; j) and distorted image H'(i; j). Obtain the NVF of the image.

2) Create a binary image B(i; j) corresponding to Region of Interest (ROI) of the image such that binary '1' is assigned at ROI area and binary '0' is assigned at Region of Background (ROB) area.

3) Fix the Just Noticable Difference(JND) value according to the subjective assessment.

4) Initialize i = j = 1.

5) If B(i; j) = 1, R = 9. Otherwise, R = 1 where R is an index corresponding to ROI. The minimum value is selected as 1 because the Mean Square Error(MSE) will remain same as in the original expression for WPSNR. R = 9 corresponds to maximum penalty to noise in ROI part.

6) Find difference between the images. If Difference<JND; then Th = 1. Otherwise, Th = 9. Th is the threshold value corresponding to JND value. Minimum value of Th is selected as unity due to the reason stated in step 5.

7)A new variable is defined: $\lambda = R \times \partial^2 \times Th$

8) If $\partial! = 0$, then H(i; j) = $2^B - 1$, else H(i; j) = 0, where B is the resolution of the image.

9) If not last pixel, increment i and j and go to step 5.

10)Obtain denominator D of the expression:

$$D = \sum ij \sum ij \frac{(NVF^2 \times \lambda)}{M \times N}$$

11)Calulate EWPSNR in db as:

$$EWPSNR = 10log_{10}(\frac{B^2 - 1}{n \times D})$$

4. Simulation Results

Modules implemented are described below: An image to be watermarked with text is considered(lena image).The Text is watermarked on the image(case of visible watermarking).Four attacks such Ratotation,applying Gray effect,addition of noise,fixed resolution are considered.

Figure1: Lena image to be watermaked.

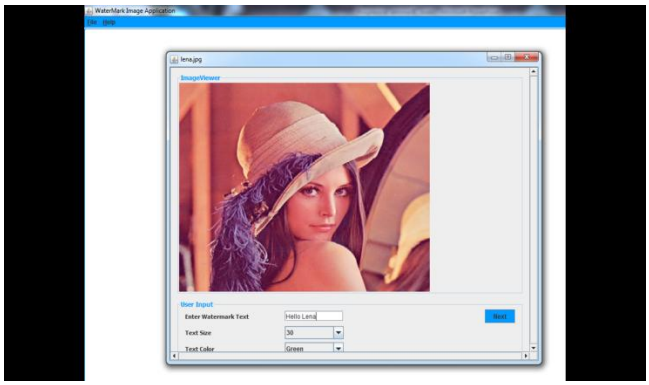


Figure 2: Text watermarked(in green colour) on lena image.

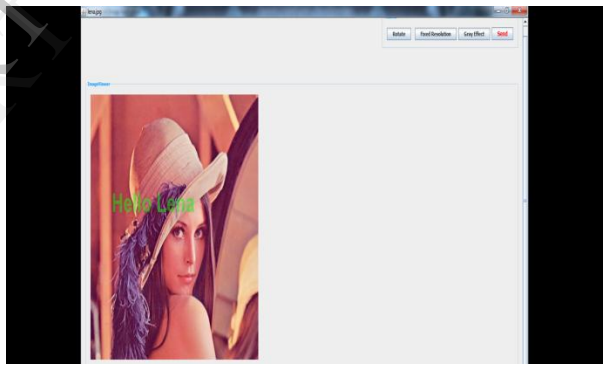


Figure 3:After applying rotation attack

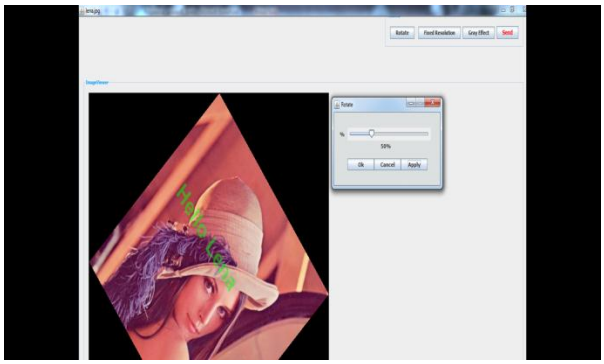


Figure 4: After applying fixed resolution attack.

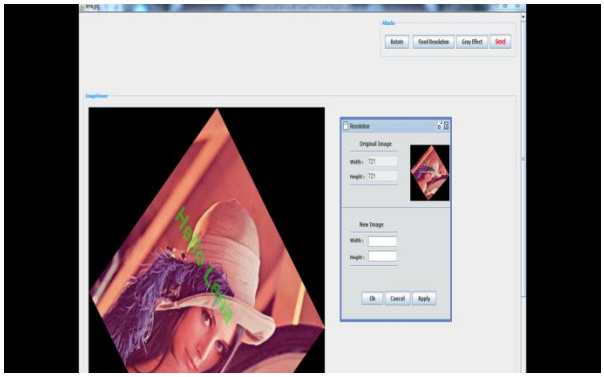


Figure 5:Increasing/reducing size of watermarked original image.

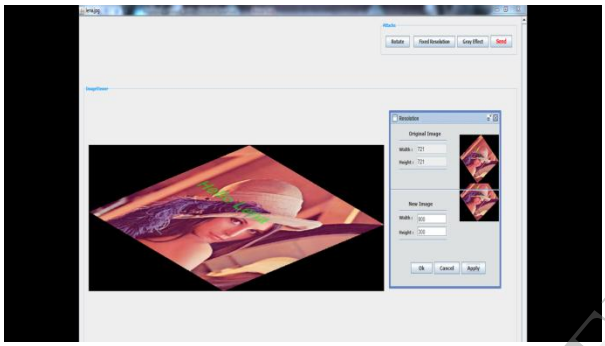
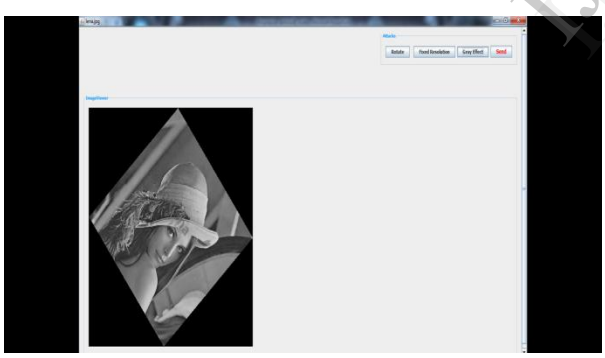


Figure 6:After applying gray effect



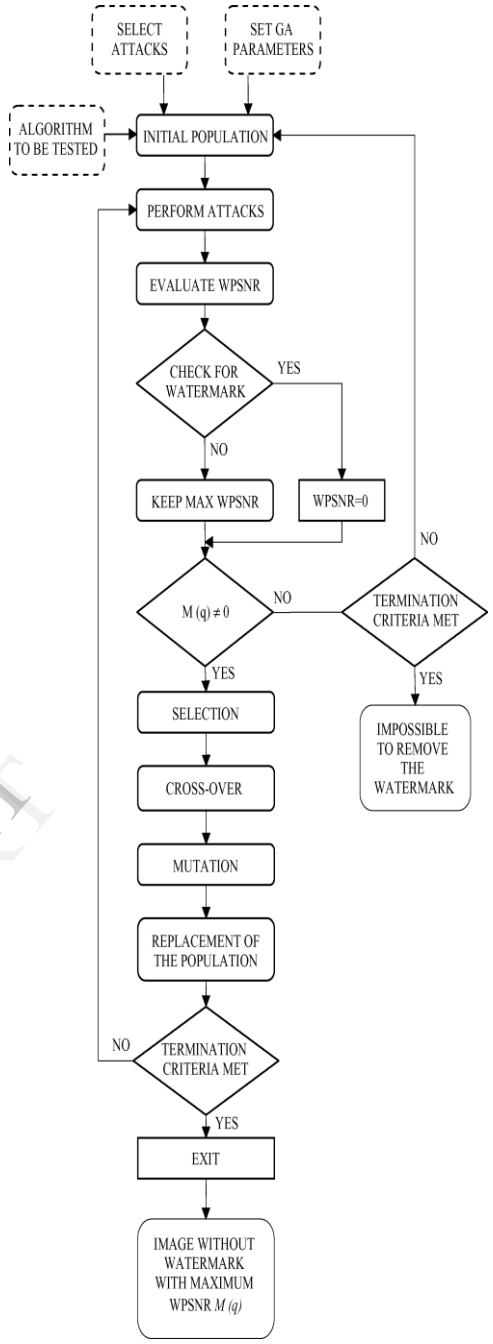


Figure 1: Block diagram of proposed work

The final output will be shown in tabular format as follows:

Table 1:Final Output

Image	Watermarking Technique	q	M(q)	MSE	SNR	PSNR	EWPSNR	Attacks R F G	Order	Output
Say Lena	Visible								R-F-G	Non Robust
Boat	Invisible								F-G-R	Robust

5. Conclusion

An innovative benchmarking tool have been presented to evaluate the robustness of any digital watermarking technique considering the quality of the unmarked images in terms of perceived quality. Therefore, a new metric based on WPSNR is introduced. The goal is to remove the watermark from a content while maximizing perceptual quality. So, given a set of attacks,we look for a parameterization able to remove the watermark, optimizing the WPSNR of the unmarked image.The poor correlation of PSNR and WPSNR with HVS, was explored and experimentally proved the superiority of the proposed metric EWPSNR. The new fidelity metric can be used for the evaluation of the fidelity of images in the areas of compression, filtering, denoising,data embedding etc.

6. References

[1] Giulia Boato, Valentina Conotter, Francesco G. B. De Natale, , and Claudio Fontanari:" Watermarking Robustness Evaluation Based on Perceptual Quality via Genetic Algorithms", IEEE Transaction on information forensics and security,vol 4,No 2,June 2009.

[2] Fabien A. P. Petitcolas,"Watermarking schemes evaluation", in IEEE Signal Processing, vol. 17, no. 5, 2000, pp. 58–64.

[3] Fabien A. P. Petitcolas, Ross J. Anderson, Markus G. Kuhn: "Information Hiding:A Survey",Proceedings of IEEE, vol. 87, No. 7, July 1999.

[4] Fabien A. P. Petitcolas, Ross J. Anderson, Markus G. Kuhn: "Attacks on copyright marking systems", in Proc. Of David Aucsmith (Ed), Information Hiding, U.S.A., 1998.

[5Jan C. Vorbruggen,Franois Cayre:"The Certimark Benchmark:Architecture and future perspectives", 2002 IEEE.

[6] V. Solachidis, A. Tefas, N. Nikolaidis, S. Tsekeridou, A. Nikolaidis,I.Pitas, ``A benchmarking protocol for watermarking methods'', in IEEE Int. Conf. on Image Processing (ICIP'01), 2001, pp. 1023-1026.

[7]Zhou Wang, and A-C Bovik, Mean Squared Error: Love It or Leave It?,IEEE Signal Processing Magazine, 98-117, January 2009.

[8] Wen Lu, and Xinbo Gao, and Xuelong Li, and Dacheng Tao, An image quality assessment metric based contourlet, University of London, 2008.

[9] K. A. Navas and M. Sasikumar Image Fidelity Metrics: Future Directions,IETE Technical review, Vol 28, Issue 1, Jan-Feb 2011.