Journal of Information Hiding and Multimedia Signal Processing ©2010 ISSN 2073-4212
Ubiquitous International Volume **1**, Number **4**, October **2010**

Robust Image Hashing Based on Statistical Invariance of DCT Coefficients

Fa-Xin Yu
School of Aeronautics and Astronautics
Zhejiang University
Hangzhou 310027, P.R.China.
fxyu@zju.edu.cn

Yan-Qiang Lei and Yuan-Gen Wang
School of Information Science and Technology
Sun Yat-Sen University
Guangzhou 510275, P. R. China.
is04leiy@mail2.sysu.edu.cn; wygen@mail2.sysu.edu.cn

Zhe-Ming Lu
School of Aeronautics and Astronautics
Zhejiang University
Hangzhou 310027, P.R.China.
zheminglu@zju.edu.cn

Received May 2009; revised June 2010

Abstract. *It is well-known that discrete cosine transform (DCT) coefficients can be statistically modeled as the generalized Gaussian distribution (GGD) whose shape parameters can be estimated by the maximum likelihood (ML) estimation method. This paper presents a novel image hashing scheme based on the statistical invariance of DCT coefficients, where we extract the invariant parameters with the modified ML principle. Experimental results show that the proposed hash can resist most content-preserving operations such as JPEG compression, filtering, scaling, brightness enhancement, histogram equalization and rotation with small angles.*

Keywords: Image hash, Content authentication, Discrete cosine transform, Generalized Gaussian distribution, Maximum likelihood estimation

1. Introduction.

Image hashing is a technique to extract the robust perceptual feature from an image to form its compact representation, which can be found applications in copyright protection, content authentication and image retrieval. Robustness to content-preserving distortions and fragility to malicious attacks are two important requirements in designing a hashing scheme. Recently, many perceptual image hashing schemes have been published, which can be roughly classified into methods based on image statistics [1], relations [2], preservation of coarse image representation [3] and low-level image feature extraction [4]. These methods first perform the DCT or DWT transform on the original image, and then directly make use of the coefficients to generate hashes. However, these hashes are very sensitive to global as well as local distortions that do not cause perceptually significant changes to the images. In this paper, we propose a novel hashing scheme based on the distribution of DCT coefficients.

2. **Statistical Distribution of DCT Coefficients.** Over the past two decades, there have been various studies on the distribution of the DCT coefficients for images. They concentrate on fitting the empirical data from different pictures with a variety of well known statistical distributions. Reininger and Gibson [5] pointed out that the DC coefficient is best modeled as a Guassian distribution, and the AC coefficients are best modeled as a Laplacian distribution with the Kolmogorov-Smirnow (KS) tests. The generalized Gaussian distribution (GGD) was used to model the DCT coefficients by Mller [6] with the tests, where the Maximum Likelihood (ML) formula is employed to estimate the shape parameters [7]. To reduce the computational complexity, Krupiski and Purczyski [8] proposed an approximated fast estimator for the shape parameter of GGD. In this paper, we adopt the GGD model in [6] that is defined as

$$f(x) = \frac{v\alpha(v)}{2\sigma\Gamma(1/v)} \exp\{-[\alpha(v)|\frac{x}{v}|]^v\} \tag{1}$$

with

$$\alpha(v) = \sqrt{\frac{\Gamma(3/v)}{\Gamma(1/v)}} \tag{2}$$

where v denotes the shape parameter and σ denotes the standard deviation of the generalised Gaussian function, both positive real valued. $\Gamma(t)$ is the gamma function defined as follows

$$\Gamma(t) = \int_0^\infty u^{t-1}e^{-u}du \quad t > 0 \tag{3}$$

If a random variable (RV) has a PDF of Eq. (1), then we can declare that the RV accords with the GGD. Several special cases must be considered. If $v{\to}0^+$, then $f(x)$ becomes a dirac delta function distribution. If $v{\to}\infty$, then $f(x)$ approaches a uniform distribution. For the special cases v=1 or v=2, the generalized Gaussian function becomes a Laplacian or a Gaussian PDF. It is proved that the ML estimation performs better to fit the GGD parameter. Assume a RV has n samples $x_1, x_2, \ldots, x_n$, the ML estimation formula for the GGD parameter can be obtained through solving the following equation

$$\frac{\psi(1+1/v)+\log(v)}{v^2} + \frac{1}{v^2}\log(\frac{1}{n}\sum_{i=1}^n |x_i|^v) - \frac{\sum_{i=1}^n |x_i|^v \log(x_i)^v}{v\sum_{i=1}^n |x_i|^v} \tag{4}$$

where

$$\psi(\tau) = -\gamma + \int_0^1 (1-t^{\tau-1})(1-t)^{-1}dt \tag{5}$$

and γ=0.577 denotes the Euler constant. The root of Eq. (4) gives the ML estimation $\hat{v}$. Then the standard deviation estimation can be obtained as follows

$$\hat{\sigma} = \left[\frac{(\hat{v}\alpha(\hat{v})^{\hat{v}}\sum_{i=1}^n |x_i|^{\hat{v}})}{n}\right]^{1/\hat{v}} \tag{6}$$

3. **Proposed Algorithm.** It has been found that the DCT coefficients in the low or middle frequency sub-bands are robust to general image manipulations. Thus good estimations of and v can σ keep this robustness. In practice, we modify Eq. (4) with log10 instead of log empirically to obtain more strong robustness to normal signal processing. Our scheme can be described as follows.

Step 1: Partition the input image of size $M{\times}N$ into $M{\times}N/256$ non-overlapping blocks of 16×16 pixels, denoted as B_i, where i=1,2,. . .,$M{\times}N/256$. Then we perform the DCT on each block B_i, and select the first 9 AC coefficients in the zigzag order, denoted as S_ij, where j=1,2,. . .,9. We then define $x_j=(s_{1j}, s_{2j},\ldots,s_{(M\times N/256)j})$.

Step 2: Since the sample set X_j is obtained, we can use the modified ML estimation formula to compute the statistical invariant parameter V_j.

Step 3: Based on the 9 values V_j, j=1,2,. . .,9, we compute the binary result of the big-and-small relationship between any two of them to generate the hash with the length of C_2^9=36 bits.

4. **Experimental Results.**

To evaluate the performance of the proposed method, the 512×512 Lena image with 8bits/pixel resolution is used as the test image. The Lena image is divided into 1024 blocks of size 16×16 for statistical invariant extraction. Here, we use the bit error rate (BER) to measure the similarity between the hash of the original image and that of its processed version. The results in the rows but the last one of Table 1 and Table 2 show the estimated parameters for various versions of the Lena image based on the modified ML principle, while the last row of Table 1 and Table 2 shows the corresponding BER results. The first column denotes the 9 AC DCT coefficients in a 16×16 DCT block. From Table 1 and Table 2, we can find that the estimated parameters are invariant to content-preserving operations, and thus our proposed scheme can capture the main feature of the image and can tolerate most content-preserving operations.

Table 1. Estimated parameters $\hat{v}$ from various content-preserving versions of the Lena image and the corresponding BER values with respect to the original image (part 1)

	Original	JPEG(80)	JPEG(50)	JPEG(30)	Mean (3×3)
C_{01}	1.335	1.336	1.338	1.338	1.357
C_{02}	1.215	1.214	1.217	1.212	1.271
C_{03}	1.180	1.183	1.195	1.202	1.258
C_{10}	1.205	1.205	1.208	1.197	1.231
C_{11}	1.111	1.112	1.115	1.130	1.114
C_{12}	1.145	1.147	1.160	1.151	1.146
C_{20}	1.079	1.079	1.074	1.035	1.135
C_{21}	1.108	1.114	1.121	1.082	1.115
C_{30}	1.160	1.169	1.181	1.186	1.207
BER	0	0.028	0.028	0.028	0.111

To further evaluate the robustness and fragility properties, our algorithm is compared with Lin's [2] method on an image database with 4700 images. This database contains 94 original gray images (such as Lena, boat, peppers, baboon, goldhill, etc), each of size 512512. We perform 50 content-preserving operations with various parameters on each original image, including JPEG compression, filtering, and rotation. The comparison results are shown in Figs. 1-4 in terms of BER. From Figs. 1-3, we can see that the proposed scheme outperforms Lin's method under JPEG compression, filtering and rotation. Fig. 4 compares the capability of distinguishing dissimilar images, where each original gray image is compared with all the images in the database. From Fig.4, we can see that our method can obtain low BER values for similar images while obtaining high BER values for dissimilar images, however Lin's method obtain the BER values around 0.5, which means it is hard to determine whether an image is a dissimilar image of the input image or not, i.e., the uncertainty is biggest. From above results, we can see that our

Table 2. Estimated parameters $\hat{\upsilon}$ from various content-preserving versions of the Lena image and the corresponding BER values with respect to the original image (part 2)

	Median (3×3)	Low-pass Gaussian	Brighten (16%)	Scaling (0.8)	Histogram equalization
C_{01}	1.332	1.340	1.335	1.329	1.344
C_{02}	1.209	1.232	1.215	1.184	1.235
C_{03}	1.173	1.201	1.180	1.188	1.213
C_{10}	1.201	1.206	1.205	1.202	1.221
C_{11}	1.107	1.112	1.111	1.189	1.126
C_{12}	1.137	1.145	1.145	1.149	1.168
C_{20}	1.073	1.098	1.079	1.127	1.080
C_{21}	1.100	1.109	1.108	1.134	1.116
C_{30}	1.160	1.207	1.160	1.151	1.158
BER	0	0.056	0	0.167	0.028

proposed algorithm has higher capability of distinguishing content-preserving operations from dissimilar images.

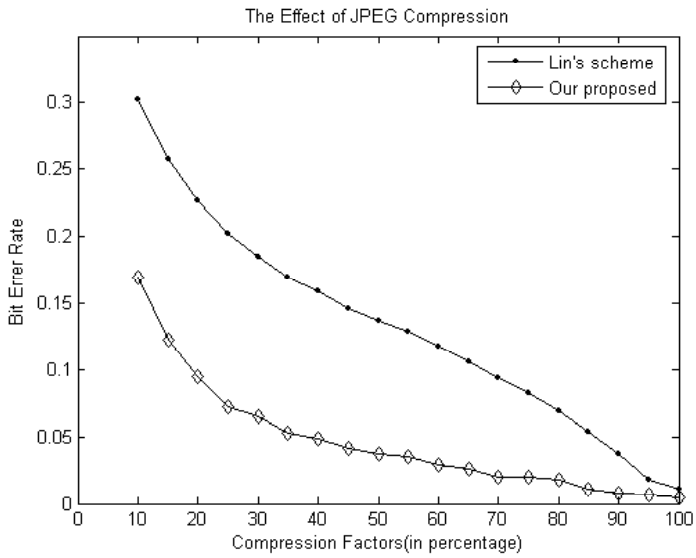

Figure 1. Comparisons of robustness between the proposed method and Lin's scheme under the JPEG compression operations with different QFs.

5. **Conclusions.** In this paper, a robust image hashing algorithm for image authentication is proposed. The statistical invariant parameters of DCT coefficients are estimated by the modified ML estimation firstly. Then the big-and-small relationship between any of two estimated parameters is used to generate the final hash. Experimental results demonstrate that our proposed technique is robust to most content-preserving operations like JPEG compression, filtering, brightness enhancement, histogram equalization and rotation with small angles.

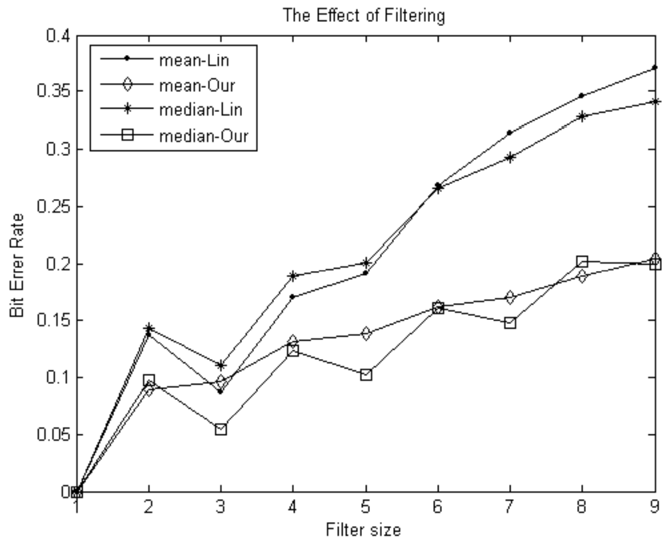

Figure 2. Comparisons of robustness between the proposed method and Lin's scheme under the filtering operations with different sizes.

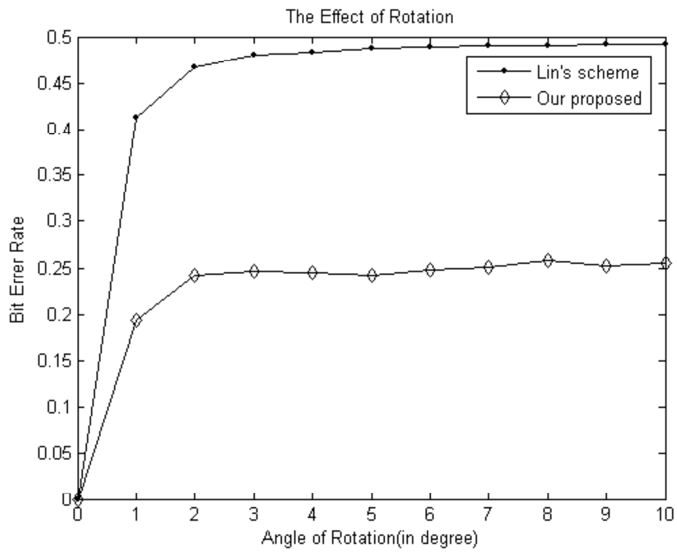

Figure 3. Comparisons of robustness between the proposed method and Lin's scheme under the rotation operations in different degrees.

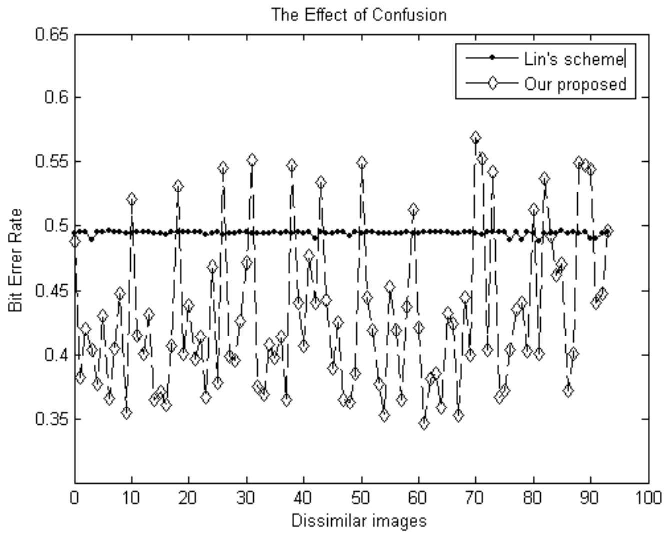

FIGURE 4. Comparisons of robustness between the proposed method and Lin's scheme using 100 dissimilar images.

REFERENCES

[1] R. Venkatesan, S. M. Koon, M. H. Jakubowski, and P. Moulin, Robust image hashing, *Proc. of IEEE International Conference on Image Processing*, vol. 3, pp. 664–666, 2000.

[2] C. Y. Lin, and S. F. Chang, A robust image authentication method distinguishing JPEG compression from malicious manipulation, *IEEE Trans. Circuits and Systems for Video Technology*, vol. 11, no. 2, pp.153–168, 2001.

[3] A. Swaminathan, Y. N. Mao, and M. Wu, Robust and secure image hashing, *IEEE Trans. Information Forensics and Security*, vol. 1, no. 2, pp. 215–230, 2006.

[4] V. Monga, and B. L. Evans, Perceptual image hashing via feature points: performance evaluation and tradeoffs, *IEEE Trans. Image Processing*, vol. 15, no. 11, pp. 3452–3465, 2006.

[5] R. Reininger, and J. Gibson, Distributions of the two-dimensional DCT coefficients for images, *IEEE Trans. Communications*, vol. 31, no. 6, pp. 835–839, 1993.

[6] F. Mller, Distribution shape of two-dimensional DCT coefficients of natural images, *Proc. of IEEE Electronics Letters*, vol. 29, no. 22, pp. 1935–1936, 1993.

[7] Y. Du, Ein spharish invariantes Verbunddichtemodell fur Bildsignale, *Arrchiv fur Elektronik und Ubertragungstechnik*, vol. AEU-45, no. 3, pp. 148–159, 1991.

[8] R. Krupinski, and J. Purczynski, Approximated fast estimator for the shape parameter of generalized Gaussian distribution, *Signal Processing*, vol. 86, no. 2, pp. 205–211, 2006.