Quantitative Evaluation Criteria for the Selection of Standard Images used on Watermarking Performance Test

Sang-Il Na, Ju-Kyong Jin, Dong-Seok Jeong; Inha University; Incheon, Korea
Yung-Eun Jung; TTA; Sungnam, Korea

Abstract

The purpose of this paper is to present the quantitative evaluation criteria for the selection of standard images which are used to objectively evaluate the performance of PAT such as watermarking or fingerprinting technology.

When evaluating the performance of PAT, the result could be varying by the image used and evaluation criteria employed. Therefore to evaluate the performance of watermarking technologies objectively, standardizing of test images is essential. This paper provides the quantitative evaluation guidelines for the selection of standard test images which could be used to evaluate the performance of watermarking technologies objectively.

Experimental result shows that the proposed evaluation criteria have relatively high consistency in evaluating the PAT technologies.

Motivation

The importance of DRM technologies, especially the watermarking technology, is getting larger and larger as the demand for the digital contents is increased. But the standard for the evaluation of watermark technology is not set up properly due to the conflicts between interested parties and technical difficulties. When evaluating the performance of PAT, the result could be varying by the image used and evaluation criteria employed. Therefore to evaluate the performance of watermarking technologies objectively, standardizing of test images is essential. This paper provides the quantitative evaluation guidelines for the selection of standard test images which could be used to evaluate the performance of watermarking technologies objectively.

This paper describes standard test images with quantitative criteria to objectively evaluate the performance of watermarking products developed by DRM industries. By providing the opportunity to evaluate the DRM product in objective and quantitative manner, watermark industry can expedite its technology development and consumer can get objective and universally validated performance result.

Key Technologies

Four key concepts are involved to set up the experiment and derive the consistency property from the result. They are watermarking method, attacking algorithm, performance measure, and quantitative image evaluation measure. We will explain each of these concepts in detail.

Watermarking

The property of digital contents which make them be copied perfectly has created several serious copyright problems. The copyrighted digital contents can be easily copied and this characteristic has caused major concerns to content providers who produce digital contents commercially. In order to protect the interest of the content providers, we need some techniques to represent the original copyright of contents and then digital watermarking can be one of solutions. Digital watermarking is a branch of information hiding techniques which is used to hide copyright information imperceptibly in digital media such as digital music, images, or video. Figure 1 shows the flowchart of general watermarking algorithm.

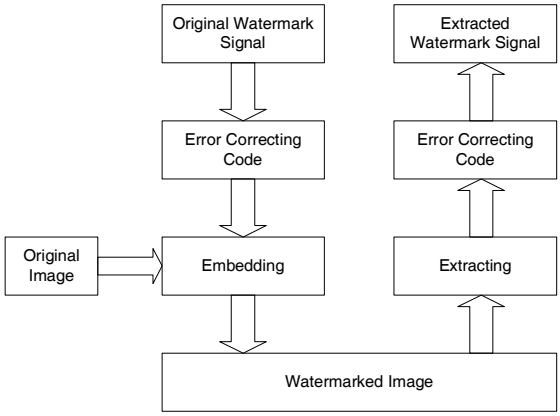


Figure 1. *The flowchart of general watermarking*

Numerous watermarking methods are developed and announced. For a complete listing of the watermarking method, please refer to the reference [1].

Requirements of Watermarking

Cox et al. suggested three main requirements of digital watermarking [2]. They are transparency, robustness, and capacity. In this paper we focused on robustness.

Transparency or Fidelity

The digital watermark should not affect the quality of the original image after it is watermarked. Cox et al. define transparency or fidelity as "perceptual similarity between the original and the watermarked versions of the cover work" [1]. Watermarking should not introduce visible distortions because if such distortions are introduced it reduces the commercial value of the image.

Robustness

Cox et al. define the robustness as the "ability to detect the watermark after common signal processing operations". Water-

marks could be removed intentionally or unintentionally by simple image processing operations such as contrast or brightness enhancement, gamma correction etc. Hence watermarks should be robust against various attacks.

Capacity or Data Payload

Cox et al. define capacity or data payload as "the number of bits to be needed to encode a watermark within a unit of time or work". This property describes how much data should be embedded as a watermark to successfully detect during extraction. Watermark should be able to carry enough information to represent the uniqueness of the image. In general, different application needs different payload requirements.

Attacking

To check the robustness of watermarking algorithm, we intentionally deteriorate the embodied watermarking information by attacking the watermarked image.

Attacks are tools to decrease the robustness of watermark. If only partial knowledge is available (for example, the exact location of the watermark in an image is unknown), then attempts to remove or destroy a watermark should result in severe degradation in fidelity before the watermark is lost. There are numerous ways of attacking as summarized in Table 1.

Table 1: List of attacking methods on watermarking

rotation	translation	Up sampling
Down sampling	filtering	clipping
A/D or D/A conversion	compression	flip
Geometric modification	shearing	Aspect ration

In general, those watermarking methods can be categorized into three areas as explained below.

Common signal processing

The watermark should still be retrieved even if common signal processing operations are applied to the watermarked data. These include digital-to-analog and analog-to-digital conversion, resampling, requantization including dithering and recompression, and common signal enhancements such as image contrast and color, or filtering.

Common geometric distortions

Watermarks in image and video data should also be immuned from geometric image operations such as rotation, translation, cropping and scaling.

Subterfuge attacks (collusion and forgery)

The watermark should be robust to collusion by multiple individuals who each possess a watermarked copy of the data. The watermark should be robust to combining copies of the same data set to destroy the watermarks. Furthermore, if a digital watermark is used in litigation, it must be impossible for colluders to combine their images to generate a different valid watermark with the intention of framing a third party.

Performance Measure

We need to define the performance measure of watermarking algorithm. In general, the performance is measured by comparing the extracted watermarking data with the originally embedded one. The comparison can be quantified by computing the correlation between them as described in Equation 1. Equation 1 is normalized correlation measure. W is the original watermark and W' is the extracted watermark.

$$NC(W, W') = \frac{\sum WW'}{\sqrt{\sum W_i^2 \sum W'^2_i}} \quad (1)$$

Quantitative Image Evaluation Criteria

Images can be categorized in many ways based on the criteria used. In this paper, our goal is to evaluate the performance of watermarking technologies. So we define the 5 evaluation criteria, 4 in spatial and 1 in frequency domain respectively. For each criterion, we divide images into 3 levels by thresholding the computed criteria. This makes total of 243(= 3 levels**5 criteria) subgroups of images which is too many to handle. So typically we may use one or two from spatial domain and one from frequency domain which result in 9 or 27 categorization

Let us explain the each criterion in detail.

Brightness

This criterion evaluates the overall brightness of the subject image. By computing the average gray level of pixels, we classify the given image as one of three groups according to the thresholds given in Table 2.

Table 2: Evaluation criteria for brightness

Level	Brightness range	Meaning
1	$0 \leq B < 85$	Dark
2	$86 \leq B < 170$	Medium
3	$171 \leq B \leq 255$	Bright

Complexity

This criterion measures how much information is contained in the image. Complexity is derived by computing edge levels using 4-level FCM algorithm and discarding level 1. We classify the given image as one of three groups according to the thresholds given in Table 3.

Table 3: Evaluation criteria for complexity

Level	Complexity value	Meaning
1	2	Low complexity
2	3	Medium complexity
3	4	High complexity

Repeatedness

This criterion measures the repeatedness of similar pattern in the subject image. Repeatedness is derived using texture browsing which is explained in MPEG-7 [3]. We classify the given image as one of four groups according to the thresholds given in Table 4.

Table 4: Evaluation criteria for repeatedness

Level	Range (%)	Meaning
1	$R < 5$	Irregular
2	$5 \leq R < 10$	Slightly regular
3	$10 \leq R < 20$	Regular
4	$20 \leq R$	Highly regular

Color distribution

This criterion measures the color property of the subject image. Color distribution is derived by clustering the color value using GLA and keeps the largest one and gets the percentile by comparing with the total area. We classify the given image as one of three groups according to the thresholds given in Table 5.

Table 5: Evaluation criteria for color distribution

Level	Range (%)	Meaning
1	$0 \leq C < 20$	Small distribution
2	$20 \leq C < 40$	Medium distribution
3	$40 \leq C \leq 100$	Large distribution

Energy concentration

This criterion measures the energy concentration of the subject image. Energy concentration is derived in frequency domain by computing the distribution of low, medium and high frequency components. Either DCT or DWT can be used. We classify the given image as one of three groups according to the thresholds given in Table 6.

Table 6: Evaluation criteria for energy concentration

Level	Range (%)	Concentration of Low frequency
1	$0 \leq E < 20$	High concentration
2	$20 \leq E < 55$	Medium concentration
3	$55 \leq E \leq 100$	Low concentration

Experiments

The justification of the proposed criteria can be certified by showing the consistency between the watermarking algorithm and its performance on image categorization upon watermarking attacks.

Consistency Check Methodology

We used two evaluation criteria with 3 levels each, which resulted in 9 categories. For all images belong to one particular group among 9 categorizations, we derive the average correlation values under four conditions, which is the combination of two watermarking methods and two attacks.

Experimental Condition

Used Watermarking

Two watermarking methods have been employed for the experiment. They are Cox algorithm in DCT domain and Kim's algorithm [4] in wavelet domain. Embedding strength is 0.3 in both algorithm and Kim's algorithm used 4-level wavelet.

Used Watermark

We used Pseudo-Random Gaussian sequence. It is a sequence of numbers comprised in 1 and -1. This watermark sequence's total length is 100.

Used Attack

Two attacks have been applied to the watermarked image. They are filtering attack in frequency domain and noise insertion attack in spatial domain.

Used Performance Measure

The measure to evaluate the performance of watermarking is the correlation between the original and extracted watermarking information.

Used Evaluation Criteria

Two evaluation criteria have been employed. They are complexity measure in spatial domain and energy concentration in frequency domain. Therefore the image set has been divided into 9 groups.

The size of image set used in experiment is 243 and the number of images in each group is given in Table 7.

Table 7: The number of images in each group

Spatial / Energy	Low Complexity	Medium Complexity	High Complexity
High Concentration	26	23	8
Medium Concentration	20	73	35
Low Concentration	Non	26	32

In Appendix, we provide a few sample images with varying combination which are chosen from Mammoth DVD [5] as explained in Table 7.

Experimental Result and Analysis

As can be seen in Table 7, many ordinary images are fall into categories where complexity is medium and frequency concentration is medium. For those images in this category, the performance of Cox watermarking algorithm is superior to that of Kim's watermarking as shown in Table 8. The number in each cell is the average of correlation extracted in this cell.

Table 8: Experimental result for medium complexity and medium concentration

Attack / Algorithm	Noise Insertion	Filtering
Cox	0.43	0.61
Kim	0.23	0.46

But for those images with low complexity and high concentration of low frequency, Cox performance is better in noise insertion attack, but Kim's watermarking is superior to Cox's one in case of filtering attack as shown in Table 9.

Table 9: Experimental result for low complexity and high concentration

Attack / Algorithm	Noise Insertion	Filtering
Cox	0.36	0.47
Kim	0.25	0.57

For those images with high complexity and high concentration of low frequency, Kim's watermarking is superior to Cox's one in both attacks as shown in Table 10.

Table 10: Experimental result for high complexity and high concentration

Attack / Algorithm	Noise Insertion	Filtering
Cox	0.31	0.42
Kim	0.37	0.48

In general, Cox performance is strong in noise insertion attack in spatial domain and Kim's performance is strong in filtering attack in frequency domain.

Conclusion

As presented in experimental result, the proposed evaluation criteria for the classification of images show consistency in evaluating the PAT performance. Further study will eventually be able to set up firm evaluation criteria which can be used universally in image processing society.

Acknowledgement

This research has been supported in part by TTA of Korea.

References

[1] Vidyasagar M. Potdar, Song Han, Elizabeth Chang , "A Survey of Digital Image Watermarking Techniques", IEEE International Conference of Industrial Informatics, pp.709-716 (2005)

[2] Ingemar J. Cox, Joe Kilian, F. Thomson Leighton and Talal Shamoon, "Secure Spread Spectrum Watermarking for Multimedia", IEEE Transactions on Image Processing, Volume 6, NO. 12, December 1997, pp. 1673-1678

[3] MPEG-7 Visual Group, "Text of ISO/IEC 15938-3/FDIS Information technology Multimedia content description interface – Part 3 Visual", ISO/IEC JTC1/SC29/WG11 N4358, Sydney, July 2001, pp.61-63

[4] Jong Ryul Kim, Young Shik Moon, "A robust wavelet-based digital watermark using level-adaptive thresholding", Proceedings. 1999 International Conference on Volume 2, Oct. 1999, pp. 226-230

[5] Mammoth DVD with 180,000 images from Amazon, UK.

Author Biography

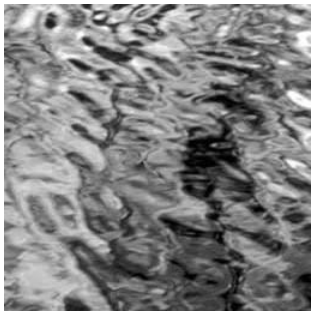
Sang-Il Na received his BS in Electronic engineering from Inha University, Incheon, Korea(2002) and his MS in Electronic engineering from Inha University, Incheon, Korea(2004). He is now in his doctoral process at Inha University.

Ju-Kyong Jin received his BS in Electronic engineering from Inha University, Incheon, Korea(2003) and his MS in Electronic engineering from Inha University, Incheon, Korea(2005).

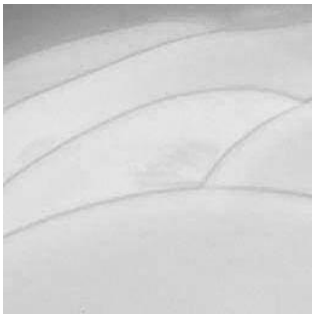
Dong-Seok Jeong received his BS in Electronic engineering from Seoul National University, Seoul, Korea(1977) and his MS and Ph.D. in Electronic engineering from Virginia Tech, Blacksurg, VA in 1985 and 1988 respectively. From 1988, Dr. Jeong is the faculty of Inha University, Incheon, Korea.

Appendix

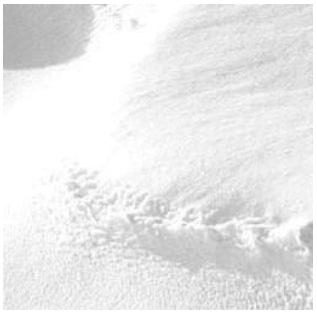
Medium complexity and medium concentration



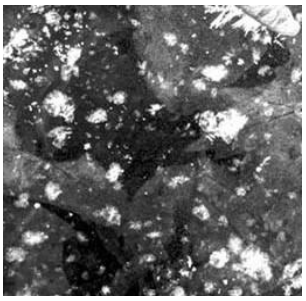
High complexity and medium concentration



Low complexity and high concentration



Medium complexity and high concentration



Medium complexity and low concentration

Medium complexity and low concentration