A New Statistical Image Watermark Detector in RHFMs Domain using Beta Exponential Distribution

Panpan Niu
Liaoning Normal University
Jing Tian
Liaoning Normal University
Jialin Tian
Liaoning Normal University
Xiangyang Wang (wxy37@126.com)
Liaoning Normal University

Research Article

Keywords: Image watermarking, Beta-exponential distribution, FRHFMs domain magnitudes, locally most powerful test.

Posted Date: August 23rd, 2021

DOI: https://doi.org/10.21203/rs.3.rs-709977/v1

A New Statistical Image Watermark Detector in RHFMs Domain using Beta Exponential Distribution

Pan-pan NIU, Jing TIAN, Jia-lin TIAN, Xiang-yang WANG

***Abstract*—The detection of watermarks can be achieved by statistical approaches. How to select robust modeling object, appropriate statistical model, and decision rules is one of the major issues in statistical image watermark detection. In this paper, we propose a new image watermark detector in robust fast radial harmonic Fourier moments (FRHFMs) magnitudes domain, wherein the Beta exponential distribution model and locally most powerful (LMP) decision rule are used. We first investigate the statistical modeling of the robust FRHFMs magnitudes by the Beta exponential distribution. It is shown that the Beta exponential distribution model fits the empirical data more accurately than the formerly employed statistical distributions, such as the Cauchy, Weibull, BKF and Exponential, do. Motivated by the statistical modeling results, we design a blind image watermark detector in FRHFMs magnitudes domain by using Beta exponential distribution and LMP test. Also, we utilize the Beta-exponential model to derive the closed-form expressions for the watermark detector. We provide comparative experimental results to alternative approaches to demonstrate the advantages of the proposed image watermark detector.**

***Index Terms*—Image watermarking, Beta-exponential distribution, FRHFMs domain magnitudes, locally most powerful test.**

1. INTRODUCTION

With the rapid development of multimedia and Internet technologies, digital data can be easily acquired, represented, manipulated and distributed without any quality degradation. As a result, intellectual property right protection has become a major issue worldwide. Owing to its effectiveness and practicality, digital watermarking is one promising solution for copyright protection and integrity authentication in an open network environment. Digital watermarking technology can be used in many applications such as source tracking, secret communication, broadcast monitoring, billing security and so on. Two basic approaches regarding digital image watermarking include watermark decoding [1][2][3] and watermark detection [4][5][6][7]. In watermark decoding, the problem to be solved is the extraction of watermark information. While in watermark detection, we need to determine if particular watermark information exists in the given data using a binary decision criterion. This paper mainly studies the copyright protection of images, so watermark detection based on a binary decision criterion is sufficient to declare legal ownership. Watermark detection algorithms can be divided into two major categories base on whether the original signal is provided: non-blind detection [8] and blind detection [9][10]. When watermark carrier signals obey Gaussian distribution, the correlation-based detection method is optimal. However, research results have shown that digital signals in both the frequency and spatial domains do not obey Gaussian distribution [5]. Hence, the detection method considering statistical properties of the carrier image coefficients can improve the correctness of watermark detection.

Image watermark algorithms based on statistical model need to solve three basic problems, they are also important indicators to measure the pros and cons of a watermarking scheme, namely robustness, imperceptibility and capacity. Meanwhile, there is a

P.-P. Niu, J. Tian, J.-L. Tian and X.-Y. Wang are with the School of Computer and Information Technology, Liaoning Normal University, Dalian 116029, P. R. China.

Corresponding author: Prof. X.-Y. Wang, E-mail: wxy37@126.com.

mutually restrictive relationship between the three. Robustness is a core requirement of robust watermarking systems, and it is also a significant sign for judging the resistance of watermarking algorithms. The better a robust watermarking algorithm, the stronger its ability to resist attacks. It is a popular method to evaluate the robustness of detector by using receiver operating characteristic curve. The aim of this work is to enhance the balance between robustness and invisibility while making sure the watermark capacity. Invisibility means that the signal containing the watermark is not different from the original signal visually, and the peak signal-to-noise ratio (PSNR) is the most frequently used method to test imperceptibility in image watermarking. Capacity indicates the quantity of watermarking data that can be hidden. Hence, to maintain the robustness and invisibility of watermark signals in the relational database, we choose the multiplicative embedding method [11][7][12]] to achieve the embedded watermark.

According to different embedding domains, the image watermark is mainly separated into two categories: spatial [13] and frequency [1-6][14-16]. The spatial watermarking algorithm indicates that watermark data is directly inserted into the pixels of the original image. The operation of this method is simple, but the watermark is not robust enough to resist common signal attacks. In the frequency-domain watermark algorithms, watermarking is embedded by altering the image transform domain coefficients. Compared with spatial domain watermark embedding schemes, its robustness is improved to a certain extent. The most widely used transform domains include wavelet transform [6][7][10], non-subsampled shearlet transform (NSST) [17], non-subsampled contourlet transform (NSCT) [18-19], discrete cosine transform (DCT) [20], contourlet transform [5][16][12][21], discrete shearlet transform (DST) [9] and dual tree complex wavelet transform (DTCWT) [14][22]. In recent years, researchers have proposed a watermarking method considering geometric invariants. Before embedding and detecting the watermark, the geometric invariants of the original image are determined. The geometric attack invariant features are utilized to ensure the optimal watermark embedding position. In 2000, Alghoniemy et al. [23] used 7 Hu moment invariants to apply image moment to image watermarking technology for the first time. However, watermark detection methods that combine statistical model and moment invariant is still of great research significance. Therefore, this paper combines the anti-attack ability of geometric moments with statistical models to propose a robust watermark detector.

The accuracy of watermark detection is affected by many aspects. Besides watermark embedding objects, it also includes statistical model establishment, model parameter estimation and detector construction methods. Some statistical models are often used, mainly including the Bessel K Form (BKF) distribution [4][12], t location-scale distribution [11][16], generalized Gaussian (GG) distribution [10][14], Cauchy distribution [4][19], Gaussian mixture model (GMM) [1], Laplacian distribution [9], normal inverse Gaussian (NIG) distribution [5] and Weibull distributions [20][22]. To consider the correlation between coefficients more fully, multivariate Cauchy distribution [15], multivariate generalized Gaussian (MVGG) model [13] and Hidden Markov Model (HMM) [7][24] were proposed. Then, a valid closed expression based on Bayesian log-likelihood ratio test (LLRT) [5][15] is established. In addition, the performance of watermark detection is affected by the accuracy of the parameter estimation algorithm. At present, expectation maximization (EM) and maximum likelihood estimation (MLE) methods are widely used in parameter estimation of statistical models. The function of detector is to detect whether there is hidden binary information from the observed image coefficients. Watermarking detection is often regarded as binary hypothesis testing of signals. In the past studies,, the decision rules for constructing detectors include LLRT, the RAO test [18], generalized likelihood ratio test (GLRT) [14], locally most powerful (LMP) test [19] and log-likelihood ratio test (LRT) [9][21][22].

Although statistical models based digital watermark technology has been generally used in information security, the performance still has many room for improvement. First, embedding the watermark method directly by modifying the transform domain coefficients can not resist the geometric attack well. Second, a single distribution can not well describe the characteristics of coefficients distribution. Thirdly, the traditional parameter estimation methods have low accuracy or high time

complexity, so they cannot accurately calculate the parameters of the statistical model. Fourthly, the detectors using decision criteria such as GLRT or LRT have good detection effects on the Gaussian distribution. However, the detection probability is relatively poor for non-Gaussian distribution and weak signals. Therefore, a statistical model-based watermark detector needs a strong decision criterion.

In this paper, we propose a locally optimal (LO) image watermark detector by modeling FRHFMs magnitudes with Beta exponential distribution. The validity and superiority of the scheme are proved by the simulation experiment.

In conclusion, the characteristics of this method are as follows:

- Robust fast radial harmonic Fourier moment (FRHFMs) magnitudes is introduced to digital image watermarking domain, and is applied for embedding watermark message and developing watermark detector.
- We use Beta-exponential distribution to model the FRHFMs magnitudes, whose peak and heavy tail statistical characterization can be described accurately.
- The modified ML estimation algorithm is employed to calculate the parameters of the Beta-exponential distribution.
- Based on Beta-exponential distribution and LMP test, a locally optimal image watermark detector is developed. In addition, the closed-form expressions of the detection statistics are derived from the Beta-exponential model to verify the performance of the detector.
- The excellent performance of the proposed watermark detector is proved by a lot of experiments.

The remaining chapters are organized as follows. Section 2 mainly introduces the digital image watermarking technology based on a statistical model in recent years. The concept of the FRHFMs is briefly introduced, and the robustness of the FRHFMs magnitudes is studied in Section 3. Section 4 mainly studies the statistical characteristics of FRHFMs magnitudes and then uses Beta-exponential model to fit the moment magnitude coefficients. MMLE parameter estimation method is also given to improve the accuracy and reliability of the model. In Section 5, we detail the watermark embedding process of this scheme. Section 6 deduces the LO watermarking detector based on Beta-exponential model, and discusses the performance of the constructed detection method. In Section 7, we analyze the detection probability of the suggested watermarking detection method and contrast to other excellent detectors through simulation experiments. Section 8 draws conclusions.

2. RELATED WORK

The primary target of image watermark technology is to settle the balance problems among the transparency, payload and robustness of watermark information. Therefore, watermark methods based on statistical models have been widely studied.

In paper [16], an additive watermark detector has been proposed according to Neyman-Pearson (N-P) criterion in contourlet domain. This method has modeled the contourlet transform coefficients using t location-scale distribution. In [6][8][11][13] [16][18][20][22][23]new detection method based on 2D-GARCH model is proposed, which fully considering the dependencies between wavelet coefficients. Khalil et al. [14] used GG distribution for modeling in DT-CWT domain and developed an additive watermark detector using a generalized likelihood ratio test. However, the additive watermark algorithm is not strong in robustness and invisibility. And multiplication embedding rule can improve the detection rate of watermarking. Therefore, the multiplicative watermarking method is more popular in watermarking embedding. Wang et al. [19] developed a multiplicative watermark detector based on Cauchy distribution by using the LMP test criterion, which can well describe the local correlation of NSCT difference coefficients and improve the detection probability. Meanwhile, the robustness of the detector has been improved by using the multiplicative watermark embedding method. However, since Cauchy distribution is only suitable for symmetric data types, many coefficient features cannot be fully fitted. Therefore, it is necessary to select a more fit distribution

to build the model. Sadegh et al. [11] developed an optimal detector using t location-scale distribution to model the contourlet coefficients, wherein the receiver operating characteristics (ROC) curve has been obtained for testing the detection probability of the suggested detector in the contourlet domain. In [22], the digital image watermarking technology based on a binary hypothesis test was introduced. The statistical models such as Gamma, Rayleigh and Weibull have been used to fit the DT-CWT coefficients. But when images are subjected to geometric attacks, the detector is less robust.

Sadreazami et al. [5] developed a blind watermark detector modeling the Contourlet coefficients, and in which the transform coefficients obeying non-Gaussian distribution were modeled by normal inverse Gaussian distribution (NIG). Nonetheless, since the inter-scale correlations of the transform coefficients are ignored, Linear correlation detector has many shortcomings for non-Gaussian signals. Therefore, Amini et al. [4] developed a LO detector based on HMM model, which provided a better probability of detection than linear correlation detectors by using image signal statistics. Dong et al. [20] developed a full band watermark scheme in DCT domain, and constructed a LO detector based on Weibull distribution to detect whether DCT coefficients contain watermarks. Although the DCT has better noise immunity, it lacks some properties such as directionality, translation invariance and multiresolution. In [10], developed a blind watermark detector based on generalized Gaussian distribution (GGD) in wavelet domain by using Neiman-Pearson (NP) criterion. This watermark detector usually assumes that wavelet transform coefficients are isolated and uniformly distributed. Hence, characteristics of these coefficients such as correlation cannot be fully considered. In paper [24], a new watermark detection method based on a log-likelihood ratio test has been proposed in color images, which detected signals submerged in the noise by a binary decision criterion. The inter-channel correlations in RGB color channels and the inter-scale correlations of image coefficients have been considered by adopting the hidden Markov model.

In [7], proposed a multi-channel blind watermark detector based on color images, which used a log-likelihood ratio decision criterion to obtain a valid closed expression for the test statistics. In paper [15], a multiplicative watermarking scheme based on Bayesian log-likelihood ratio has been designed. To consider the inter-scale correlations of contourlet coefficients, a multivariate Cauchy distribution was introduced, which can accurately fit the distribution characteristics of the transform coefficients and eliminate the inaccuracy of the single model to the coefficients. In [9], introduced a watermark detector based on Laplace distribution to model DST coefficients, which was detected according to the principle of likelihood ratio test. In [12], a watermark detection method is designed according to maximum likelihood (ML) criterion, which used BKF distribution to model Contourlet coefficients, and they analyzed its receiver operating characteristics by Monte Carlo simulations. However, transformation domain coefficients have a weak ability to resist various attacks.

Hosny et al. [25] derived the new fractional-order multi-channel orthogonal exponent moments (MFrEMs), and proposed MFrEMs based color image watermarking algorithm. Zhou et al. [26] proposed a novel robust reversible watermarking (RRW) scheme based on the discrete wavelet transform (DWT), in which the Zernike moments based geometric correction is utilized to predict attack parameters. Xia et al. [27] proposed a geometrically invariant color medical image null-watermarking scheme based on quaternion polar harmonic Fourier moments (QPHFM). Based on quantization technique and the distribution of moment magnitude, Hosny et al. [28] inserted the watermark information into host color images by modifying the quaternion radial substituted Chebyshev moments (QSRCMs) magnitudes. Hosny et al. [29] presented a geometrically invariant color image watermarking method using Quaternion Legendre-Fourier moments (QLFMs). These moments based image watermarking schemes generally have better robustness, but they all ignore the tradeoff among imperceptibility, robustness and watermark capacity.

3. ROBUSTNESS ANALYSIS OF FRHFMS DOMAIN MAGNITUDES

3.1 An Introduction to FRHFMs

The gray image in polar coordinates is $f(r,\theta)$, then traditional radial harmonic Fourier moments (RHFMs) on the unit circle can be expressed as

$$\psi_{nm} = \frac{1}{2\pi}\int_0^{2\pi}\int_0^1 f(r,\theta)T_n(r)e^{-jm\theta}rdrd\theta \tag{1}$$

where $0 \le r < 1,\ 0 \le \theta \le 2\pi$, the RHFMs are denoted by ψ_{nm}, $m(|m| \ge 0)$ represents repetition and $n(n \ge 0)$ is order. The angular function $e^{(-jm\theta)}$ represents the Fourier exponential factor and $T_n(r)$ represents the radial function

$$T_n(r) = \begin{cases} \sqrt{1/r}, & while\ n = 0 \\ \sqrt{2/r}\cos n\pi r, & while\ n\ is\ even \\ \sqrt{2/r}\sin(n+1)\pi r, & while\ n\ is\ odd \end{cases} \tag{2}$$

The function set $P_{nm}(r,\theta) = T_n(r)e^{(-jm\theta)}$ is orthogonal inside unit circular satisfies

$$\int_0^{2\pi}\int_0^1 P_{nm}(r,\theta)P_{kl}^*(r,\theta)rdrd\theta = 2\pi\delta_{nk}\delta_{ml} \tag{3}$$

where δ is Kronecker delta and 2π indicates normalization factor. δ_{nk} and δ_{ml} represent Kronecker symbols, $P_{kl}^*(r,\theta)$ is the conjugate of $P_{kl}(r,\theta)$.

The original grayscale image $f(r,\theta)$ is reconstructed as

$$f(r,\theta) = \sum_{n=0}^{N}\sum_{m=-M}^{M}\psi_{nm}T(r)e^{(jm\theta)} \tag{4}$$

where ψ_{nm} denotes the RHFMs, and $T(r)$ is the radial function.

To obtain better performance, we adopted a fast radial harmonic Fourier moments (FRHFMs) algorithm [30] based on FFT. The traditional RHFMS for calculating the inscribed circle mapping has rotation invariance. Therefore, the inscribed circle mapping is still used in the image watermark for FRHFMs [30][31]. In addition, FRHFMs provide higher image reconstruction quality, lower computational complexity, lower noise sensitivity and magnitude invariance. The following describes the specific calculation method in the polar coordinate system.

In the unit circle, radial r_x and angular θ_y are first divided into H equal parts, and the unit circle is nearly segmented into H^2 small regions. So converting Cartesian coordinate system of the image with pixel $A \times A$ to $f_p(r_x,\theta_y)$ [31] in polar coordinates is

$$f_p(r_x,\theta_y) = f\left(-\left|r_x \times A/2 \times \sin\theta_y\right| + A/2 + 1, \left|r_x \times A/2 \times \cos\theta_y\right| + A/2\right) \tag{5}$$

where $r_x = x/H$, $\theta_y = 2\pi y/H$, $x, y = 0,1,\Lambda\ ,H-1$ and $H = 4A$.

In addition, the FRHFMS φ_{nm} obtained by FFT can be expressed as:

$$\begin{aligned}
&\varphi_{0,m} = \sqrt{2}T\left(H/2+1, H/2+1+m\right), \quad k=n=0 \\
&\varphi_{n=2k,m} = T\left(H/2+1-k, H/2+1+m\right)+T\left(H/2+1+k, H/2+1+m\right), \quad n=2k, k=1,2,\Lambda \\
&\varphi_{n=2k-1,m} = j\left(T\left(H/2+1+k, H/2+1+m\right)-T\left(H/2+1-k, H/2+1+m\right)\right), \quad n=2k-1, k=1,2,\Lambda
\end{aligned} \tag{6}$$

Where, T is the FFT of function $G_p\left(r_u,\theta_v\right)=f_p\left(r_u,\theta_v\right)\sqrt{r_u/2}$ that moves zero-frequency component to the center of the spectrum.

3.2 Robust FRHFMs Domain Magnitudes

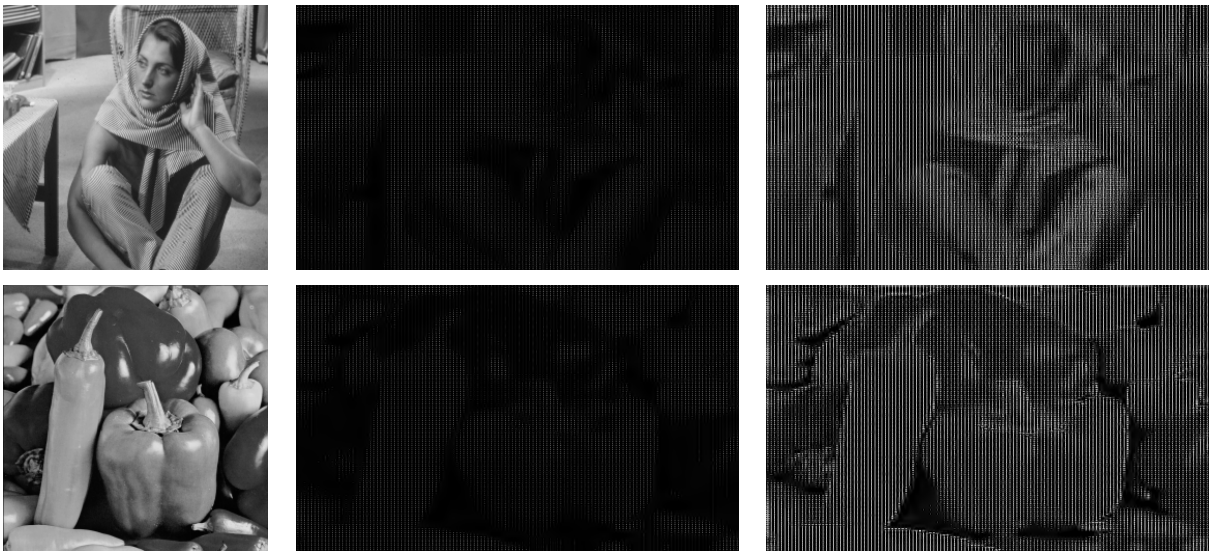
Because FRHFMS has geometric invariance, low time complexity and strong anti-noise ability [27], the FRHFMs amplitude of the image block is selected as the embedding position of the watermark in this paper. Firstly, the 512×512 pixel carrier image is split into 4*4 non-overlapping sub-blocks. Next, a second-order FRHFMs transform is performed in each block to get the FRHFMs magnitude of the host image. Fig. 1 shows second-order magnitude domains of different images with the size of 640×384.

In this paper, to verify that the FRHFMs magnitudes possess better robustness than spatial domain, and is more suitable for watermark watermarking, the normalized error is introduced. In order to facilitate the comprehensive comparison and evaluation, the paper needs to standardize the initial information to ensure that the error values in space and magnitude domains have the same order of magnitude. Data Z-score normalization is the most classic normalization way, which maps the data uniformly to the interval [0,1]. Then the normalized error is expressed as

$$P = \left|I_0 - I_{\text{attack}}\right| \tag{7}$$

$$E = \frac{1}{n}\sum_{i}^{n}\left|\frac{P_i-\mu}{\sigma}\right| \tag{8}$$

Here, I_{attack} denotes the attacked signal, and I_0 denotes the original unattacked signal. The mean of P is μ and the standard deviation of P is σ. The amount of signals is n and Σ is the cumulative sum. Table 1 records the normalized error values of the second-order FRHFMs magnitudes under different attacks. And the experimental images are three grayscale images of Lena, Barbara and Peppers.



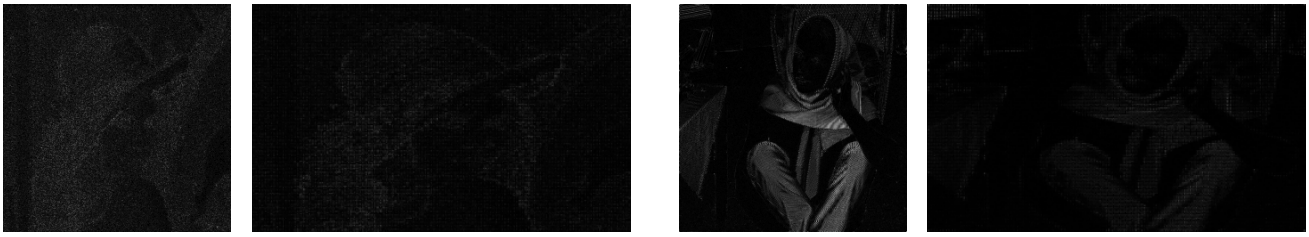
(a) Host images (b) FRHFMs magnitudes images (c) FRHFMs magnitudes images (×10)

Fig. 1. Original images and FRHFMs magnitudes images.

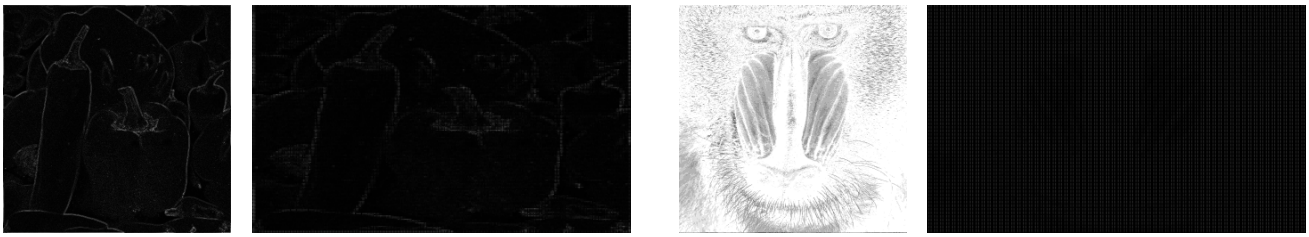
Table 1. Normalize error between the original signal and the attacked signal.

Attack types	Lena		Barbara		Peppers	
	FRHFMs magnitudes	Host image	FRHFMs magnitudes	Host image	FRHFMs magnitudes	Host image
JPEG Compression（QF=90）	**0.0244**	0.0651	**0.0252**	0.0518	**0.0280**	0.0668
JPEG Compression（QF=30）	**0.0339**	0.0838	**0.0314**	0.1087	**0.0371**	0.1137
Median filtering（9×9）	**0.0119**	0.0377	**0.0375**	0.0673	**0.0136**	0.0250
Median filtering（5×5）	**0.0111**	0.0271	**0.0260**	0.0611	**0.0076**	0.0184
Gaussian filtering（9×9）	**0.0216**	0.0518	**0.0412**	0.0700	**0.0219**	0.0383
Gaussian filtering（5×5）	**0.0207**	0.0511	**0.0389**	0.0698	**0.0212**	0.0380
Gamma correction γ =2	**0.0667**	0.8482	**0.0654**	0.7824	**0.0632**	0.7892
Gamma correction γ =0.9	**0.0341**	0.8882	**0.0343**	0.8504	**0.0325**	0.8346

It is well known that the smaller normalized error value means the stronger robustness. According to the normalized error formula, we test the robustness of four grayscale images: Lena, Barbara, Peppers and Baboon. Fig. 2 shows the error images of the spatial pixels and moment magnitudes.



(a) JPEG (QF=30) (b) Median filtering（5×5）



(c) Gaussian Filtering (9×9) (d) Gamma correction γ =0.9

Fig. 2. The normalized error images under various attacks where the left is the normalized error image of the host image and the right is the standardization error image of moment magnitudes.

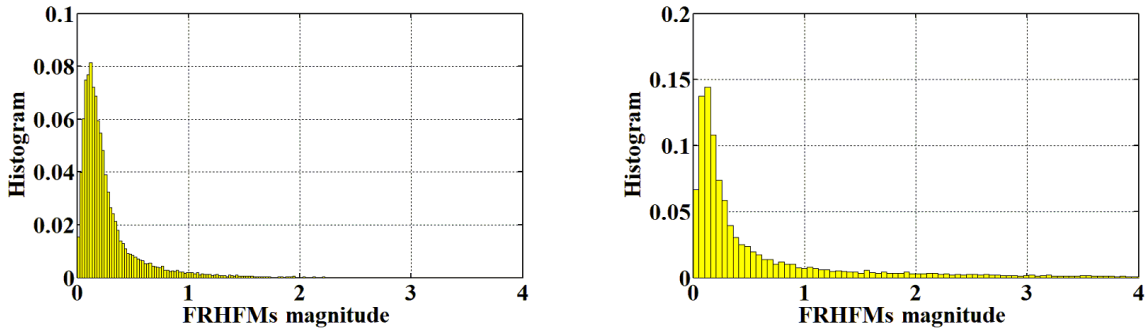
Table 1 shows the normalized error results of FRHFMs magnitudes coefficients are smaller than that of image pixels. And Fig. 2 shows that the normalized error images of FRHFMs magnitudes are darker than that of image pixels. Both the subjective and objective results indicate that the FRHFMs magnitudes are more robust than the spatial domain. Hence, this scheme selects local FRHFMs domain magnitudes to insert and detect watermarking information.

4. MODELING OF ROBUST FRHFMS DOMAIN MAGNITUDES

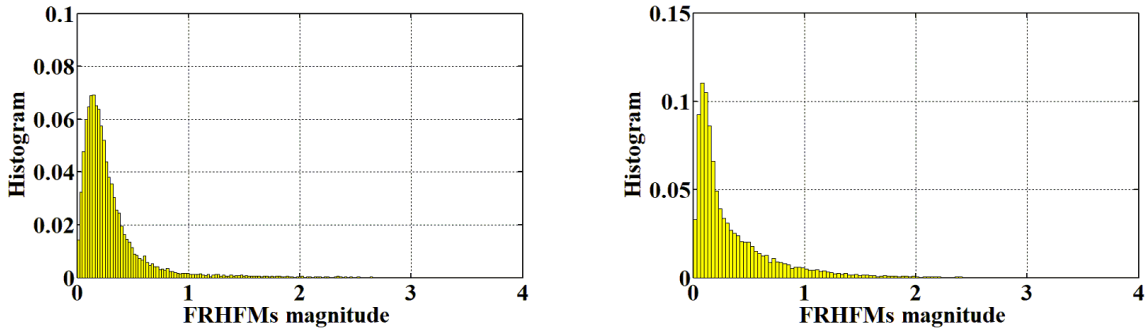
4.1 Statistical Analysis of Robust FRHFMs Domain Magnitudes

The model effectiveness in the FRHFMs magnitudes affects the performance of the suggested watermark method, and one of the key steps in accurate modeling is to study the distribution characteristics of FRHFMs magnitude coefficients. First, each test image with a size of 512×512 is divided into N_{block} non-overlapping sub-blocks of $n \times n$ in size, and the second order FRHFMs of the image blocks is calculated to obtain the moment magnitudes of each block. The most stable moment magnitude in each block is selected to form N_{block} magnitude coefficients.

Here, we take four typical grayscale images as examples and use distribution histogram and kurtosis value to analyze the edge statistical character of FRHFMs magnitudes. In the experiment, the carrier images with 512*512 pixels are chosen, and each image is split into 16384 non-overlapping sub-blocks, and FRHFMs of each image block are calculated. The position (2, 2) of each block is chosen to form a total of 16384-moment magnitudes and Fig. 3 provides the histograms of these moment magnitudes. We can clearly see from the histogram that the FRHFMs magnitude coefficients have the feature of sharp peak and heavy tail. The kurtosis values are 16.7605, 11.3751, 21.5277 and 15.1866 respectively, which are far greater than 3, indicating that they have non-Gaussian distribution characteristics. Therefore, a reasonable model is needed to accurately describe the characteristics of the magnitude coefficients.



(a) Lena (b) Barbara



(c) Peppers (d) Boat

Fig. 3. Distribution histograms of FRHFMs magnitude coefficients.

4.2 Statistical Modeling of Robust FRHFMs Domain Magnitudes

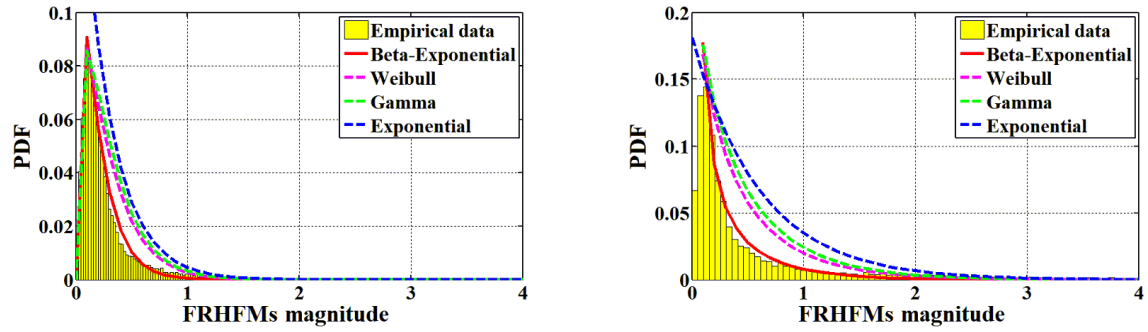
The performance of the watermark detector largely determined by the modeling accuracy of the FRHFMS magnitudes, so Beta-exponential distribution [3][32] suitable for the magnitudes coefficients is selected to describe the statistical characteristics of the FRHFMs magnitudes in this scheme.

The Exponential distribution is a very simple distribution function. However, the three-parameter Beta-exponential distribution appears, which effectively makes up for the deficiency of two-parameter exponential distribution. Then the probability density function (PDF) $f(x_i;k,m,n)$ of Beta-exponential distribution is

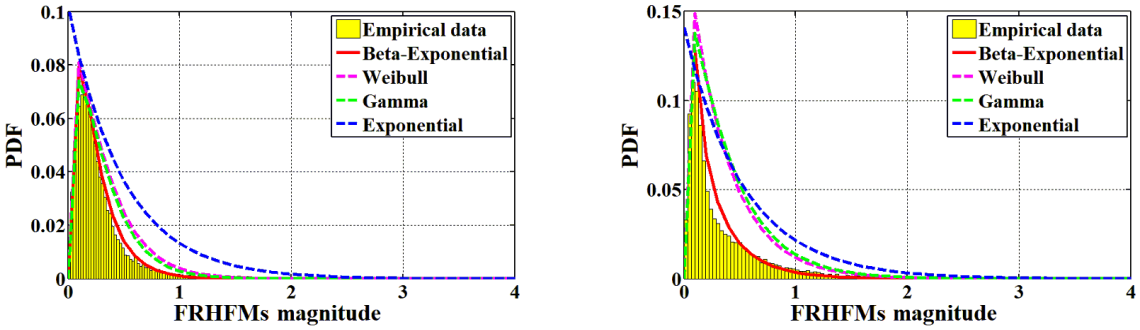
$$f(x_i;k,\alpha,\beta)=\frac{k}{C(\alpha,\beta)}e^{-\beta k x_i}\left(1-\exp^{-kx_i}\right)^{\alpha-1} \tag{9}$$

Where, k is the scale parameter , α and β denote the shape parameters of Beta-exponential distribution function. Here, $C(\alpha,\beta)=\Gamma(\alpha)\Gamma(\beta)/\Gamma(\alpha+\beta)$ and $x_i>0$ denotes the ith random variable. And the distribution has the characteristics of high peak and heavy tail.

We next study how to precisely select the appropriate model to fit the FRHFMs magnitudes. In Fig. 4, the modeling results of the magnitude coefficients, in which four images are fitted by different distribution functions. It is observed that the Beta-exponential model has a higher fitting degree than other distributions. Hence, the Beta-exponential distribution can delineate the FRHFMs magnitudes more accurately..



(a) Lena (b) Barbara



(c) Peppers (d) Boat

Fig. 4. Fitting graphs of FRHFMs magnitude coefficients.

In addition to the subjective tests above, we also compare the results based on the Kolmogorov-Smirnov (KS) metric. The KS test value is calculated as

$$Q_{ks} = \max\left|C_e(x) - C_t(x)\right| \tag{10}$$

Among them, $C_t(x)$ and $C_e(x)$ denote the referenced and empirical cumulative distribution function respectively. The smaller the KS value, the better the fitting effect of the distribution function used. In this paper, the FRHFMs magnitudes of Lena, Barbara, Peppers and Boat images are fitted using different distributions. Then, the KS test values of each distribution are calculated separately. Table 2 shows that the KS test values of Beta-exponential distribution is the smallest. It is reasonable to believe that the Beta-exponential distribution can better describe the FRHFMs magnitudes.

Table 2. Comparison of KS values of various statistical distributions.

Images	Gamma distribution	BKF distribution	Exponential distribution	Cauchy distribution	Weibull distribution	Beta-Exponential distribution
Barbara	0.1427	0.2027	0.1910	0.2126	0.1100	**0.0244**
Peppers	0.0806	0.3355	0.1106	0.1463	0.0840	**0.0128**
Boat	0.0891	0.1893	0.0707	0.2031	0.0727	**0.0206**
Lena	0.0868	0.2862	0.1041	0.1548	0.0859	**0.0135**
Average	0.0998	0.2535	0.1191	0.1792	0.0882	**0.0178**

4.3 Modified Maximum Likelihood Parameter Estimation

Parameter estimation is an important work in statistical model watermarking technology, and accurate parameters can ensure the performance of the watermarking detector, so an appropriate parameter estimation algorithm is very important. As optimization of the maximum likelihood estimation (MLE), the modified maximum likelihood estimation (MMLE) method has more generality. Moreover, when the sample data is small, the estimator obtained by MMLE convergence still has the advantages of consistency and unbias. Since direct iteration may lead to some problems such as local optimality, the likelihood function is linearized by Taylor expansion method to accurately solve the estimate values. Hence, The MMLE method not only reduces the computational complexity but also improves the numerical accuracy. Kumar et al. [33] demonstrated that MMLE is stable for the results of estimating finite populations, and the estimators of this method can be obtained easily with the use of computational tools.

Then, the parameter values of Beta-exponential model are estimated by MMLE method. Let random samples be $x_1, x_2, \Lambda\ , x_h$, then according to the function $\Phi(x) = d\ln\Gamma(x)/dx$, the logarithmic likelihood function in Equation (9) can be

$$\ln L(\alpha,\beta,k) = h\ln k - h\ln C(\alpha,\beta) + (\alpha-1)\sum_{i=1}^{h}\ln\left(1-\exp(-kx_i)\right) - \beta k\sum_{i=1}^{h}x_i \tag{11}$$

The specific process of the robust MMLE method is as follows [3][33]:

Step 1: The likelihood equation is denoted by ordinal variables: $x_1 \le x_2 \le \Lambda\ \le x_h$.

Step 2: The linearized awkward function e^{-kx_i} is derived from Taylor expansion method around the population quantile. Let function $g(x_i) = e^{-kx_i}$ expanded at point $x_i = t_i$ ($t_i = E(x_i)$), and we can obtain

$$g(x_i) = g(t_i) + \left(\frac{dg(x_i)}{dx_i}\Big|_{x=t_i}\right)\cdot(x_i - t_i) \cong \delta_i + \gamma_i x_i \qquad x_i > 0, i = 1,2,\Lambda\ ,h \tag{12}$$

Among them, $\delta_i = e^{-kt_i} + kt_i e^{-kt_i}$, $\gamma_i = -ke^{-kt_i}$. In order to calculate $x_i = t_i$ ($t_i = E(x_i)$), the PDF of a virtual random variable *v* is defined as $\mathrm{g(v) = e^{v}}$ [34], and $E(X) = \mu_i = F(x_i)$, where $F(u) = e^{u}$. When $h \ge 20$, t_i can be obtained from the following formula [35]: $\int_{-\infty}^{t_i} g(v)dv = i/(h+1)$. Therefore, t_i can be derived as $t_i = \ln(i/(h+1))$.

Step 3: In the end, the likelihood equation is solved and the unique solution is obtained. The modified likelihood function of parameters α, β and k can be obtained as follows

$$\begin{aligned}
\frac{\partial\ln L}{\partial\alpha} &\cong -h\Phi(\alpha) + h\Phi(\alpha+\beta) + \sum_{i=1}^{h}\ln\left(1-(\delta_i+\gamma_i x_i)\right)\\
\frac{\partial\ln L}{\partial\beta} &\cong -h\Phi(\beta) + h\Phi(\alpha+\beta) - k\sum_{i=1}^{h}x_i\\
\frac{\partial\ln L}{\partial k} &\cong \frac{\mathrm{h}}{k} - \beta\sum_{i=1}^{h}x_i + (\alpha-1)\sum_{i=1}^{h}\frac{x_i(\delta_i+\gamma_i x_i)}{1-(\delta_i+\gamma_i x_i)}
\end{aligned} \tag{13}$$

Let Equation (13) equals to 0, the simultaneous three equations and use the function $\Gamma(x) = \int_0^{+\infty} t^{x-1}e^{-t}dt \cong \sqrt{2\pi}x^{x-1/2}e^{-x}$ to get the specific parameter values.

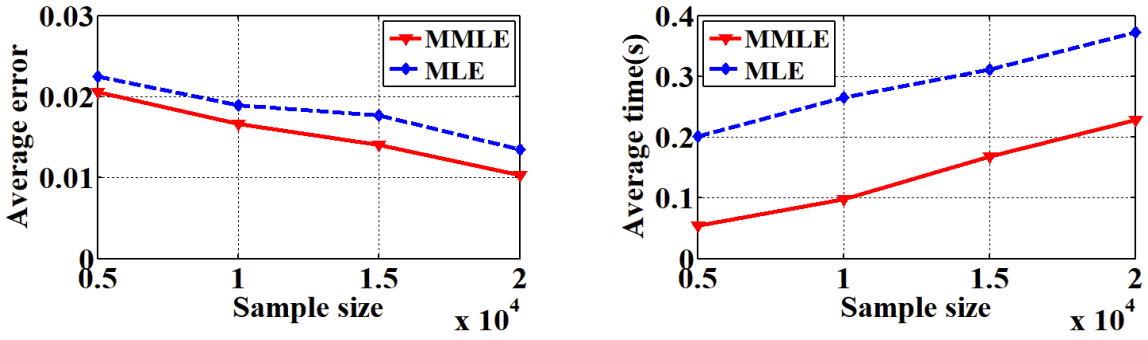
To prove the powerful performance of this method, we use Beta-exponential distribution to conduct Monte Carlo simulation experiments for MMLE and MLE methods. For the convenience of comparison, the shape parameter $\beta = 1$ and scale parameter $k = 1$ are first fixed and the discrete random variables are generated, and then the shape parameter α is estimated. We set the sample size of 5000 and randomly generate 1000 groups of samples in the experiment. Estimates of different parameter α are generated for each group of sampling experiment and run independently for 1000 times. Table 3 reports the parameter estimation results using different approaches. It implies that MMLE method is better than traditional MLE in terms of estimation accuracy and computational complexity.

To compare the two algorithms more intuitively, Fig. 5 shows the average running time and average errors of the two algorithms in different sample sizes. It can be concluded that MMLE method is superior to MLE method in both estimation

accuracy and computational complexity under different amount of sample sets. As the sample size increases, the parameter estimation error decreases and the average calculation time becomes longer. The main reason for such a change rule is that the small sample sizes cannot adequately represent the overall trend, resulting in the lack of accuracy of the estimation values. Furthermore, more sample data will inevitably lead to more calculation time. Hence, MMLE algorithm is used to calculate the parameters of Beta-Exponential distribution in this scheme.

Table 3. The average estimated result of shape parameter α

Actual shape parameters α	MMLE		MLE	
	Average errors	Average estimated values	Average errors	Average estimated values
5.0	0.0220	5.0220	0.0246	5.0246
4.0	0.0178	4.0178	0.0173	3.9827
3.0	0.0115	3.0115	0.0151	3.0151
2.0	0.0164	1.9836	0.0167	2.0167
1.0	0.0098	0.9902	0.0116	0.9884



(a) Average errors (b) Average times

Fig. 5. The compare results of two methods under different sample sizes

5. DIGITAL WATERMARK EMBEDDING

This section describes the embedding part of digital image watermarking technology in detail. This embedding method selects the multiplicative method to hide watermark information in FRHFMs magnitudes with local geometric invariance. Fig. 6 shows the embedding process of watermarking information. where $I = \{f(x, y), 0 \le x \le N, 0 \le Y \le N\}$ is the original carrier image, $f(x, y)$ denotes the image element, $w = \{w_l \in \{-1, -1\}, 1 \le l \le L\}$ are binary watermark bits with the same probability of +1 and −1. (i.e. $\sum_{l=1}^{L} w_l = 0$), and I' is a watermarked image.

Step 1: Divide the original image into 4×4 blocks. The original carrier image I is divided into *N* non-overlapping, equally sized sub-blocks, each of which has a size of 4×4. Then the *N* sub-blocks are sorted by high entropy values.

An imperceptible watermarked image can be effectually acquired by using the entropy masking model. The model shows that the high entropy regions of an image are highly complex. The larger the entropy value, the greater the uncertainty of image information sources. In addition, high entropy regions contain more image texture features, which is beneficial to resist noise and information hiding. Then the entropy (H) [2] formula is expressed as

$$H = -\sum_{i=1}^{R} p(a_i) \cdot \log p(a_i) \tag{14}$$

where a_i indicates an array of discrete possible events, and its probability is indicated by $p(a_i)$. *R* represents the number of possible events.

Step 2: High entropy blocks choice. The first *L* high entropy blocks $B_l \ (l = 1,2,3,...L)$ are selected and the magnitude coefficients based on the second-order FRHFMs are calculated for each image block. The target point (2, 2) of the magnitude coefficient blocks is changed by multiplicative rule to achieve the embedding of the watermark sequence w_l. What is particularly noted here is that each amplitude is embedded with the same watermark bit. The embedded expression is written as

$$y_i = \begin{cases} x_i \cdot (1+\lambda) & if \ watermark \ bit \ w_l = 1 \\ x_i \cdot (1-\lambda) & if \ watermark \ bit \ w_l = -1 \end{cases}, \quad i \in B_l \tag{15}$$

Among them, y_i indicates containing watermark moment magnitudes, x_i indicates original moment magnitudes, and λ denotes an embedding strength (positive weighting factor), which can well adjust the balance between imperceptibility and robustness of watermarking. In order to keep watermark invisible, the watermarking strength is usually $0 < \lambda < 1$.

The embedding strength λ is determined by the formula of watermark document ratio (WDR) [11]

$$WDR = 10\log_{10}\left(\frac{\lambda^2 \sigma_w^2}{\sigma_{x_i}^2}\right) \tag{16}$$

where the variance of the original image moment magnitudes is $\sigma_{x_i}^2 = \frac{1}{q}\sum_i x_i^2$ and *q* represents the count of magnitude coefficients. σ_w^2 represents the variance of the watermarking data, which is equal to 1 in this scheme. The image may be slightly distorted during the watermarking process, so WDRs are negatively related to the quality of images. According to Equation (16), the embedding strength λ is given by

$$\lambda = \sqrt{10^{\frac{WDR}{10}} \times \sigma_{x_i}^2} \tag{17}$$

Step 3: Obtain watermarked image blocks. The formula for obtaining image blocks containing watermarking information is

$$f_e(x, y) = f(x, y) - f_r(x, y) + f_{e'}(x, y) \tag{18}$$

Among them, $f_r(x, y)$ and $f_{e'}(x, y)$ represents the image block reconstructed by original FRHFMs and modified FRHFMs respectively, and $f(x, y)$ is defined the original image block.

Step 4: Acquire watermarked image. The high entropy image blocks with the watermark are swapped with the original image blocks to get a watermarked image *I′*.

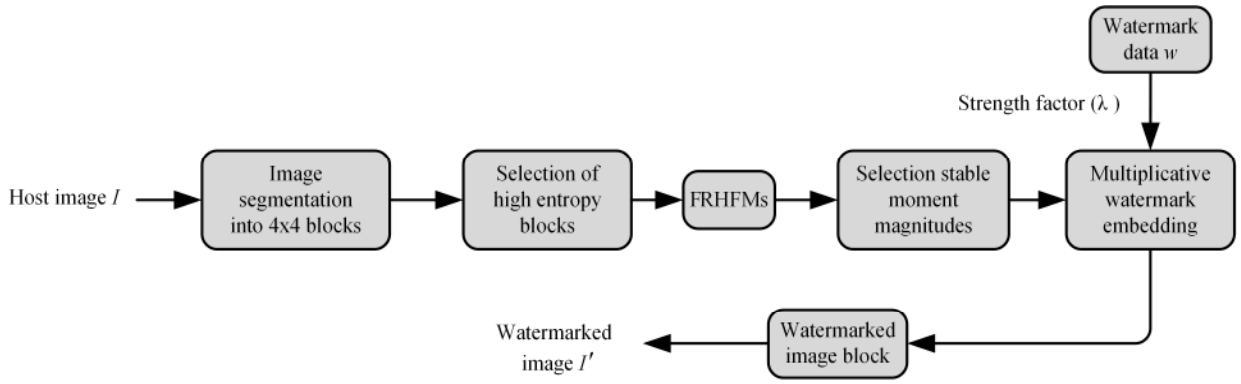


Fig. 6. The process of embedding watermark data.

6. DIGITAL WATERMARK DETECTION

This section describes the construction of the watermark detector in detail. Actually, the purpose of watermarking detection is to detect whether the host image contains watermark information. For watermark detection, a detector based on the statistical property of moment magnitude coefficients helps to obtain accurate and reliable results. If I' is a watermarked image with $n \times n$ pixels, then the specific process of watermarking detection is shown in Fig. 7.

The image I' with watermark is split into N non-overlapping sub-blocks of size 4×4. After calculating the entropy value of each block, these blocks are sorted in descending order. The second-order FRHFMs of the first L high-entropy blocks with the same number of watermarks are calculated to be the magnitude coefficients. Then, using the FRHFMs magnitudes in the same area as the embedding watermark position to form the target domain, and then L accurate moment magnitudes are obtained. A basic assumption is that after the watermark is embedded, the statistical distribution of FRHFMs magnitudes will not change. The watermark bit is defined as equal probability, and the moment magnitudes are assumed to be isolated and uniformly distributed. To detect watermark information hidden in the FRHFMs magnitudes, a statistical watermark detector based on the Beta- exponential model is constructed through the LMP test.

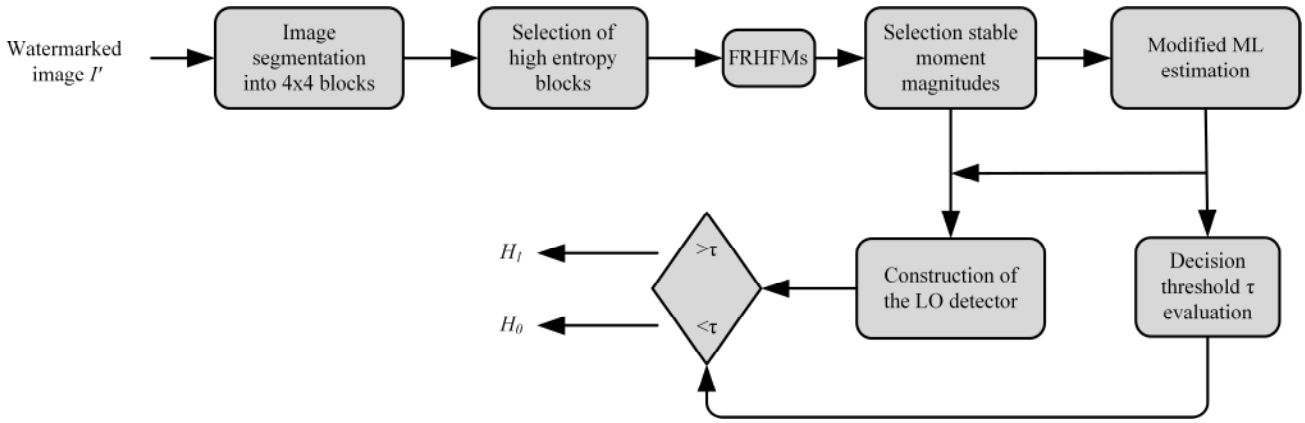


Fig. 7. Detection process of watermark data.

6.1 Locally Optimal Watermark Detector

When watermark embedding intensity is weak, the watermark detection can be distinctly expressed as a weak signal detection problem. Otherwise, it can be regarded as a strong signal detection problem. Since the strength of the watermark is

suppressed by some attacks such as noise, rotation and filtering, watermark detection under strong signals can also be considered as a smaller signal detection problem. The LO detector is specifically designed to detect weak signals, so it is very significant to introduce this detector in watermark detection scheme.

The watermarking detection problem is customarily regarded as a binary hypothesis testing problem, then the multiplicative watermark detection method is

$$\begin{aligned} H_0 &: \mathbf{y} = \mathbf{x} \\ H_1 &: \mathbf{y} = \mathbf{x} \cdot (1 + \lambda \mathbf{w}) \end{aligned} \tag{19}$$

Among them, H_1 represents the alternative hypothesis that there is hidden information, and H_0 is the null hypothesis. $\mathbf{y} = \{y_1, y_2, \Lambda\ , y_L\}$ and $\mathbf{x} = \{x_1, x_2, \Lambda\ , x_L\}$ are the original FRHFMs magnitude coefficients and the FRHFMs magnitude coefficients with watermark respectively. $\mathbf{w}= w_i \in \{+1,-1\}, 1 \le i \le L\}$ is watermark information and λ is watermark strength. A watermark detector based on Neyman-Pearson lemma is presented

$$\Lambda(\mathbf{y}) = \frac{f_Y(\mathbf{y} \mid H_1)}{f_Y(\mathbf{y} \mid H_0)} \underset{H_0}{\overset{H_1}{\gtrless}} \eta \tag{20}$$

where $\Lambda(\mathbf{y})$ represents the likelihood ratio and η denotes the threshold. Assuming the FRHFMs magnitudes of the watermarked image follows Beta-exponential distribution (optimal distribution). The conditional probability density functions under both assumptions are expressed as

$$\begin{aligned} f_Y(y_i \mid H_0) &= f_X(y_i) \\ f_Y(y_i \mid H_1) &= \frac{1}{1+\lambda w_i} f_X\left(\frac{y_i}{1+\lambda w_i}\right) \end{aligned} \tag{21}$$

Watermarks can be considered as weak signals added to a strong background (the original image), so the statistical properties of original magnitude coefficients do not be changed by the embedded watermark. Then the logarithmic likelihood ratio is determined by

$$l_{LOD}(\mathbf{y}) = \ln[\Lambda(\mathbf{y})] = \sum_{i=1}^{L} \ln \frac{f_Y(y_i \mid H_1)}{f_Y(y_i \mid H_0)} = \sum_{i=1}^{L} \left[\ln \frac{1}{1+\lambda w_i} + \ln \frac{f_X\left(\frac{y_i}{1+\lambda w_i}\right)}{f_X(y_i)} \right] \underset{H_0}{\overset{H_1}{\gtrless}} \tau \tag{22}$$

where $\tau=\ln(\eta)$. Equation (22) is expanded to Taylor series at λ=0 based on the approximation of the likelihood ratio test, and the LO detector is obtained after ignoring the second and higher orders by

$$\begin{aligned} l_{LOD}(y_i)\big|_{\lambda} &= l(y_i)\big|_{\lambda=0} + \left.\frac{\partial l(y_i)}{\partial \lambda}\right|_{\lambda=0} \cdot \lambda + o(\lambda) \\ &\cong -\lambda w_i - \frac{\frac{\partial f_X(y_i)}{\partial y_i}}{f_X(y_i)} \cdot \lambda y_i w_i = -\lambda w_i + g_{LO}(y_i) \cdot \lambda y_i w_i \end{aligned} \tag{23}$$

where $g_{LO}(y)$ denotes "locally optimal nonlinearity". The derivation process of applying the PDF of Beta-exponential model to this formula is given by

$$g_{LO}(y) = -\frac{\frac{\partial f_X(y_i)}{\partial y_i}}{f_X(y_i)} = -\frac{f'_X(y_i)}{f_X(y_i)} = \beta k - \frac{(\alpha-1)\cdot k e^{-ky_i}}{1-e^{-ky_i}} \tag{24}$$

Now using (23) and (24) in (22), the final statistical decision formula of the LO detector is expressed as

$$\begin{aligned} l_{LOD}(\mathbf{y}) &= \sum_{i=1}^{L} -\lambda w_i + g_{LO}(y_i)\cdot \lambda y_i w_i = -\lambda \sum_{i=1}^{L} w_i + \sum_{i=1}^{L}\left(\beta k - \frac{(\alpha-1)\cdot k e^{-ky_i}}{1-e^{-ky_i}}\right)\cdot \lambda y_i w_i \\ &= \sum_{i=1}^{L}\left(\beta k - \frac{(\alpha-1)\cdot k e^{-ky_i}}{1-e^{-ky_i}}\right)\cdot \lambda y_i w_i \underset{H_0}{\overset{H_1}{\gtrless}} \tau \end{aligned} \tag{25}$$

where the embedding strength λ can be obtained from Equation (17), if l_{LOD} is more than the decision threshold τ, H_1 is accepted; otherwise, H_0 is accepted.

6.2 Performance Analysis of the Proposed Watermark Detector

Performance of watermark detection methods must be analyzed before they are applied in practice. Next, we test the performance of the watermark detector for the given image based on the detection probability P_{det} and the false alarm probability P_{fa}. Generally, the false alarm probability P_{fa} is fixed. The optimal detector should minimize the probability of miss (P_m), that is, maximize the detection probability P_{det}=1−P_m. The determination threshold τ is gained by Naiman-Pearson criterion. This threshold minimizes the watermark missing probability P_m under the condition that the false alarm probability P_{fa} is bounded. We can get the following expression

$$\begin{aligned} P_{fa} &= P\left(T_{LOD}(\mathrm{y}) > \tau \mid H_0\right) \\ &= P\left(\frac{T_{LOD}(\mathrm{y})}{\sigma_0} > \frac{\tau-\mu_0}{\sigma_0}\right) \\ &= Q\left(\frac{\tau-\mu_0}{\sigma_0}\right) \end{aligned} \tag{26}$$

where $Q(x) = \frac{1}{2} erfc\left(\frac{x}{\sqrt{2}}\right)$. μ_0 is the mean and σ_0 is the variance under the H_0 assumption, and the specific process of the calculation is shown in the appendix A. $erfc(\cdot) = 1 - erf(\cdot)$ represents the complementary error function. For a given P_{fa}, the threshold expression is derived by

$$\tau = \mu_0 + \sigma_0 Q^{-1}(P_{fa}) \tag{27}$$

If $Q(x) = P_{fa}$, then $Q^{-1}(P_{fa}) = x$. According to the above formulas, the relationship between P_{fa} and P_{det} (that is the ROC curve of the proposed detector) is expressed as

$$\begin{aligned} P_{\mathrm{det}} &= Q\left(\frac{\tau-\mu_1}{\sigma_1}\right) \\ &= Q\left(\frac{\sigma_0}{\sigma_1} Q^{-1}\left(P_{fa}\right) - \frac{m_1-m_0}{\sigma_1}\right) \end{aligned} \tag{28}$$

7. EXPERIMENTAL RESULTS

In this section, we first evaluate the performance of the proposed watermark detector on some standard grayscale images with different sizes from Computer Vision Group Test Images database s [36], and various length pseudorandom watermark sequences. Then, we compare our approach with the state-of-the-art methods such as Etemad's t LS[11], Rabizadeh's BKF[12], Sadreazami's Cauchy[15], Amirmazlaghani's CT-GARCH[38], Sadreazami's NIG[5], Amini's CHMM[24], Amirmazlaghani's WT-GARCH [37], and Amini's WHMM[7] based approaches.

In this work, all experiments are implemented in MATLAB R2016a, where the personal computer configuration is Windows 10 system and Intel(R) Xeon(R) CPU i5-3470 @ 3.20 GHz 8GB memory.

7.1 Performance Evaluation of the Proposed Watermark Detector

7.1.1 Accuracy

For the purpose of validating the theoretical expressions of the suggested detection method, the theoretical and experimental ROC curves are compared through simulation experiments. Fig. 8 exhibits the averaged ROC curves for 96 test images, in which WDR varies from −30dB to −36dB in the range of $10^{-12} \leq P_{fa} \leq 10^{-4}$. In Monte Carlo simulation experiments, 100 binary watermark sequences with length of 4000 bits are generated randomly. As can be observed from the figure, the two ROC curves are basically coincident, indicating the availability of the closed-form theoretical expressions of statistical properties.

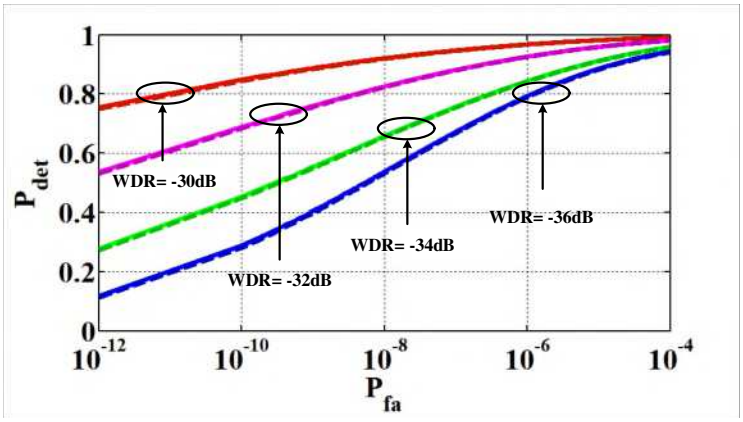


Fig. 8. The experimental (solid) and theoretical (dashed) ROC curves.

7.1.2 Imperceptibility

Imperceptibility is one of the main requirements of watermark algorithms and the objective measure [3] for assessing this feature is the PSNR between original and the watermarked image. Fig. 9 shows the test results of the imperceptibility of watermarked images using our proposed watermarking method. We choose host images with 512×512 pixels as the test images. At the same time, the WDR is defined as −40 dB and a set of 1000-bit pseudo-random sequence is used. Fig. 9 (c) shows that the naked eye cannot notice the distinction between the watermarked and no-watermark image without the help of image processing technology. Moreover, PSNR values are all over 38, which is enough to show that our watermarking scheme has good imperceptibility.

Fig. 9. Imperceptibility analysis: (a) original images, (b) images with watermark and (c) the difference image (×10).

7.1.3 Robustness

Next, we discuss the robustness of the presented LO detection method under different attacks, including JPEG compression, Gaussian filtering, cropping and AWGN. For a given image, we compare the statistical decision formula l_{LOD} with the decision threshold τ to get the detector response under a given false alarm probability (P_{fa}=10^{-8}). And we give the average detection responses of the Lena image in 100 randomly generated binary watermark sequences with length of 6000 bits. Fig. 10 (a) demonstrates detection responses under JPEG compression attacks, in which the quality factor increases from 10 to 100. Fig. 10 (b) shows detection responses based on Gaussian filtering, where the window sizes are 3×3, 5×5 and 7×7. Fig. 10 (c) and (d) show detection responses under cropping (cropping ranges from 2% to 20%) and AWGN attacks (σ_n varies from 5 to 35) respectively. The results show that the Beta-exponential detector based on the LMP test can provide higher detection rates under different attacks. Therefore, the proposed detector has strong robustness.

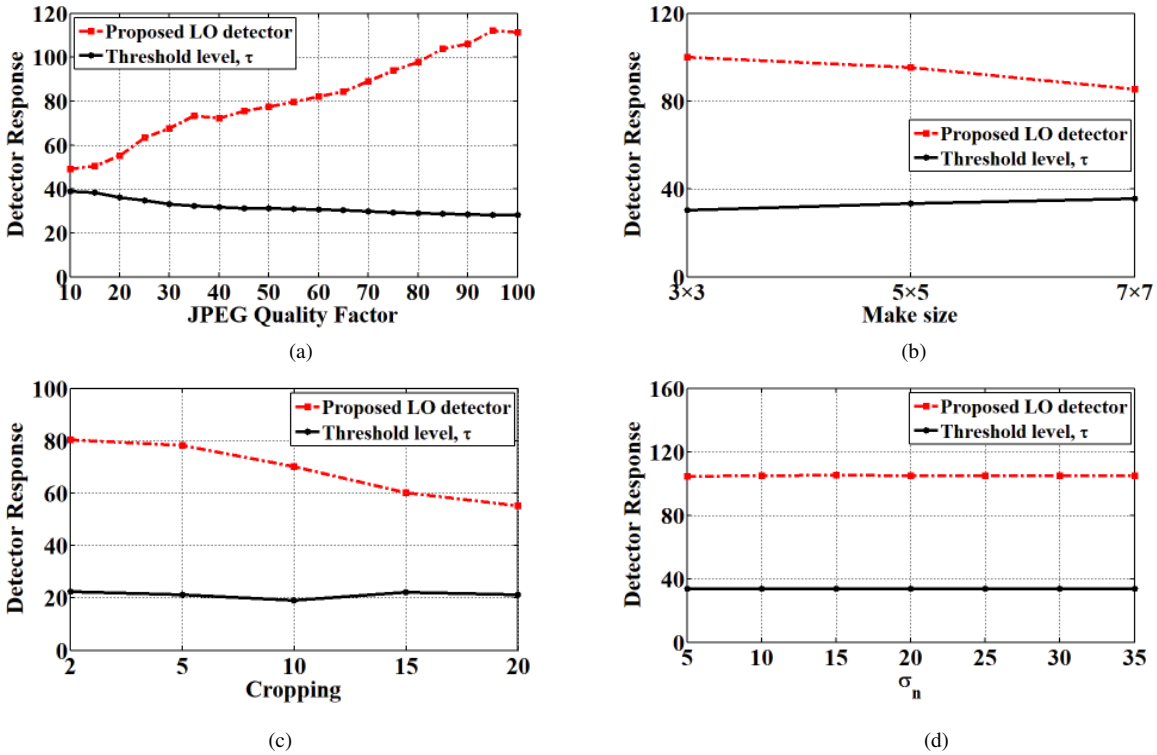


Fig. 10. The detection responses of Lena image under WDR = −40dB. (a) JPEG compression, (b) Gaussian filtering, (c) cropping and (d) AWGN attacks.

7.1.4 Capacity and Time

In the simulations, we embed watermark sequences of different message lengths into twenty standard grayscale images (512×512×8 bits). Table 4 shows the relationship between average PSNR, average time of watermark embedding/ detection and watermark capacity. As shown in this table, the proposed watermark scheme provides lower time complexity, larger watermark capacity and stronger imperceptibility.

Table 4. The average performance of the proposed watermark algorithm.

Watermark length (bits)	The average embedding time (seconds)	The average PSNR (dB)	The average detecting time (seconds)
1000bit	2.5189	48.7496	2.5189
5000bit	3.6118	42.6870	3.2358
10000bit	4.9220	40.5230	4.0671

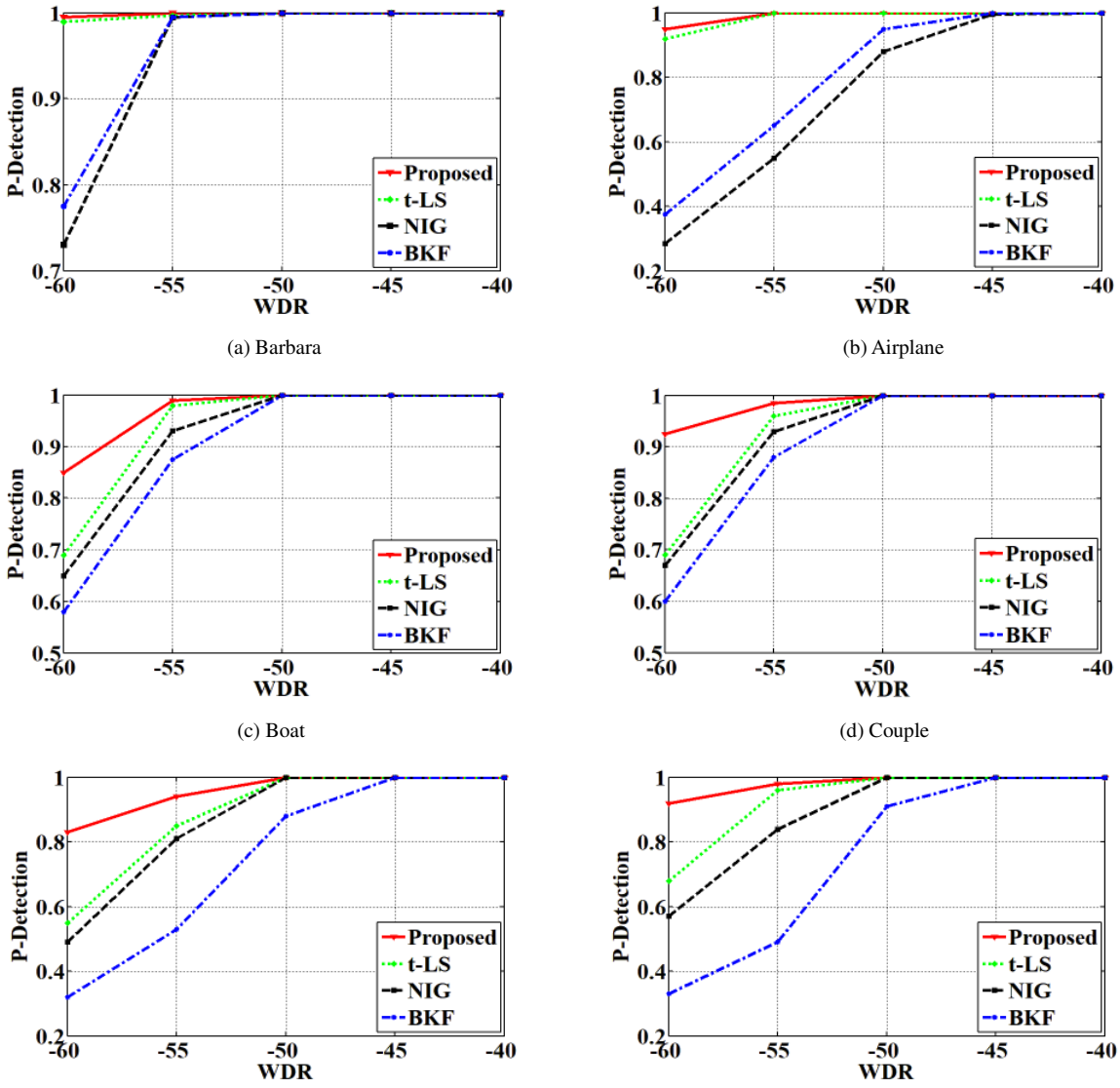
7.2 Comparisons with State-of-The-Art Methods

In this section, we compare the proposed approach with eight state-of-the art statistical image watermarking methods, including Etemad's t LS[11], Rabizadeh's BKF[12], Sadreazami's Cauchy[15], Amirmazlaghani's CT-GARCH[38], Sadreazami's NIG[5], Amini's CHMM[24], Amirmazlaghani's WT-GARCH [37], and Amini's WHMM[7] based methods. We selected these eight methods based on their similarities to the proposed approach, and based on the presence of sufficient algorithm descriptions (including implementation details and parameter settings etc.) provided in the respective publications.

7.2.1 Proability of Detection for Varying Watermark Strengths

For investigating the proposed detector performance under various watermark powers, we take five different WDRs into

account, ranging from −60 (dB) to −40 (dB). In Fig. 11, we plot the detection probabilities for different WDRs with the false alarm probability of 0.01, and test 6 gray images of 512 by 512, including Barbara, Airplane, Boat, Couple, Lena and Peppers. It can be noticed that as the watermark powers enhances, the detection probabilities of four detectors increase. As the same time, we can observe that the detection performance of the Beta-exponential detector appears more powerful than other contourlet domain detectors (t-LS [11], BKF [12] and NIG [5]) for different watermark strengths.



(a) Barbara (b) Airplane

(c) Boat (d) Couple

(e) Lena (f) Peppers

Fig. 11. Comparison tests of detection probability under different watermark intensities

.

7.2.3 AUROC Values under Various Attacks

In this part, we compare the suggested digital image watermark detector with other detectors based on multivariate Cauchy distribution [15], BKF distribution [12] and HMM [7][24]. The 100 experiments on 24 grayscale images with size of 256×256 are tested under pseudo-random watermark sequences of the same size as the compared algorithm. In Table 5, we give the average AUROC values of 24 experimental images in the range of $0 \le P_{fa} \le 10^{-4}$. As can be observed from this table, the suggested multiplicative Beta-exponential detector provides the highest AUROC value, indicating the detector has superior performance to that of other existing detectors.

In Table 6, the average AUROC values of multiple test images are obtained under Gaussian filtering, cropping, rotation, scaling and gamma correction attacks. As can be observed from the table, although the performance of the detector in this paper is similar to that of HMM-based detector [24] under strong gamma correction and cropping attacks, on the whole, the proposed detector provides larger AUROC values than other detectors under both conventional attacks and geometric attacks.

Table 5. AUROC values ($\times 10^{-4}$) obtained using different watermark detectors in the area [0, 10^{-4}] (WDR =-42 dB)

Methods	AUROC
WHMM [7]	0.9117
BKF [12]]	0.7286
Cauchy [15]	0.8362
CHMM [24]	0.9934
Proposed	**0.9948**

Table 6. The AUROC values ($\times 10^{-4}$) obtained under different attacks.

	WHMM [7]	BKF [12]	Cauchy [15]	CHMM [24]	Proposed
Cropping					
5%	0.8567	0.69983	0.8310	0.9104	**0.9267**
10%	0.7517	0.6118	0.7369	**0.8045**	0.7928
Gaussian filtering					
3×3	0.8854	0.7009	0.7893	0.9007	**0.9315**
5×5	0.8032	0.6875	0.7245	0.8865	**0.9047**
7×7	0.7769	0.4765	0.6879	0.8644	**0.8830**
Gamma correction					
0.9	0.8876	0.6998	0.8004	0.9032	**0.9185**
1.1	0.8132	0.6435	0.7993	**0.9007**	0.8974
Rotation					
0.5°	0.8921	0.8821	0.7832	0.9121	**0.9370**
1°	0.8764	0.8054	0.7251	0.9003	**0.9243**
2°	0.8021	0.7994	0.6673	0.8732	**0.8821**
Scaling					
0.8	0.7591	0.5889	0.6554	0.8548	**0.8940**
1.2	0.7254	0.5982	0.6118	0.8003	**0.8335**

To clearly prove the robustness of the suggested algorithm, Fig. 12-15 provide the average AUROC test results of this detector and other existing advanced detectors under various attacks, where the watermarked images undergo different types of attacks including JPEG compression, salt & pepper noise, median filtering and AWGN. In Fig. 12, we can see that the suggested LO detector under JPEG compression attacks provides more robust properties than that of other detectors. Especially compared with the optimal algorithm [24] in existing detectors, the proposed detector is more likely to detect watermarks under strong attack condition with QF =5.

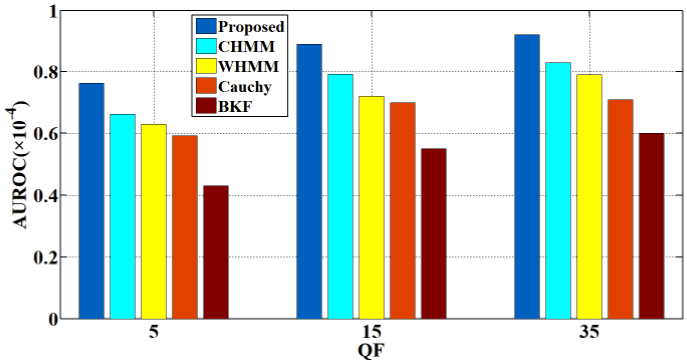


Fig. 12. AUROC of different detectors under JPEG compression attacks.

Fig. 13 shows that under AWGN attacks, the suggested LO detector provides the largest AUROC values among all the detection algorithms compared. It should be observed that when σ_n =40, the proposed detector still outperforms to other methods. Salt & pepper noise and median filtering attacks are considered as common attacks when assessing the performance of any watermarking method. Fig. 14 and Fig. 15 indicate that the suggested watermark detector has greater advantages than competing techniques when the watermarked image undergoes common signal attacks.

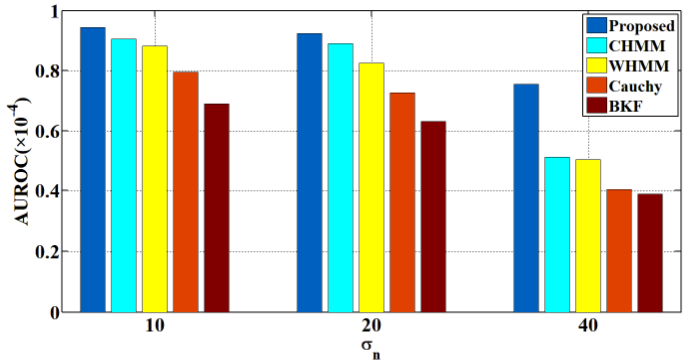


Fig. 13. AUROC of different detectors under AWGN attacks.

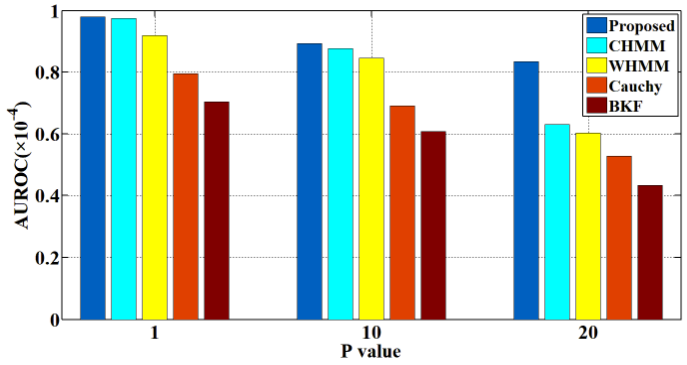


Fig. 14. AUROC of different detectors under salt & pepper noise attacks.

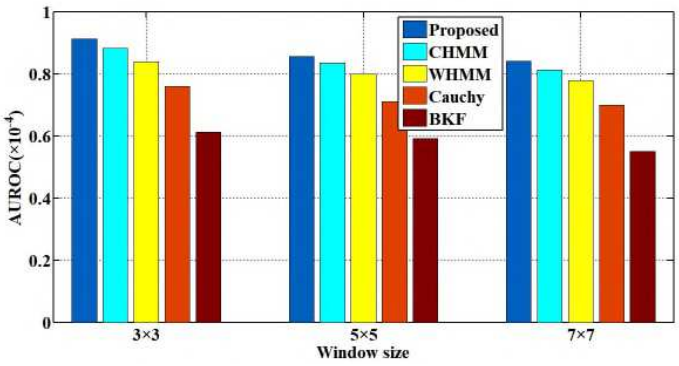


Fig. 15. AUROC of different detectors under median filtering attacks.

Next, we also compare the average performance of the presented watermark detector and other existing watermark detectors, including CT-GARCH [38] and WT-GARCH [37], as shown in Table 7. Here, we used 24 images with size of 512×512×8bits as host images, including Peppers, Living room, Lake, Pirate, Bridge, and Gold hill etc. Meanwhile, we randomly generated 24 different watermark sequences (128×256 bits), the range of the given P_{FA} is [0,1]. Thus, 576 different combinations of watermark messages and host images (24 watermarks×24 hosts) were used in the evaluation. The comparative experiments are carried out under the same experimental conditions. According to the above experimental results, the proposed detector demonstrates excellent performance against various attacks under different WDR values.

Table 7 Average AUROC values under various attacks.

Attack Types		WT-GARCH [37]	CT-GARCH [38]	Proposed
JPEG Compression (QF=60)	WDR=−50dB	0.8591	0.8994	**0.9282**
	WDR=−45dB	0.9413	**0.9978**	0.9853
Gaussian Filtering (5×5)	WDR=−60dB	0.6401	0.9038	**0.9539**
Median Filtering (5×5)	WDR=−50dB	0.8504	0.9688	**0.9993**
Gaussian Filtering (5×5) and AWGN (σ =10)	WDR=−50dB	0.7582	0.9780	**0.9931**
Median Filtering (5×5) and AWGN (σ =10)	WDR=−50dB	0.8149	0.9334	**0.9803**
Scaling with WDR= −50dB	SF=0.75	0.8063	0.9926	**0.9986**
	SF=2	0.7814	0.9157	**0.9578**
Rotation with WDR= −45dB	θ =3	0.8561	0.9529	**0.9633**
	θ =−3	0.8774	0.9454	**0.9768**

According to the above comparison results, we can clearly conclude that our proposed Beta-exponential distribution based watermark detector achieves high work performance compared with some state-of-the-art methods. This improvement mainly comes from four aspects: First, we introduced FRHFMs to statistical image watermarking, and apply robust local FRHFMs magnitudes for inserting watermark signal and developing watermark detector. Second, we modeled the robust local FRHFMs magnitudes with Beta-exponential distribution, which can capture accurately the non-Gaussian and heavy-tailed statistical characterization of local FRHFMs magnitudes. Also, we estimate effectively the statistical model parameters of the Beta-exponential PDF by modified ML estimation approach. Third, we developed the blind statistical watermark detector using Beta-exponential distribution and locally most powerful test.

8. CONCLUSION

In this algorithm, we have used Beta-exponential distribution to fit the RHFMs magnitude coefficients and designed an optimal watermark detector. The multiplicative method has been used to insert the watermarking information into the magnitude coefficients. To enhance the detection probability, we also used MMLE algorithm to calculate the model parameters. Further, the optimal detector is derived by the LMP test and assessed its performance. A theoretical expression of the detection has been verified through Monte Carlo simulation experiments in detail. Then the AUROC curves and the ROC curves of this algorithm are compared with other advanced detection algorithms. It has been observed that this detector presents a higher detection probability than other detection methods based on the t-LS, NIG, BKF, GG and 2D-GARCH distributions with predetermined false alarm probability. The robustness of this watermark detector under regular attacks and geometric attacks has also been researched, and the experimental results indicate that our detector has better detection performance than other existing schemes.

Nevertheless, this method still has some problems, such as inaccurate watermark detection probability in strong signals. In the future, more robust modeling objects and more versatile models will be further explored and studied to obtain better the performance of the watermark detector.

Appendix A. Variance and mean of log-likelihood ratio under hypotheses H_0 and H_1.

In this section, the likelihood ratio provided can be regarded to obey the Beta-exponential distribution conditioned on each of the H_0 and H_1 hypotheses. We can calculate the variance and mean under the two hypotheses, i.e., σ_0, σ_1, μ_0, μ_1. An expression for the mean μ_0 under the H_0 hypothesis is derived by

$$\begin{aligned}\mu_0 &= E(T_{LOD}(\mathbf{y}) \mid H_0) = E(T_{LOD} \mid \mathrm{x}) \\ &= E\left[\sum_{i=1}^{L}\left(\beta k - \frac{(\alpha-1)\cdot k e^{-k x_i}}{1-e^{-k x_i}}\right)\cdot \lambda x_i w_i\right] \\ &= \sum_{i=1}^{L}\left(\frac{\lambda x_i}{2}\right)\left(\beta k - \frac{(\alpha-1)\cdot k e^{-k x_i}}{1-e^{-k x_i}}\right)+\left(-\frac{\lambda x_i}{2}\right)\left(\beta k - \frac{(\alpha-1)\cdot k e^{-k x_i}}{1-e^{-k x_i}}\right)=0\end{aligned} \tag{A.1}$$

Similarly, we also give the mean μ_1 of the log-likelihood ratio based on hypothesis $H_1 : \mathbf{y} = \mathbf{x}(1+\lambda\mathbf{w})$ by

$$\begin{aligned}\mu_1 &= E(T_{LOD}(\mathbf{y}) \mid H_1) = E(T_{LOD} \mid \mathbf{x}+\lambda\mathbf{x}\mathbf{w}) \\ &= E\left[\sum_{i=1}^{L}\left(\beta k - \frac{(\alpha-1)\cdot k e^{-k\left(x_i+\lambda x_i w_i\right)}}{1-e^{-k\left(x_i+\lambda x_i w_i\right)}}\right)\cdot \lambda\left(x_i+\lambda x_i w_i\right) w_i\right] \\ &= \sum_{i=1}^{L}\left(\left(\frac{\lambda\left(x_i+\lambda x_i\right)}{2}\right)\left(\beta k - \frac{(\alpha-1)\cdot k e^{-k\left(x_i+\lambda x_i\right)}}{1-e^{-k\left(x_i+\lambda x_i\right)}}\right)+\left(-\frac{\lambda\left(x_i-\lambda x_i\right)}{2}\right)\left(\beta k - \frac{(\alpha-1)\cdot k e^{-k\left(x_i-\lambda x_i\right)}}{1-e^{-k\left(x_i-\lambda x_i\right)}}\right)\right) \\ &= \sum_{i=1}^{L}(\omega_i+\upsilon_i)\end{aligned} \tag{A.2}$$

where $\omega_i = \left(\frac{\lambda\left(x_i+\lambda x_i\right)}{2}\right)\left(\beta k - \frac{(\alpha-1)\cdot k e^{-k\left(x_i+\lambda x_i\right)}}{1-e^{-k\left(x_i+\lambda x_i\right)}}\right)$, $\upsilon_i = \left(-\frac{\lambda\left(x_i-\lambda x_i\right)}{2}\right)\left(\beta k - \frac{(\alpha-1)\cdot k e^{-k\left(x_i-\lambda x_i\right)}}{1-e^{-k\left(x_i-\lambda x_i\right)}}\right)$. The variance under hypothesis H_0 is expressed by

$$\begin{aligned}\sigma_0^2 &= Var(T_{LOD}(\mathbf{y}) \mid H_0) = Var(T_{LOD}(\mathbf{y}) \mid \mathrm{x}) \\ &= E\left[\left(\sum_{i=1}^{L}\left(\beta k - \frac{(\alpha-1)\cdot k e^{-kx_i}}{1-e^{-kx_i}}\right)\cdot \lambda x_i w_i\right)^2\right] \\ &= \sum_{i=1}^{L}\left(\left(\beta k - \frac{(\alpha-1)\cdot k e^{-kx_i}}{1-e^{-kx_i}}\right)\cdot \lambda x_i\right)^2\end{aligned} \tag{A.3}$$

The variance under hypothesis H_1 is given by

$$\begin{aligned}\sigma_1^2 &= Var(T_{LOD}(\mathrm{y}) \mid H_1) = E[\left((T_{LOD}(\mathrm{y}) \mid H_1) - \mu_1\right)^2] \\ &= \sum_{i=1}^{L} E\left[\left(\left(\beta k - \frac{(\alpha-1)\cdot k e^{-k(x_i+\lambda x_i w_i)}}{1-e^{-k(x_i+\lambda x_i w_i)}}\right)\cdot \lambda\left(x_i + \lambda x_i w_i\right) w_i - \omega_i - \upsilon_i\right)^2\right] \\ &+ \sum_{l}^{L}\sum_{l\neq i} E\left[\left(\left(\beta k - \frac{(\alpha-1)\cdot k e^{-k(x_l+\lambda x_l w_l)}}{1-e^{-k(x_l+\lambda x_l w_l)}}\right)\cdot \lambda(x_l + \lambda x_l w_l) w_l - \omega_l - \upsilon_l\right)\cdot\right. \\ &\left.\left(\left(\beta k - \frac{(\alpha-1)\cdot k e^{-k(x_i+\lambda x_i w_i)}}{1-e^{-k(x_i+\lambda x_i w_i)}}\right)\cdot \lambda(x_i + \lambda x_i w_i) w_i - \omega_i - \upsilon_i\right)\right] \\ &= \sum_{i=1}^{L}\left(\omega_i - \upsilon_i\right)^2\end{aligned} \tag{A.4}$$

Conflicts of interest The authors declare that they have no conflict of interest.

Ethical standard All procedures performed in studies involving human participants were in accordance with the ethical standards of the institutional and/or national research committee and with the 1964 Helsinki Declaration and its later amendments or comparable ethical standards.

Informed consent Informed consent was obtained from all individual participants included in the study.

REFERENCES

[1] M. Amirmazlaghani, M. Rezghi, H. Amindavar. A novel robust scaling image watermarking scheme based on Gaussian mixture model. Expert Systems with Applications, 2015, 42(4):1960-1971. =>1

[2] P. Bhinder, K. Singh, N. Jindal. Image-adaptive watermarking using maximum likelihood decoder for medical images. Multimedia Tools and Applications, 2018, 77(8):10303-10328.

[3] X. Y. Wang, J. Tian, J. L. Tian, P. P. Niu, H. Y. Yang. Statistical image watermarking using local RHFMs magnitudes and Beta exponential distribution. Journal of Visual Communication and Image Representation, 2021, 77: 103123.

[4] M. Amini, M. O. Ahmad, M. N. S. Swamy. A new locally optimum watermark detection using vector-based hidden Markov model in wavelet domain. Signal Processing, 2017, 137:213-222.

[5] H. Sadreazami, M. O. Ahmad, M. N. S. Swamy. Optimum multiplicative watermark detector in contourlet domain using the normal inverse Gaussian distribution. Proceeding of the IEEE International Symposium on Circuits & Systems. Lisbon, Portugal, 2015:1050-1053.

[6] M. Amirmazlaghani. Additive watermark detection in the wavelet domain using 2D-GARCH model. Information Sciences, 2016, 370-371:1-17.

[7] M. Amini, H. Sadreazami, M. O. Ahmad, M. N. S. Swamy. Multichannel color image watermark detection utilizing vector-based hidden Markov model. Proceedings of the 2017 IEEE International Symposium on Circuits and Systems, Baltimore, MD, USA, 2017:1-4.

[8] A. K. Singh. Improved hybrid algorithm for robust and imperceptible multiple watermarking using digital images. Multimedia Tools and Applications, 2017, 76(6):8881-8900.

[9] B. Ahmaderaghi, F. Kurugollu, J. M. D. Rincon, A. Bouridane. Blind image watermark detection algorithm based on discrete shearlet transform using statistical decision theory. IEEE Transactions on Computational Imaging, 2018, 4(1):45-59.

[10] J. Liu. An image watermarking algorithm based on energy scheme in the wavelet transform domain. Proceedings of the 2018 IEEE 3rd International Conference on Image, Vision and Computing, Chongqing, China, 2018: 668-672.

[11] S. Etemad, M. Amirmazlaghani. A new multiplicative watermark detector in the contourlet domain using t location-scale distribution. Pattern Recognition, 2017, 77: 99-112.

[12] M. Rabizadeh, M. Amirmazlaghani, M. A. Attari. A new detector for contourlet domain multiplicative image watermarking using Bessel K form distribution. Journal of Visual Communication and Image Representation, 2016, 40:324-334.

[13] V. Sedighi, J. Fridrich, R. Cogranne. Content-adaptive pentary steganography using the multivariate generalized Gaussian cover model. Media Watermarking, Security, and Forensics, 2015, 9409H:1-13.

[14] K. Zebbiche, F. Khelifi, K. Loukhaoukha. Robust additive watermarkig in the DTCWT domain based on perceptual masking. Multimedia Tools and Applications, 2018, 77(16):21281-21304.

[15] H. Sadreazami, M. O. Ahmad, M. N. S. Swamy. A robust multiplicative watermark detector for color images in sparse domain. IEEE Trans. on Circuits and Systems II: Express Briefs, 2015, 62(12):1159-1163.

[16] S. Etemad, M. Amirmazlaghani. Additive watermark detector in contourlet domain using the t location-scale distribution. Proceeding of the 2016 2nd International Conference of Signal Processing and Intelligent Systems. Tehran, Iran, 2016.

[17] X. Y. Wang, Y. N. Liu, H. Xu, A. L. Wang, H. Y. Yang. Blind optimum detector for robust image watermarking in nonsubsampled shearlet domain. Information Sciences, 2016, 372:634-654.

[18] H. B. Bi, Y. Liu, M. M. Wu, Y. L. Ge. NSCT domain additive watermark detection using RAO hypothesis test and Cauchy distribution. Mathematical Problems in Engineering, 2016, 2016:1-18.

[19] X. Y. Wang, S. Y. Zhang, T. T. Wena, H. Y. Yang. P. P. Niu. Coefficient difference based watermark detector in nonsubsampled contourlet transform domain. Information Sciences, 2019, 503:274-290.

[20] L. Dong, Q. Yan, Y. Lv, S. Y. Deng. Full band watermarking in DCT domain with Weibull model. Multimedia Tools and Applications, 2016, 76(2):1-18.

[21] M. Amirmazlaghani. A novel statistical detector for contourlet domain image watermarking using 2D-GARCH model. International Conference on Image Analysis & Processing, 2017:547-557.

[22] M. Barazandeh, M. Amirmazlaghani. A new statistical detector for additive image watermarking based on dual-tree complex wavelet transform. Proceeding of the 2016 2nd International Conference of Signal Processing and Intelligent Systems. Tehran, Iran, 2016.

[23] M. Alghoniemy, A. H. Tewfik. Image watermarking by moment invariants. Proceeding of the 2000 International Conference on Image Processing. Vancouver, BC, Canada, 2000:73-76.

[24] M. Amini, H. Sadreazami. M. O. Ahmad, M. N. S. Swamy. A channel-dependent statistical watermark detector for color images. IEEE Transactions on Multimedia, 2019, 21(1):65-73.

[25] K. M. Hosny, M. M. Darwish, M. M. Fouda. Robust color images watermarking using new fractional-order exponent moments. IEEE Access, 2021, 9: 47425-47435.

[26] X. Zhou, Y. Ma, Q. Zhang, M. A. Mohammed, R. Damaševičius. A reversible watermarking system for medical color images: balancing capacity, imperceptibility, and robustness. Electronics, 2021, 10: 1024. https://doi.org/10.3390/electronics10091024.

[27] Zhiqiu Xia, Xingyuan Wang, Mingxu Wang, Salahuddin Unar, Chunpeng Wang, Ying Liu. Geometrically invariant color medical image null-watermarking based on precise quaternion polar harmonic Fourier moments. IEEE Access, 2019, 7: 122544-122560.

[28] K. M. Hosny, M. M. Darwish. Resilient color image watermarking using accurate quaternion radial substituted Chebyshev moments. ACM Transactions on Multimedia Computing, Communications, and Applications, 2019, 15(2): 1-25.

[29] K. M. Hosny, M. M. Darwish. Robust color image watermarking using invariant quaternion Legendre-Fourier moments. Multimedia Tools and Applications, 2018, 77(19): 24727-24750.

[30] C. P. Wang, X. Y. Wang, Y. W. Li, Z. Q. Xia, C. Zhang. Quaternion polar harmonic Fourier moments for color images. Information Sciences, 2018, 450:141-156.

[31] C. P. Wang, X. Y. Wang, Z. Q. Xia. Geometrically invariant image watermarking based on fast radial harmonic Fourier moments. Signal Processing: Image Communication, 2016, 45:10-23.

[32] S. Nadarajah, S. Kotz. The beta exponential distribution. Reliability Engineering & System Safety, 2006, 91(6):689-697.

[33] S. Kumar, P. Chhaparwal, G. Zou. A robust unbiased dual to product estimator for population mean through modified maximum likelihood in simple random sampling. Cogent Mathematics, 2016, 3(1):1168070.

[34] E. Oral. Modified maximum likelihood estimation in Poisson regression. Biom Biostat Int J, 2017, 6(1):00154.

[35] D. C. Vaughan, M. L. Tiku. Estimation and hypothesis testing for a nonnormal bivariate distribution with applications. Mathematical and Computer Modelling, 2000, 32(1–2):53-67.

[36] XAvailable: http://decsai.ugr.es/cvg/dbimagenes/index.php.

[37] H. J. Qu, Y. H. Peng. Contourlet coefficient modeling with generalized Gaussian distribution and application. Proceedings of the International Conference on Audio, Language and Image Processing, Shanghai, China, 2008:531-535.

[38] M. Amirmazlaghani. Heteroscedastic watermark detector in the contourlet domain. IET Computer Vision, 2019, 13(3): 249-260.