Fractional-Order Spatial Steganography and Blind Steganalysis for Printed Matter: Anti-Counterfeiting for Product External Packing in Internet-of-Things

Yi-Fei Pu, Ni Zhang, and Huai Wang

Abstract—**This paper advocates a novel conceptual formulation of the fractional-order spatial steganography (FSS) and blind steganalysis for printed matter, which can be efficiently employed in the anti-counterfeiting for product external packing in Internet-of-Things (IoT). Traditional digital steganography is not printable. Within the limits of our knowledge, until now, there are not a well-established steganography and a corresponding steganalysis for printed matter in IoT, which should receive desired attention. Fractional calculus has potentially received prominence in applications in the domain of image processing mainly because of its strengths like long-term memory, nonlocality, and weak singularity. Therefore, in an attempt to overcome the aforementioned technical limitation of traditional digital steganography, this paper has studied here, as an interesting theoretical problem, would it be possible to apply the capability of preserving the edges and textural details of fractional calculus to the achievement of the steganography and steganalysis for printed matter in IoT. Motivated by this inspiration, in this work, this paper introduces a novel conceptual formulation of an FSS and a fractional-order blind steganalysis (FBS) for printed matter. At first, according to the opponent process theory of color vision, to better achieve the imperceptibility of the hidden secret information, this paper uses both the self-similar complex textures in a neighborhood and the opponent channel of blue versus yellow to implement FSS for printed matter. Second, without requiring *a priori* knowledge regarding the characteristics of the original carrier image, hidden secret image, and steganography, an FBS, a fractional-order multimodal function optimization algorithm, is proposed. Finally, the efficient capability of hiding secret information of FSS and that of detecting secret information of FBS are analyzed in detail experimentally, respectively. These two important advantages lead to the superiority of the proposed approach for defending against statistics attack, rotation and distortion attack, cropping attack, scaling attack, noise attack, and color copy attack. The main contribution of this paper is the first preliminary attempt of a feasible achievement of a spatial steganography and a blind steganalysis for printed matter.**

Index Terms—**Anti-counterfeiting, fractional calculus, fractional-order blind steganalysis (FBS), fractional-order spatial steganography (FSS), printed matter.**

I. Introduction

STEGANOGRAPHY and steganalysis are a pair of inverse operations of an achievement of hiding a secret information (file, message, image, or video) into another carrier information (file, message, image, video, or printed matter) and the art of detecting hidden information, respectively. Steganography is a form of security through obscurity, which lacks a shared secret. The key-dependent steganographic schemes follow Kerckhoffs's principle [1]. Cryptography is an implementation of protecting the contents of a message alone, however, steganography concerns itself with hiding intended secret information that does not attract attention to itself as an object of scrutiny. Numerous methods of steganography ranging from the simple approaches to highly sophisticated algorithms are available in literatures: in digital text, a steganographic method for data concealing in Microsoft Word documents using the word processor's change tracking feature was proposed [2]. In telecommunication network, network steganography uses communication protocols' control elements and their intrinsic functionality that was already applied in the late 1980s by Girling [3] and Wolf [4]. Typical network steganography involves the modification of the properties of a single network protocol [5], [6]. Moreover, specific network steganography uses the relationship between two or more different network protocols to achieve secret communication [7], [8]. In puzzle image, the art of hiding data in a puzzle utilizes the starting information to encode a key within the puzzle image [9]. In cyber-physical systems (CPS)/Internet-of-Things (IoT), the steganography for CPS/IoT overlaps with network steganography, whose secret data are hided in communication protocols used in CPS/IoT or in CPS components [10], [11]. To promote secure data transfer in smart IoT environment, a security scheme is advocated to employ a combined approach of lightweight cryptography and variable least significant bit substitution steganography technique [12]. Djebbar and Abu-Ali [13]

Manuscript received August 1, 2018; revised November 11, 2018 and November 28, 2018; accepted December 1, 2018. Date of publication December 14, 2018; date of current version July 31, 2019. This work was supported in part by the National Natural Science Foundation of China under Grant 61571312, in part by the National Key Research and Development Program Foundation of China under Grant 2018YFC0830300 and Grant 2017YFB0802300, and in part by the Science and Technology Support Project of Chengdu PU Chip Science and Technology Company, Ltd. *(Corresponding authors: Yi-Fei Pu; Ni Zhang.)*

Y.-F. Pu is with the College of Computer Science, Sichuan University, Chengdu 610065, China, and also with the Research and Development Department, Chengdu PU Chip Science and Technology Company, Ltd., Chengdu 610066, China (e-mail: puyifei@scu.edu.cn).

N. Zhang is with the College of Computer Science, Sichuan University, Chengdu 610065, China (e-mail: zhangni77@yeah.net).

H. Wang is with the Research and Development Department, Chengdu PU Chip Science and Technology Company, Ltd., Chengdu 610066, China (e-mail: 478961375@qq.com).

Digital Object Identifier 10.1109/JIOT.2018.2886996

presented a combined maximum entropy energy approach for audio steganalysis. Bairagi *et al.* [14] proposed three information hiding techniques for protecting communication in critical IoT infrastructure with the help of steganography, where RGB images are used as carriers for the information. Kim *et al.* [15] proposed an anti-reverse-engineering dynamic tamper detection scheme that applies image steganography to distribute and hide code in portable network graphics image files. Elhoseny *et al.* [16] proposed a hybrid security model for securing the diagnostic text data in medical images. Soni *et al.* [17] illustrated the advantage of discrete fractional Fourier transform as compared to other transforms for steganography in image processing. Roy and Goel [18] reviewed the major steganography techniques in spatial and transformational domain keeping the main focus on image steganography. In particular, for the anti-counterfeiting in IoT, electronic digital steganography output can be in the form of printed matters, i.e., the product external packing. Bacon's cipher is an approach of steganography proposed by Francis Bacon that a message is concealed in the presentation of text rather than its content [19]. However, the ciphertext produced by most of classic digital steganography methods is not printable. Traditional digital methods rely on perturbing noise in the channel file to hide the message, and as such, the channel file must be transmitted to the recipient with no additional noise from the transmission. Although some types of modern color laser printers integrate the model, serial number, and timestamps on each printout for traceability by using a dot-matrix code made of small, yellow dots not recognizable to the naked eye, printing inevitably introduces much noise in the ciphertext, as a result, generally rendering the message undetectable. There are techniques that address this limitation, such as ASCII art steganography [20]. Until now, steganography and steganalysis for printed matter in IoT have been seldom studied, which require extensive research attention.

In recent times, fractional calculus has evolved as an important, contemporary branch of mathematical analyses [16]–[21], which now seems to be gaining its acceptance as a novel promising mathematical method among the physical scientists and engineering technicians. Fractional calculus extends the concepts of the integer-order difference and Riemann sums. The fractional differential, except based on the Caputo definition, of a Heaviside function is nonzero, whereas its integer-order differential must be zero [16]–[21]. The fractional calculus of various functions possesses one obvious feature: the fractional calculus of most functions is equal to a power series, whereas that of the remaining functions is equal to the superposition or product of a certain function and a power function [16]–[21]. Several scientific studies, such as the fractional diffusion processes [22], [23], fractional viscoelasticity [24], fractal dynamics [25], fractional control [26], [27], fractor (fractional resistor) and fracmemristor (fractional memristor) [28]–[32], fractional image processing [33]–[36], fractional signal processing [37], fractional neural networks [38], [39], have demonstrated that a fractional-order or a fractional dimensional approach is now the best way that many natural phenomena can be used to be described.

However, the application of fractional calculus to the steganography and steganalysis for printed matter in IoT is an emerging field of research that has seldom received desired attention. The properties of the fractional calculus of a signal are quite different from those of its integer order calculus. Fractional calculus has been applied to signal processing and image processing mainly because of its inherent strengths in terms of long-term memory, nonlocality, and weak singularity [16]–[21]. Some progress in the studies on fractional-order image processing not only validates the fractional-order partial differential equations, but also provides interesting and practical suggestions for future research. For instance, a fractional differential provides the flexibility of enhancing the complex textural details of an image in a nonlinear manner [31]–[33], it can maintain the low-frequency contour features in the smooth area of an image in a nonlinear fashion, and creates the possibility of enhancing the high-frequency edges and textural details, in a nonlinear manner, in those areas, where the gray level undergoes frequent or unusual variations [31]–[33]. Therefore, to overcome the aforementioned technical limitation (traditional digital steganography is not printable), an interesting theoretical problem emerges naturally: would it be possible to apply the capability of preserving the edges and textural details of fractional calculus to the achievement of the steganography and steganalysis for printed matter in IoT. Motivated by this inspiration, in this paper, this work introduces a novel conceptual formulation of a fractional-order spatial steganography (FSS) and a fractional-order blind steganalysis (FBS) for printed matter, which are a pair of efficient inverse operations of the anti-counterfeiting for product external packing in IoT. In the light of the opponent process theory of color vision, to better implement the imperceptibility of the hidden secret information, both the self-similar complex textures in a neighborhood and the opponent channel of blue versus yellow are applied to implement FSS for printed matter. Furthermore, without requiring *a priori* knowledge regarding the characteristics of the original carrier image, hidden secret image, and steganography, this paper proposes an FBS that is a fractional-order ant colony algorithm. The efficient capability of hiding secret information of FSS and that of detecting secret information of FBS are two important advantages that lead to the superiority of the proposed approach for defending against statistics attack, rotation and distortion attack, cropping attack, scaling attack, noise attack, and color copy attack.

The rest of this paper is organized as follows. Section II presents in brief the necessary mathematical background of fractional calculus, required for subsequent presentation of the work carried out. Section III proposes the formulation of a spatial FSS and a blind FBS for printed matter in IoT. At first, this paper implements a spatial FSS for printed matter based on the theory of fractal dynamics, the trichromatic theory of color vision, and the opponent process theory of color vision. This is followed by the formulation and implementation of a blind FBS for printed matter inspired by the classic integer-order ant colony algorithm.

Section IV presents the experiment results obtained and the associated analyses carried out. Here, by employing seven examples, this paper achieves the performance analysis of FSS and that of FBS for printed matter in IoT. This paper further analyzes the efficient capability of FSS and FBS to defense against statistics attack, rotation and distortion attack, cropping attack, scaling attack, noise attack, and color copy attack. In Section V, the conclusions of this paper are presented.

II. Mathematical Background

This section presents a brief introduction to the necessary mathematical background of fractional calculus and fractional difference.

The commonly used fractional calculus definitions are those of Grünwald–Letnikov, Riemann–Liouville, and Caputo [16]–[21]. In this paper, this work mainly adopts the Grünwald–Letnikov defined fractional calculus for the following mathematical derivation. The Grünwald–Letnikov definition of fractional calculus of order v, in a convenient form, for a causal function $f(x)$, is defined by

$$ {}^{G-L}_{\ a}D^{v}_{x}f(x) = \lim_{N\to\infty}\left\{\frac{\left(\frac{x-a}{N}\right)^{-v}}{\Gamma(-v)}\sum_{k=0}^{N-1}\frac{\Gamma(k-v)}{\Gamma(k+1)}f\left[x-k\left(\frac{x-a}{N}\right)\right]\right\} \tag{1}$$

where $f(x)$ is a differintegrable function [16]–[21], $[a, x]$ is the duration of $f(x)$, v is a noninteger, $\Gamma(\alpha) = \int_0^\infty e^{-x}x^{\alpha-1}dx$ is the Gamma function, N is an integer and ${}^{G-L}_{\ a}D^{v}_{x}$ denotes the Grünwald–Letnikov defined fractional differential operator. Let us use $\Delta x = (x-a)/N$ to denote the discrete interval of duration $[a, x]$. Thus, from (1), in duration $[x - N\Delta x, x]$, the v order Grünwald–Letnikov defined fractional forward difference, ${}^{G-L}_{\ a}\mathrm{Diff}^{v}_{x}$, can be derived as

$$\begin{aligned} {}^{G-L}_{\ a}\mathrm{Diff}^{v}_{x}f(x) &= \frac{1}{(\Delta x)^{v}}\sum_{k=0}^{N-1}\frac{\Gamma(k-v)}{\Gamma(-v)\Gamma(k+1)}f(x-k\Delta x)\\ &= \frac{1}{(\Delta x)^{v}}\left[f(x)+\sum_{k=1}^{N-1}\frac{\Gamma(k-v)}{\Gamma(-v)\Gamma(k+1)}f(x-k\Delta x)\right]. \end{aligned} \tag{2}$$

In (2), when the weighting coefficient of $f(x - k\Delta x)$ is taken as its absolute value, $|[(\Gamma(k-v))/(\Gamma(-v)\Gamma(k+1))]|$, ${}^{G-L}_{\ a}\mathrm{Diff}^{v}_{x}f(x)$ converts to be the v order absolute fractional difference of $f(x)$. In particular, from (2), the classic first-order forward difference, for a causal function $f(x)$, can be given as

$$ {}_{a}\mathrm{Diff}^{1}_{x}f(x) = \frac{1}{\Delta x}\left[f(x) - f(x-\Delta x)\right] \tag{3}$$

where ${}_{a}\mathrm{Diff}^{1}_{x}$ denotes the first-order difference. Equations (2) and (3) show that the long-term memory, nonlocality and weak singularity characteristics of fractional difference are major advantages compared with those of the classic first-order difference.

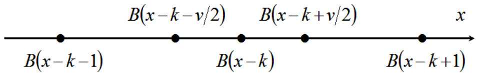


Fig. 1. FSS in x direction.

III. FSS and Blind Steganalysis for Printed Matter

A. Implementation of FSS for Printed Matter

In this section, an FSS for printed matter is implemented.

FSS for printed matter is introduced based on the theory of fractal dynamics [25], the trichromatic theory of color vision [40], and the opponent process theory of color vision [21]. Media files are ideal for FSS because of their large size. For instance, a hider might start with an original carrier image and adjust the color of every hundredth pixel to correspond to a hidden secret letter or image. The change is so subtle that someone who is not specifically looking for it is unlikely to notice the change. According to the theory of fractal dynamics [25], an important rule of complex systems is of evolution. Most of the fractal structures are the evolutionary processes (such as fractal growth) or evolutionary final products (such as fracture surface) of objective things. For a natural image, the gray level values of pixels in a neighborhood are highly correlative and self-similar. In a natural image, such fractal-like structures are usually presented as self-similar complex textural detail features. In addition, the trichromatic theory of color vision [40] explains how the three types of cones detect different light wavelengths, while the opponent process theory of color vision [21] explains how the cones connect to the ganglion cells. According to the trichromatic theory of color vision [40], there are three cone receptors in the retina, short-wavelength receptor (blue), medium-wavelength receptor (green), and long-wavelength receptor (red), which are responsible for the perception of color in the visible spectrum. The visual sensitivity of the naked eye to blue light is much lower than those to green light and red light. Further, according to the opponent process theory of color vision [21], these three cone receptors have some overlap in the wavelengths of light to which they respond. There are three opponent channels: 1) red versus green; 2) blue versus yellow; and 3) black versus white. Response to one color of an opponent channel is antagonistic to that to the other color. That is, opposite opponent colors are never perceived together. There is no "greenish red" or "yellowish blue." From aforementioned discussion, to better achieve the imperceptibility of the hidden secret information, this paper uses both the self-similar complex textures in a neighborhood and the opponent channel of blue versus yellow to implement FSS for printed matter.

Since the opponent channel of blue versus yellow is merely applied, for an original carrier image $S(x, y)$, this paper only uses its B value in the RGB color space, $B(x, y)$, for further processing. For digital image processing, the smallest discrete sampling interval of $B(x, y)$ is equal to one pixel. For the convenience of illustration, this paper first discusses FSS in the x direction, as illustrated in Fig. 1.

In Fig. 1, k and $0 < v \le 1$ are an integer and the fractional-order, respectively. $B(x-k)$ is an original carrier pixel of interest. $B(x-k-1)$ and $B(x-k+1)$ are two neighboring pixels of $B(x-k)$ in its neighborhood. Fig. 1 indicates that to make full use of the self-similar complex textures in a neighborhood, FSS in the x direction introduces two additional signal values, $B(x-k-v/2)$ and $B(x-k+v/2)$, on the nonpixel, fractional pixel, pixels of $B(x)$. According to the three-point (quadratic) Lagrange interpolation formula, using $B(x-k-1)$, $B(x-k)$, and $B(x-k+1)$, $B(x-k-v/2)$ and $B(x-k+v/2)$ can be estimated as follows, respectively:

$$B(x-k-v/2) \cong \left(\frac{v}{4}+\frac{v^2}{8}\right)B(x-k-1) + \left(1-\frac{v^2}{4}\right)B(x-k) + \left(\frac{v^2}{8}-\frac{v}{4}\right)B(x-k+1) \tag{4}$$

$$B(x-k+v/2) \cong \left(\frac{v}{4}+\frac{v^2}{8}\right)B(x-k+1) + \left(1-\frac{v^2}{4}\right)B(x-k) + \left(\frac{v^2}{8}-\frac{v}{4}\right)B(x-k-1) \tag{5}$$

where the fractional-order $0 < v \le 1$ adaptively varies with the relative total variation of $B(x-k)$ with respect to $B(x-k-1)$ and $B(x-k+1)$, which can be given as

$$v(x-k) = 1 - \left|\frac{1-\exp\{-[2B(x-k)-B(x-k-1)-B(x-k+1)]\}}{1+\exp\{-[2B(x-k)-B(x-k-1)-B(x-k+1)]\}}\right|. \tag{6}$$

Equation (6) indicates that if $[2B(x-k)-B(x-k-1)-B(x-k+1)] = 0$, the fractional-order $v = 1$. That is, if the relative total variation of $B(x-k)$ with respect to $B(x-k-1)$ and $B(x-k+1)$ is equal to zero, $B(x-k-v/2)$ and $B(x-k+v/2)$ are in the middle of $[B(x-k-1)$ and $B(x-k)]$ and $[B(x-k)$ and $B(x-k+1)]$, respectively. If $[2B(x-k)-B(x-k-1)-B(x-k+1)] \neq 0$, the fractional-order $0 < v < 1$. The value of v decreases with the increase of the absolute value of the relative total variation of $B(x-k)$ with respect to $B(x-k-1)$ and $B(x-k+1)$, and vice versa. The smaller v is the closer $B(x-k-v/2)$ and $B(x-k+v/2)$ move toward to $B(x-k)$, and vice versa. Further, to better achieve the imperceptibility of the hidden secret information, from (4) and (5), the $B^*(x-k)$ after concealing manipulation is given as

$$B^*(x-k) = \begin{cases} B(x-k)+\lambda\eta(x-k)\frac{[B(x-k-v/2)+B(x-k+v/2)]}{2}, & \text{if } B(x-k) \le \xi(x-k) \\ B(x-k)-\lambda\eta(x-k)\frac{[B(x-k-v/2)+B(x-k+v/2)]}{2}, & \text{if } B(x-k) > \xi(x-k) \end{cases} \tag{7}$$

where $B^*(x-k)$ is an embedded image with secret information, $\lambda > 0$ is an concealing intensity coefficient, $\eta(x-k) = \min[([255-B(x-k)]/255), ([B(x-k)-0]/255)]$, and $\xi(x-k)$ is the neighborhood averaging of $B(x-k)$, for example, $B(x-k) = [B(x-k-v/2)+B(x-k)+B(x-k+v/2)]/3$. Note that at first, if $B(x-k) = 0$, this paper sets $\eta = 0.5$; if $B(x-k) = 255$, this paper sets $\eta = -0.5$. Second, if $B^*(x-k) < 0$, this paper sets $B^*(x-k) = 255 \times \mathrm{abs}\{B^*(x-k)/255 - \mathrm{fix}[B^*(x-k)/255]\}$; if $B^*(x-k) > 255$, we set $B^*(x-k) = 255 - 255 \times \{B^*(x-k)/255 - \mathrm{fix}[B^*(x-k)/255]\}$, where abs() denotes an absolute value function, and fix() denotes a rounding function toward zero. Equation (7) shows that at first, if $B(x-k) \le \xi(x-k)$, this paper sets $B^*(x-k) = B(x-k) + \lambda\eta(x-k)([B(x-k-v/2)+B(x-k+v/2)]/2)$; if $B(x-k) > \xi(x-k)$, we set $B^*(x-k) = B(x-k) - \lambda\eta(x-k)([B(x-k-v/2)+B(x-k+v/2)]/2)$. To achieve anti-statistics steganalysis, FSS keeps the statistical characteristics of $B^*(x-k)$ being nearly the same as those of $B(x-k)$. Second, to restrict $B^*(x-k)$ within the range of $[0, 255]$ as possible, $\eta(x-k)$ adaptively adjusts the amount of hiding information varying with the value of $B(x-k)$.

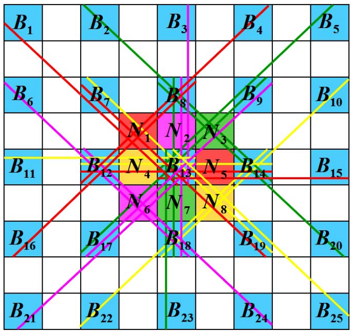


Fig. 2. 2-D FSS for printed matter.

Next, in a similar way, to make full use of the self-similar complex textures in a neighborhood, the 2-D FSS for printed matter is implemented, as illustrated in Fig. 2.

In Fig. 2, to prevent from cross-border access, we expand two pixels outward the boundary pixels of $B(x, y)$ through mirror-injection. In Fig. 2, the wathet blue squares denote the discrete pixels of $B(x, y)$, of which $B_1 = B(x-2, y-2)$, $B_2 = B(x-2, y-1)$, $B_3 = B(x-2, y)$, $B_4 = B(x-2, y+1)$, $B_5 = B(x-2, y+2)$, $B_6 = B(x-1, y-2)$, $B_7 = B(x-1, y-1)$, $B_8 = B(x-1, y)$, $B_9 = B(x-1, y+1)$, $B_{10} = B(x-1, y+2)$, $B_{11} = B(x, y-2)$, $B_{12} = B(x, y-1)$, $B_{13} = B(x, y)$, $B_{14} = B(x, y+1)$, $B_{15} = B(x, y+2)$, $B_{16} = B(x+1, y-2)$, $B_{17} = B(x+1, y-1)$, $B_{18} = B(x+1, y)$, $B_{19} = B(x+1, y+1)$, $B_{20} = B(x+1, y+2)$, $B_{21} = B(x+2, y-2)$, $B_{22} = B(x+2, y-1)$, $B_{23} = B(x+2, y)$, $B_{24} = B(x+2, y+1)$, and $B_{25} = B(x+2, y+2)$. B_{13} is an original carrier pixel of interest. Moreover, the white squares, yellow ones, green ones, amaranthine ones, and red ones denote the additional fractional pixel pixels of $B(x, y)$, of which $N_1 = B(x-v/2, y-v/2)$, $N_2 = B(x-v/2, y)$, $N_3 = B(x-v/2, y+v/2)$, $N_4 = B(x, y-v/2)$, $N_5 = B(x, y+v/2)$, $N_6 = B(x+v/2, y-v/2)$, $N_7 = B(x+v/2, y)$, and $N_8 = B(x+v/2, y+v/2)$. In Fig. 2, red edges, amaranthine ones, green ones, and yellow ones denote the neighborhood ranges of corresponding color squares in different directions, respectively. Every color edges come in pairs in the opposite direction. There are eight neighboring fractional pixel pixels, N_1, N_2, N_3, N_4, N_5, N_6, N_7, and N_8, around B_{13}, which from (4) and (5), can be given as

$$N_1 = \frac{1}{4}\left[\begin{array}{l} \left(\frac{v}{4}+\frac{v^2}{8}\right)B_7+\left(1-\frac{v^2}{4}\right)B_{13}+\left(\frac{v^2}{8}-\frac{v}{4}\right)B_{19}+\left(\frac{v}{4}+\frac{v^2}{8}\right)B_{13} \\ +\left(1-\frac{v^2}{4}\right)B_7+\left(\frac{v^2}{8}-\frac{v}{4}\right)B_1+\left(\frac{v}{4}+\frac{v^2}{8}\right)B_{12}+\left(1-\frac{v^2}{4}\right)B_8 \\ +\left(\frac{v^2}{8}-\frac{v}{4}\right)B_4+\left(\frac{v}{4}+\frac{v^2}{8}\right)B_8+\left(1-\frac{v^2}{4}\right)B_{12}+\left(\frac{v^2}{8}-\frac{v}{4}\right)B_{16} \end{array}\right] \tag{8}$$

$$N_2 = \frac{1}{2}\begin{bmatrix} \left(\frac{v}{4}+\frac{v^2}{8}\right)B_8+\left(1-\frac{v^2}{4}\right)B_{13}+\left(\frac{v^2}{8}-\frac{v}{4}\right)B_{18} \\ +\left(\frac{v}{4}+\frac{v^2}{8}\right)B_{13}+\left(1-\frac{v^2}{4}\right)B_8+\left(\frac{v^2}{8}-\frac{v}{4}\right)B_3 \end{bmatrix} \tag{9}$$

$$N_3 = \frac{1}{4}\begin{bmatrix} \left(\frac{v}{4}+\frac{v^2}{8}\right)B_{13}+\left(1-\frac{v^2}{4}\right)B_9+\left(\frac{v^2}{8}-\frac{v}{4}\right)B_5+\left(\frac{v}{4}+\frac{v^2}{8}\right)B_9 \\ +\left(1-\frac{v^2}{4}\right)B_{13}+\left(\frac{v^2}{8}-\frac{v}{4}\right)B_{17}+\left(\frac{v}{4}+\frac{v^2}{8}\right)B_{14}+\left(1-\frac{v^2}{4}\right)B_8 \\ +\left(\frac{v^2}{8}-\frac{v}{4}\right)B_2+\left(\frac{v}{4}+\frac{v^2}{8}\right)B_8+\left(1-\frac{v^2}{4}\right)B_{14}+\left(\frac{v^2}{8}-\frac{v}{4}\right)B_{20} \end{bmatrix} \tag{10}$$

$$N_4 = \frac{1}{2}\begin{bmatrix} \left(\frac{v}{4}+\frac{v^2}{8}\right)B_{13}+\left(1-\frac{v^2}{4}\right)B_{12}+\left(\frac{v^2}{8}-\frac{v}{4}\right)B_{11} \\ +\left(\frac{v}{4}+\frac{v^2}{8}\right)B_{12}+\left(1-\frac{v^2}{4}\right)B_{13}+\left(\frac{v^2}{8}-\frac{v}{4}\right)B_{14} \end{bmatrix} \tag{11}$$

$$N_5 = \frac{1}{2}\begin{bmatrix} \left(\frac{v}{4}+\frac{v^2}{8}\right)B_{14}+\left(1-\frac{v^2}{4}\right)B_{13}+\left(\frac{v^2}{8}-\frac{v}{4}\right)B_{12} \\ +\left(\frac{v}{4}+\frac{v^2}{8}\right)B_{13}+\left(1-\frac{v^2}{4}\right)B_{14}+\left(\frac{v^2}{8}-\frac{v}{4}\right)B_{15} \end{bmatrix} \tag{12}$$

$$N_6 = \frac{1}{4}\begin{bmatrix} \left(\frac{v}{4}+\frac{v^2}{8}\right)B_{12}+\left(1-\frac{v^2}{4}\right)B_{18}+\left(\frac{v^2}{8}-\frac{v}{4}\right)B_{24}+\left(\frac{v}{4}+\frac{v^2}{8}\right)B_{18} \\ +\left(1-\frac{v^2}{4}\right)B_{12}+\left(\frac{v^2}{8}-\frac{v}{4}\right)B_6+\left(\frac{v}{4}+\frac{v^2}{8}\right)B_{17}+\left(1-\frac{v^2}{4}\right)B_{13} \\ +\left(\frac{v^2}{8}-\frac{v}{4}\right)B_9+\left(\frac{v}{4}+\frac{v^2}{8}\right)B_{13}+\left(1-\frac{v^2}{4}\right)B_{17}+\left(\frac{v^2}{8}-\frac{v}{4}\right)B_{21} \end{bmatrix} \tag{13}$$

$$N_7 = \frac{1}{2}\begin{bmatrix} \left(\frac{v}{4}+\frac{v^2}{8}\right)B_{13}+\left(1-\frac{v^2}{4}\right)B_{18}+\left(\frac{v^2}{8}-\frac{v}{4}\right)B_{23} \\ +\left(\frac{v}{4}+\frac{v^2}{8}\right)B_{18}+\left(1-\frac{v^2}{4}\right)B_{13}+\left(\frac{v^2}{8}-\frac{v}{4}\right)B_8 \end{bmatrix} \tag{14}$$

$$N_8 = \frac{1}{4}\begin{bmatrix} \left(\frac{v}{4}+\frac{v^2}{8}\right)B_{14}+\left(1-\frac{v^2}{4}\right)B_{18}+\left(\frac{v^2}{8}-\frac{v}{4}\right)B_{22}+\left(\frac{v}{4}+\frac{v^2}{8}\right)B_{18} \\ +\left(1-\frac{v^2}{4}\right)B_{14}+\left(\frac{v^2}{8}-\frac{v}{4}\right)B_{10}+\left(\frac{v}{4}+\frac{v^2}{8}\right)B_{19}+\left(1-\frac{v^2}{4}\right)B_{13} \\ +\left(\frac{v^2}{8}-\frac{v}{4}\right)B_7+\left(\frac{v}{4}+\frac{v^2}{8}\right)B_{13}+\left(1-\frac{v^2}{4}\right)B_{19}+\left(\frac{v^2}{8}-\frac{v}{4}\right)B_{25} \end{bmatrix} \tag{15}$$

where the fractional-order $0 < v(x, y) \leq 1$ adaptively varies with the relative total variation of B_{13} with respect to $B_1 \sim B_{25}$, which can be given as

$$v(x, y) = 1 - \left| \frac{1 - \exp\left[-\sum_{i=1}^{25}(B_{13} - B_i)\right]}{1 + \exp\left[-\sum_{i=1}^{25}(B_{13} - B_i)\right]} \right|. \tag{16}$$

Further, to better achieve the imperceptibility of the hidden secret image, from (8)–(15), the $B(x, y)$ after concealing manipulation is given as

$$B^*(x, y) = \begin{cases} B(x, y) + \lambda\eta(x, y)\frac{1}{8}\sum_{i=1}^{8} N_i, & \text{if } B(x, y) \leq \xi(x, y) \\ B(x, y) - \lambda\eta(x, y)\frac{1}{8}\sum_{i=1}^{8} N_i, & \text{if } B(x, y) > \xi(x, y) \end{cases} \tag{17}$$

where $B^*(x, y)$ is an embedded image with secret information, $\lambda > 0$ is an concealing intensity coefficient, $\eta(x, y) = \min[([255 - B(x, y)]/255), ([B(x, y) - 0]/255)]$, and $\xi(x, y)$ is the neighborhood averaging of $B(x, y)$. Note that at first, if $B(x, y) = 0$, we set $\eta = 0.5$; if $B(x, y) = 255$, we set $\eta = -0.5$. Second, if $B^*(x, y) < 0$, we set $B^*(x, y) = 255 \times \text{abs}\{B^*(x, y)/255 - \text{fix}[B^*(x, y)/255]\}$; if $B^*(x, y) > 255$, we set $B^*(x, y) = 255 - 255 \times \{B^*(x, y)/255 - \text{fix}[B^*(x, y)/255]\}$. Equation (17) indicates that at first, if $B(x, y) \leq \xi(x, y)$, we set $B^*(x, y) = B(x, y) + \lambda\eta(x, y)\rho(x, y)(1/8)\sum_{i=1}^{8} N_i$; if $B(x, y) > \xi(x, y)$, we set $B^*(x, y) = B(x, y) - \lambda\eta(x, y)\rho(x, y)(1/8)\sum_{i=1}^{8} N_i$. To achieve anti-statistics attack, FSS keeps the statistical characteristics of $B^*(x, y)$ being nearly the same as those of $B(x, y)$. Second, to restrict $B^*(x, y)$ within the range of $[0, 255]$ as possible, $\eta(x, y)$ adaptively adjusts the amount of concealing information varying with the value of $B(x, y)$.

Finally, we let $B^*(x, y)$ as the B value, and combine $B^*(x, y)$ with the R and G values of the original carrier image $S(x, y)$ to obtain the final image hidden secret information, $S^*(x, y)$, for printing. Note that since the difference of structure features, performance, and parameters of various printers, the actually printed image of $S^*(x, y)$ has some kinds of distortions compared with $S^*(x, y)$.

B. Implementation of FBS for Printed Matter

In this section, an FBS for printed matter is implemented. No *a priori* knowledge regarding the characteristics of the original carrier image, hidden secret image, and steganography is either known or required.

Since the difference of structure features, physical performance, and parameters of various imaging devices, such as scanner, camera, and mobile phone, the captured pending printed image, $\hat{S}^*(x, y)$, has inevitably some kinds of distortions compared with the actually printed image of $S^*(x, y)$. Moreover, (16) and (17) indicate that the hidden secret information is small, which adaptively varies with the self-similar complex textures in a neighborhood of $B(x, y)$ at the hiding location. However, no matter how small any hidden secret information is, it always subtle changes the gray level of $B(x, y)$. That is, $B^*(x, y)$ adds nuance to $B(x, y)$. Therefore, this paper can uses a simple rule, a necessary condition, to determine whether the hidden secret information exists in the captured pending printed image $\hat{S}^*(x, y)$: whether the majority of local minimums or maximums in a neighborhood of a variational function $V(x, y)$ can be detected, which can be given as

$$V(x, y) = \hat{B}^*(x, y) - \frac{1}{2}\left[\hat{R}^*(x, y) + \hat{G}^*(x, y)\right] \tag{18}$$

where $\hat{R}^*(x, y)$, $\hat{G}^*(x, y)$, and $\hat{B}^*(x, y)$ are the R value, G value, and B value in the RGB color space of $\hat{S}^*(x, y)$. Note that at first, $V(x, y)$ could be negative. Second, to reduce the effect of noise, $V(x, y)$ is first performed by median filtering. To this end, inspired by the classic integer-order ant colony algorithm, an FBS, a fractional-order multimodal function optimization algorithm (a fractional-order ant colony algorithm), is proposed.

In the first step, provided $\chi_m = (x_m, y_m)$ is a feasible solution of a variational function $V(x, y)$, where $m = 1, 2, \ldots, Q_a$, Q_a is the quantity of ants in the ant colony of FBS, $x_m \in [\inf_x, \sup_x]$, $y_m \in [\inf_y, \sup_y]$, and ($\inf_x$ and $\sup_x$) and ($\inf_y$ and $\sup_y$) are the (infimum and supremum) of the solution space of $V(x, y)$ in the x direction and those in the y direction, respectively. In $V(x, y)$, there is $(\sup_x - \inf_x)(\sup_y - \inf_y)$ pixels. Without loss of generality, this paper sets $Q_a = (\sup_x - \inf_x)(\sup_y - \inf_y)/2$. Let us randomly generate Q_a initial feasible solutions, $\chi_m(0)$, according to the following formula:

$$\begin{cases} x_m(0) = \inf_x + \left(\sup_x - \inf_x\right) r_m \\ y_m(0) = \inf_y + \left(\sup_y - \inf_y\right) r_m \end{cases} \tag{19}$$

where $r_m \in (0, 1)$ is a random number. Further, for the v order FBS, in the t-th iteration, the mth ant transits itself from the current ith pixel to the next optional jth pixel according to the fractional-order transition probability, which can be given as

$$ {}^{m}p_{ij}^{v}(t) = \frac{1}{f_n} \begin{cases} p_{ij}(t) + \sum_{k=1}^{N_1-1} \left| \frac{\Gamma(k-v)}{\Gamma(-v)\Gamma(k+1)} \right| p_{(j+k-1)(j+k)}(t), \\ \qquad \text{if } j \in C_i^m(t) \text{ and } (j+k) \in C_i^m(t) \\ 0, \qquad \text{if } j \notin C_i^m(t) \end{cases} \tag{20} $$

where $f_n = \sum_{k=0}^{N_1-1} |([\Gamma(k-v)]/[\Gamma(-v)\Gamma(k+1)])|$ is a normalization factor, $0 < {}^{m}p_{ij}^{v}(t) < 1$ and $C_i^m(t)$ are the v order transition probability from the ith pixel to the jth one and set of next optional pixels connected with the ith one, respectively. $(N_1 - 1)$ is the quantity of sequential optional pixels closing to the jth pixel. When $k \geq 1$, $(j + k - 1)$, and $(j + k)$ denote the $(j + k - 1)$th pixel, and a next optional $(j + k)$th pixel connected with the $(j + k - 1)$th one, respectively. Comparing (20) with (2), it can be observed that at first, since iterations increase unit time, in (20), $\Delta t = 1$. Second, ${}^{m}p_{ij}^{v}(t)$ is the v order absolute fractional difference of $p_{ij}(t)$ and $p_{(j+k-1)(j+k)}(t)$ in a neighborhood of each edge (i, j), which can be given as

$$ p_{ij}(t) = \begin{cases} \frac{[\tau_{ij}(t)]^{\alpha}[\eta_{ij}(t)]^{\beta}}{\sum_{c \in C_i^m(t)} [\tau_{ic}(t)]^{\alpha}[\eta_{ic}(t)]^{\beta}}, & \text{if } j \in C_i^m(t) \\ 0, & \text{if } j \notin C_i^m(t) \end{cases} \tag{21} $$

$$ \begin{aligned} & p_{(j+k-1)(j+k)}(t) \\ & = \begin{cases} \frac{[\tau_{(j+k-1)(j+k)}(t)]^{\alpha}[\eta_{(j+k-1)(j+k)}(t)]^{\beta}}{\sum_{c \in C_{(j+k-1)}^m(t)} [\tau_{(j+k-1)c}(t)]^{\alpha}[\eta_{(j+k-1)c}(t)]^{\beta}}, & \text{if } (j+k) \in C_{(j+k-1)}^m(t) \\ 0, & \text{if } (j+k) \notin C_{(j+k-1)}^m(t) \end{cases} \end{aligned} \tag{22} $$

where $0 < p_{ij}(t) < 1$, $0 < p_{(j+k-1)(j+k)}(t) < 1$, and α and β are the weight parameters of the pheromone concentration and heuristic information, respectively. In (21) and (22), $\tau_{(j+k-1)(j+k)}(t)$ and $\eta_{(j+k-1)(j+k)}(t)$ are the pheromone concentration and heuristic information on each edge $(j + k - 1,\ j + k)$ in the t-th iteration. In (21) and (22), let us set $\tau_{ij}(t) = V[(x_i + x_j)/2, (y_i + y_j)/2]/\rho$ and $\eta_{ij}(t) = V[(x_i + x_j)/2, (y_i + y_j)/2]$, where $0 < \rho < 1$ is the rate of pheromone volatilization. From (2) and (20)–(22), it can be observed that at first, to enhance the exploration ability of FBS, when $k \geq 1$, the optional $(j + k)$th pixel connected with the $(j + k - 1)$th pixel is selected stochastically. Second, to enhance its searching ability, by using the v order absolute fractional difference, in (20), FBS takes full advantage of the long-term memory, nonlocality, and weak singularity characteristics of fractional difference. In particular, since $|\Gamma(k - v)/\Gamma(-v)\Gamma(k + 1)|$ is a nonlinear decreasing function of k, the corresponding contribution of $p_{(j+k-1)(j+k)}(t)$ to ${}^{m}p_{ij}^{v}(t)$ decreases with the increase of the distance between $(j+k-1)$th pixel and jth one. Therefore, in (20), the fractional-order transition probability of FBS avails ${}^{m}p_{ij}^{v}(t)$ to utilize the neighborhood information of current terrain, both $p_{ij}(t)$ and $p_{(j+k-1)(j+k)}(t)$, as much as possible. This helps FBS contribute positively to find a proper fractional-order nonlinear balance between its searching ability and exploration ability.

In the second step, to enhance the exploration ability of FBS, in the t-th iteration, if ${}^{m}p_{ij}^{v}(t) < p_{\text{th}}$, a local search, $x'_m(t) = x_m(t) + (2r_m - 1)\Delta x(t)$ and $y'_m(t) = y_m(t) + (2r_m - 1)\Delta y(t)$, is achieved; if ${}^{m}p_{ij}^{v}(t) \geq p_{\text{th}}$, a global search, $x'_m(t) = x_m(t) + (r_m - 1/2)(\sup_x - \inf_x)$ and $y'_m(t) = y_m(t) + (r_m - 1/2)(\sup_y - \inf_y)$, is implemented, where p_{th} is a threshold of transition probability and $\Delta x(t) = \Delta y(t) = 1/t$ is a little increment. In particular, if $x'_m(t) < \inf_x$, this paper sets $x'_m(t) = \inf_x$; if $x'_m(t) > \sup_x$, this paper sets $x'_m(t) = \sup_x$; if $y'_m(t) < \inf_y$, this paper sets $y'_m(t) = \inf_y$; and if $y'_m(t) > \sup_y$, this paper sets $y'_m(t) = \sup_y$. Then, on the one hand, for the sake of local minimum value of $V(x, y)$, if $V(x'_m, y'_m) < V(x_m, y_m)$, the mth ant transits from (x_m, y_m) to (x'_m, y'_m). Otherwise, it cannot be moved at all. On the other hand, for the sake of local maximum value of $V(x, y)$, if $V(x'_m, y'_m) > V(x_m, y_m)$, the mth ant transits from (x_m, y_m) to (x'_m, y'_m). Otherwise, it cannot be moved at all. This paper sets $V(x'_m, y'_m)$ to be the local optimal solution of $V(x, y)$ in the t-th iteration.

In the third step, after the achievement of the t-th iteration, let us update the optimal value of $V(x, y)$ in the t-th iteration. For Q_a feasible solutions, the corresponding gray levels of $V(x, y)$ at the visited pixels are sorted by size from small to large $(V_1(t) \leq \cdots \leq V_m(t) \leq \cdots \leq V_{N_3}(t) \leq \cdots \leq V_{Q_a}(t))$, where $V_m(t)$ is the gray level of $V(x, y)$ at the visited pixel of the mth ant in the t-th iteration. Then, to take advantage of the meritorious information obtained by elitist ants in the t-th iteration, let us select the ants with relatively smaller gray level of $V(x, y)$ at the visited pixel in the top $1 \leq N_3 \leq Q_a$ to be elitist ants and enhance the pheromone concentration on their visited paths. Thus, in the next $(t{+}1)$th iteration, from (1) and (2), the fractional-order pheromone update formula of FBS can be given as

$$ \tau_{ij}(t + 1) = (1 - \rho)\tau_{ij}(t) + \sum_{m=1}^{N_3} \left| \frac{\Gamma(m - v - 1)}{\Gamma(-v)\Gamma(m)} \right| \Delta\tau_{ij}^{m}(t) \tag{23} $$

where $\Delta t = 1$. In (23), the increment of pheromone concentration of the mth selected elitist ant, $\Delta\tau_{ij}^{m}(t)$, can be given as

$$ \Delta\tau_{ij}^{m}(t) = \begin{cases} V\big[(x_i + x_j)/2,\ (y_i + y_j)/2\big], & \text{if visited edge } (i, j) \\ 0, & \text{if dose not visit edge } (i, j). \end{cases} \tag{24} $$

Equations (23) and (24) show that by using the long-term memory, nonlocality and weak singularity characteristics of fractional difference, $\tau_{ij}(t + 1)$ takes advantage of meritorious information obtained by elitist ants in the previous t-th iteration as much as possible. In a similar way to (20)–(22), (23) and (24) are also inherently beneficial to fractional-order nonlinearly balance the searching ability and exploration ability of FBS.

In the fourth step, according to (20) and (23), let us update the fractional-order pheromone and implement the $(t + 1)$th iteration of FBS until the termination condition is true. This paper takes whether the number of total iterations gets to maximum as the termination condition of the iterative solution of FBS.

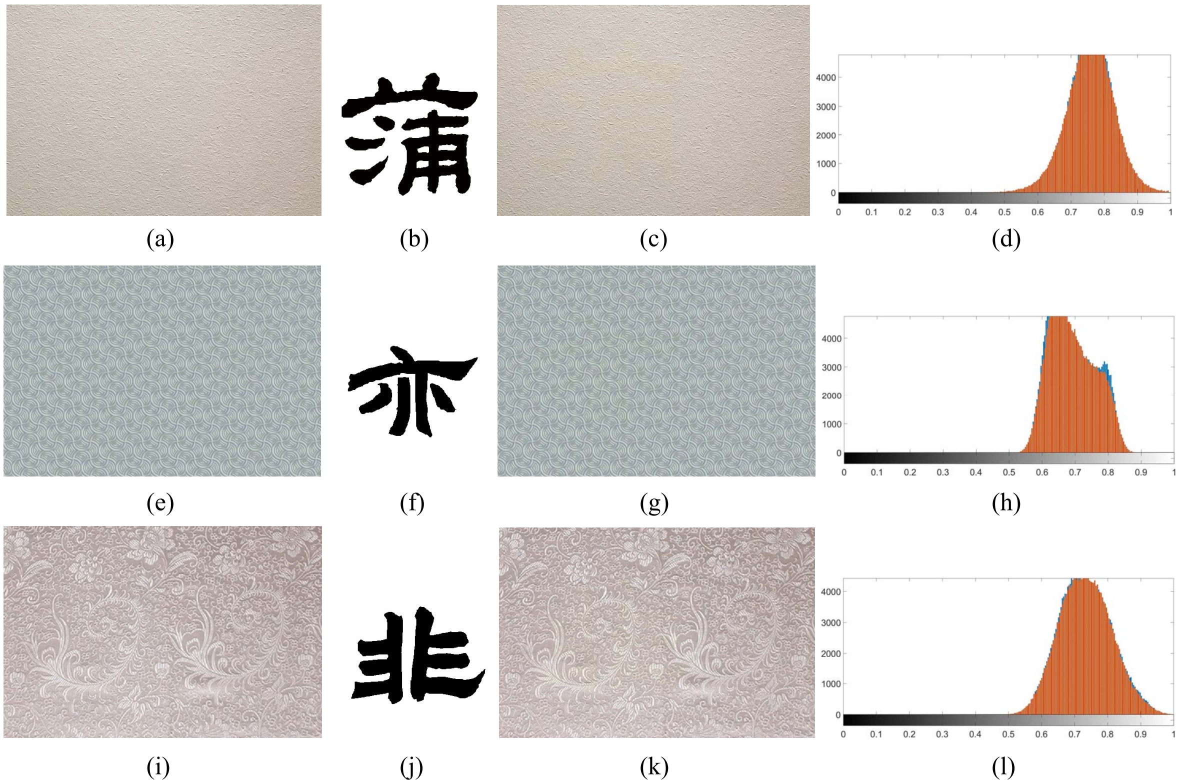


Fig. 3. Performance of FSS for printed matter. (a) China paper. (b) Chinese Pu. (c) (a) embedded with (b). (d) Gray histogram of both (a) and (c). (e) Woven design. (f) Chinese Yi. (g) (e) embedded with (f). (h) Gray histogram of both (e) and (g). (i) Sichuan brocade. (j) Chinese Fei. (k) (i) embedded with (j). (l) Gray histogram of both (i) and (k).

In the fifth step, after the termination of iteration, the gray levels of $\hat{S}^{*}(x, y)$ on the corresponding pixels of the detected local minimums or maximums in a neighborhood of $V(x, y)$ are set to be equal to zero.

IV. Experiment and Analysis

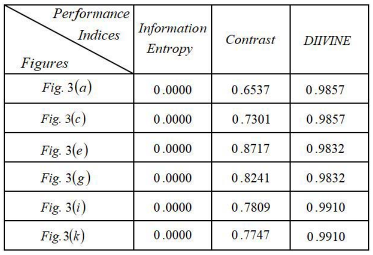
In this section, the performance analysis of FSS and that of FBS for printed matter in IoT are achieved. Within the limits of our knowledge, until now, there are not a well-established steganography and a corresponding steganalysis for printed matter in IoT. Therefore, this paper cannot consider some traditional steganography and corresponding steganalysis vis-à-vis our proposed FSS and corresponding FBS to achieve the following comparative experiments on performance analysis.

Example 1: The performance of FSS for printed matter in IoT was analyzed by using three suitable colorful texture images, i.e., a China paper image, a woven design image, and a Sichuan brocade image, as three original carrier images. The corresponding three hidden secret images are three clerical scripts of Chinese, i.e., Pu, Yi, and Fei. In particular, without loss of generality, in (17), this paper sets the hiding intensity coefficient $\lambda = 0.175$. The resolutions of an original carrier image $S(x, y)$ and a corresponding hidden secret image are equal to 600 × 400 and 370 × 370, respectively. This paper conceals a hidden secret image in the same scale original carrier region of $B(x, y)$ at the hiding location. The relative initial position of the hiding location of the original carrier region is at $(30, 30)$. Then, the results of the performance of FSS for printed matter in IoT are shown in Fig. 3.

In Fig. 3, the resolutions of Fig. 3(c), (g), and (k), are identical to those of Fig. 3(a), (e), and (i), which are all equal to equal to 600 × 400. Fig. 3(a), (e), and (i) are original carrier images. Fig. 3(b), (f), and (j) are the hidden secret images of clerical script for Fig. 3(a), (e), and (i), respectively. Fig. 3(c), (g), and (k) are the embedded images produced by FSS from [Fig. 3(a) and (b)], [Fig. 3(e) and (f)], and [Fig. 3(i) and (j)], respectively.

To consider the visual effects for the purpose of comparison, from Fig. 3, it can be observed that at first, the hidden secret images embedded by FSS in the corresponding carrier images are invisible. Since the visual sensitivity of the naked eye to blue light is much lower than those to green light and red light, in (16) and (17), this paper uses both the self-similar complex textures in a neighborhood and the opponent channel of blue versus yellow to implement FSS for printed matter. The hidden secret information adaptively slightly varies with the self-similar complex textures in a neighborhood of $B(x, y)$ at the hiding location. Then, in Fig. 3(c), (g), and (k), the hidden secret image of clerical script of Chinese Pu, Yi, and Fei are hardly perceptible, respectively. Second, FSS avails to defense against statistics attack. In (17), if $B(x, y) \leq \xi(x, y)$, $B^{*}(x, y) = B(x, y) + \lambda\eta(x, y)\rho(x, y)(1/8)\sum_{i=1}^{8} N_i$; if $B(x, y) > \xi(x, y)$, $B^{*}(x, y) = B(x, y) - \lambda\eta(x, y)\rho(x, y)(1/8)\sum_{i=1}^{8} N_i$. FSS keeps the statistical characteristics of $B^{*}(x, y)$ being nearly the same as those of $B(x, y)$. In Fig. 3(d), (h), and (l), brownish

TABLE I
PERFORMANCE INDICES BETWEEN IMAGE EMBEDDED WITH A HIDDEN SECRET IMAGE AND CORRESPONDING ORIGINAL CARRIER IMAGE UNDER CONSIDERATION



Performance Indices / *Figures*	*Information Entropy*	*Contrast*	*DIIVINE*
Fig. 3(*a*)	0.0000	0.6537	0.9857
Fig. 3(*c*)	0.0000	0.7301	0.9857
Fig. 3(*e*)	0.0000	0.8717	0.9832
Fig. 3(*g*)	0.0000	0.8241	0.9832
Fig. 3(*i*)	0.0000	0.7809	0.9910
*Fig.*3(*k*)	0.0000	0.7747	0.9910

red lines and blue ones denote the gray histograms of an original carrier image and a corresponding image embedded with a hidden secret image, respectively. In Fig. 3(d), (h), and (l), the gray histogram of an original carrier image is nearly the same as that of the corresponding image embedded with a hidden secret image. Only a few parts of the gray histogram of the image embedded with a hidden secret image are small different from those of the corresponding original carrier image.

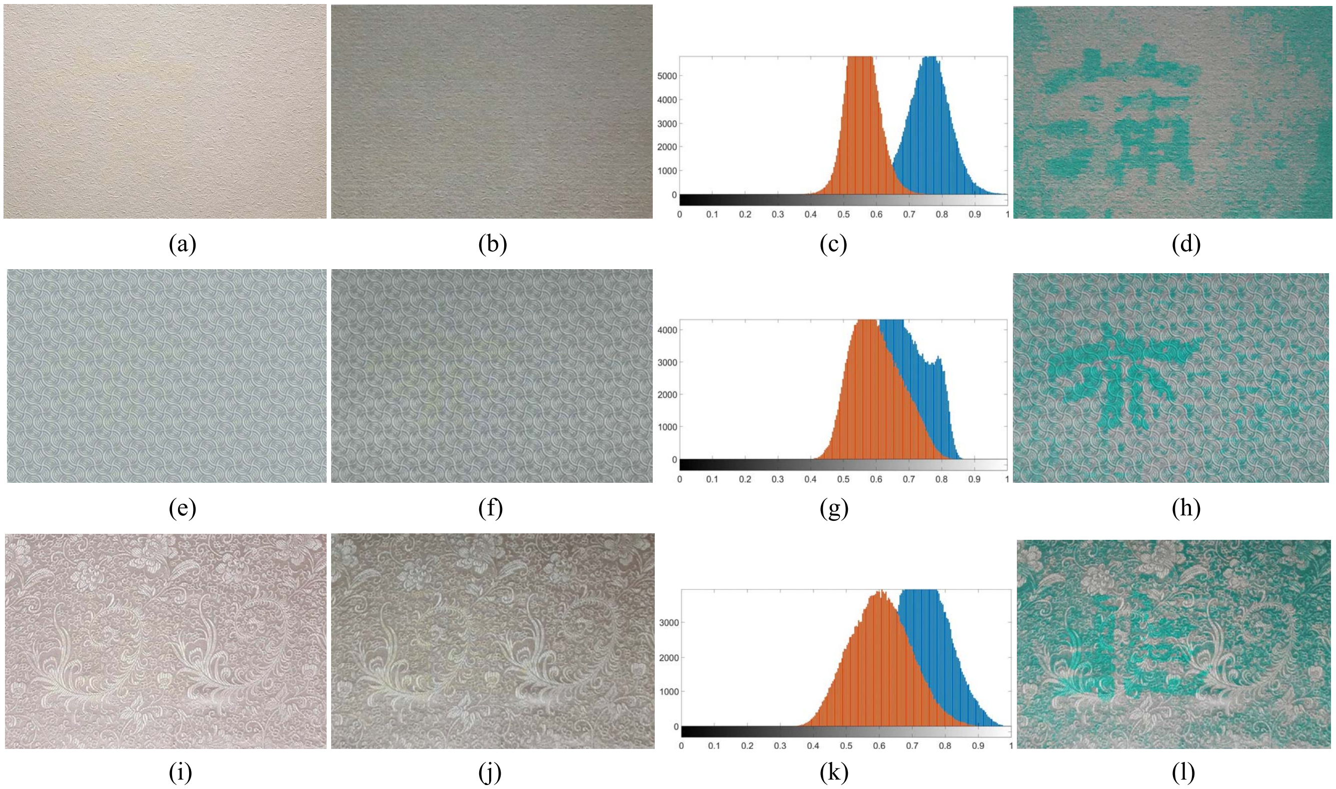
Next, with the objective of performing a quantitative analysis, this paper calculated information entropy, contrast, and the distortion identification-based image verity and integrity evaluation (DIIVINE) [42] between the image embedded with a hidden secret image produced by FSS and the corresponding original carrier image, to comprehensively evaluate the performance of FSS for printed matter in IoT under consideration. In this regard, DIIVINE is a nonreference image quality assessment index, which is based on natural scene statistics govern the behavior of natural images. DIIVINE assesses the quality of a distorted image, where the existence of a reference image is not mandatory. DIIVINE is based on a 2-stage framework involving distortion identification followed by distortion-specific quality assessment. Table I presents a comparative evaluation of the performance indices between the electronic embedded image produced by FSS and the corresponding original carrier image under consideration.

The results in Table I show that, at first, the capability of FSS to preserve the edges and textural details is efficient. The high-frequency edges and textural details of the produced images of FSS remain unchanged and well preserved. The information entropy and DIIVINE values of the images embedded with a hidden secret image produced by FSS are equal to those of corresponding original carrier image. Second, the contrast values of the electronic embedded image produced by FSS are small different from those of corresponding original carrier image, these result in their slight change of gray histograms in Fig. 3(d), (h), and (l). In addition, this paper also uses structural similarity (SSIM) [43] to evaluate the SSIM between the image embedded with a hidden secret image produced by FSS and the corresponding original carrier image. SSIM is used as a significant performance index that can be used to measure image degradation as a function of the perceived change in structural information, which is based on the human visual system. The SSIM indices between Fig. 3(a) and (c), Fig. 3(e) and (g), and Fig. 3(i) and (k) are 1.0000, 1.0000, and 1.0000, respectively. This indicates that the electronic embedded image produced by FSS and the corresponding original carrier image are complete consistent. From aforementioned quantitative analysis, it can be observed that FSS keeps the statistical characteristics of $B^*(x, y)$ being nearly the same as those of $B(x, y)$, which is beneficial to defense against statistics attack.

Example 2: The performance of FBS for printed matter in IoT was analyzed by using three captured pending printed image corresponding to Fig. 3(c), (g), and (k), respectively. In particular, without loss of generality, the copy/print papers is produced UPM Company, Ltd, whose page size is A4 (70 g/m^2). The printer is selected HP Deskjet 2520hc. When Fig. 3(c), (g), and (k) are sent to be printed, this paper sets printer properties to be plain paper and optimum printing quality. Further, this paper uses the camera self-contained in iPhone 7 to take photographs. In particular, the ambient light illumination is equal to 100–550 Lux. Then, the results of the performance of FBS for printed matter in IoT are shown in Fig. 4.

Fig. 4(b), (f), and (j) are the captured pending printed image corresponding to Fig. 4(a), (e), and (i), respectively. Fig. 4(d), (h), and (l) are the detected hidden secret image achieved by FBS from Fig. 4(b), (f), and (j), respectively.

To consider the visual effects for the purpose of comparison, from Fig. 4, it can be observed that at first, the hidden secret images embedded in the corresponding captured pending printed image are invisible. In Fig. 4(b), (f), and (j), the hidden secret image of clerical script of Chinese Pu, Yi, and Fei are almost imperceptible, respectively. Second, for the structure features, physical performance, and parameters of the selected printer camera self-contained in mobile phone, there is inevitably some degree of chromatic aberration, noise jamming, and distortion of the captured pending printed image compared with the corresponding electronic embedded image. Slight chromatic aberration between Fig. 4(b), (f), and (j) and Fig. 4(a), (e), and (i) can be observed, respectively. Third, for the same reason of the structure features, physical performance, and parameters of the selected printer camera self-contained in mobile phone, the statistical characteristics of the captured pending printed image are obviously different from those of the corresponding electronic embedded image, which can further help to defense against statistics attack. In Fig. 4(c), (g), and (k), brownish red lines and blue ones denote the gray histograms of a captured pending printed image and the corresponding electronic embedded image, respectively. In Fig. 4(c), (g), and (k), the gray histogram of a captured pending printed image is almost different from that of the corresponding electronic embedded image. Fourth, the hidden secret image can be easily detected by FBS from a captured pending printed image. In (16) and (17), no matter how small any hidden secret information is, it always subtle changes the gray level of $B(x, y)$. That is, $B^*(x, y)$ adds nuance to $B(x, y)$, which results in local minimums or maximums in a neighborhood of a variational function $V(x, y)$ in Fig. 4(b), (f), and (j). Further, in Fig. 4(c), (g), and (k), the



(a) (b) (c) (d)

(e) (f) (g) (h)

(i) (j) (k) (l)

Fig. 4. Performance of FBS for printed matter. (a) Fig. 3(c). (b) Captured image of (a). (c) Gray histogram of both (a) and (b). (d) Detected image from (b). (e) Fig. 3(g). (f) Captured image of (e). (g) Gray histogram of both (e) and (f). (h) Detected image from (f). (i) Fig. 3(k). (j) Captured image of (i). (k) Gray histogram of both (i) and (j). (l) Detected image from (j).

gray histogram of a captured pending printed image is almost different from that of the corresponding electronic embedded image, but the relative variation of the gray level between a hidden secret image and the neighborhood around its hiding location in the corresponding original carrier image are nearly remain unchanged. Therefore, in Fig. 4(d), (h), and (l), although the background textures of original carrier images are complex and fractal, the detected hidden secret images of three clerical scripts of Chinese, i.e., Pu, Yi, and Fei, produced by FBS are relatively very distinct. Fifth, (21)–(24) indicate that FBS is essentially a fractional-order ant colony algorithm. Since the Q_a initial feasible solutions, $\chi_m(0)$, are generated randomly according to (19), it cannot guarantee every ant can convergent to local minimum value of $V(x, y)$ just on the hiding location of a hidden secret image. Therefore, in Fig. 4(d), (h), and (l), except for the hidden secret images, there are some extra needless green points on the corresponding detected hidden secret images achieved by FBS.

Moreover, with the objective of performing a quantitative analysis, the corresponding computational time in terms of CPU time required for processing Fig. 4(b), (f), and (j) implemented by FBS are computed as 0.4635, 0.4722, and 0.45829 s, respectively, in a MATLAB R2009 a environment, with 3.00 GB RAM, and Intel Core i5 CPU 2.40 GHz. The time-consuming computation of FBS is a relatively smaller. Further, Table II presents a comparative evaluation of the performance indices between the electronic embedded image and the corresponding captured pending printed image under consideration.

TABLE II
PERFORMANCE INDICES BETWEEN ELECTRONIC EMBEDDED IMAGE AND CORRESPONDING CAPTURED PENDING PRINTED IMAGE UNDER CONSIDERATION

Performance Indices / *Figures*	*Information Entropy*	*Contrast*	*DIIVINE*
Fig. 3(*a*)	0.0000	0.6537	0.9857
Fig. 3(*b*)	0.0000	0.2947	0.8241
Fig. 3(*e*)	0.0000	0.8717	0.9832
Fig. 3(*f*)	0.0000	0.5539	0.8026
Fig. 3(*i*)	0.0000	0.7809	0.9910
*Fig.*3(*j*)	0.0000	0.5061	0.8265

From Table II, it can be observed that at first, there is inevitably some degree of chromatic aberration, noise jamming, and distortion of the captured pending printed image compared with the corresponding electronic embedded image. The DIIVINE value of the electronic embedded image is larger than that of the corresponding captured pending printed image. Second, the contrast values of the captured pending printed images are smaller than those of corresponding electronic embedded images, those result in their gray histograms left shift in Fig. 4(c), (g), and (k). In addition, the SSIM indices between Fig. 3(a) and (b), Fig. 3(e) and (f), and Fig. 3(i) and (j) are 0.9825, 0.9864, and 0.98748, respectively. This indicates that the high-frequency edges, textural details, and SSIM of the electronic embedded image are mostly preserved. From aforementioned quantitative analysis, it can observed that even

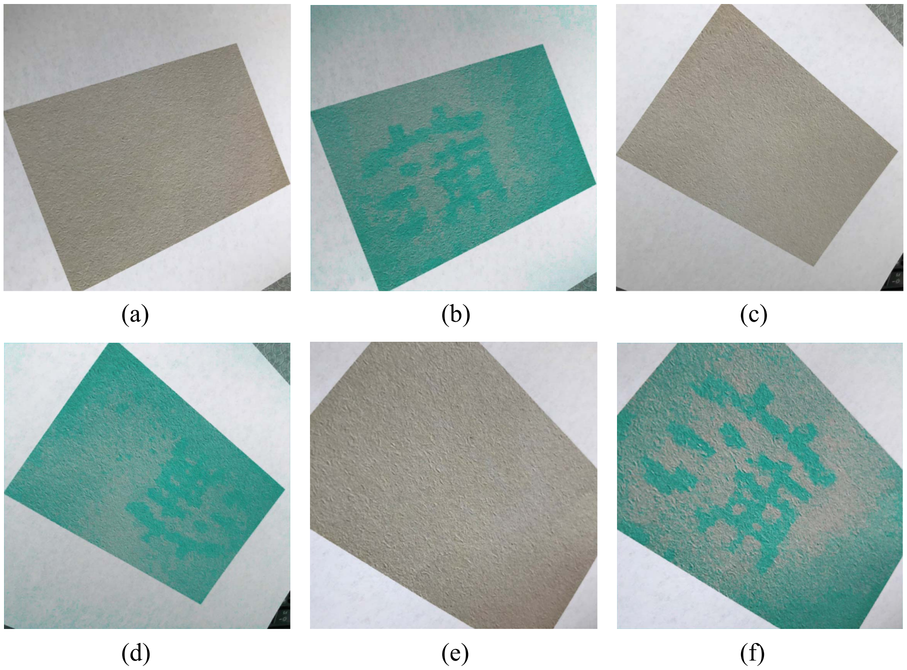


Fig. 5. Capability of FBS to defense against rotation and distortion attack. (a) Captured image1. (b) Detection from (a). (c) Captured image2. (d) Detection from (c). (e) Captured image3. (f) Detection from (e).

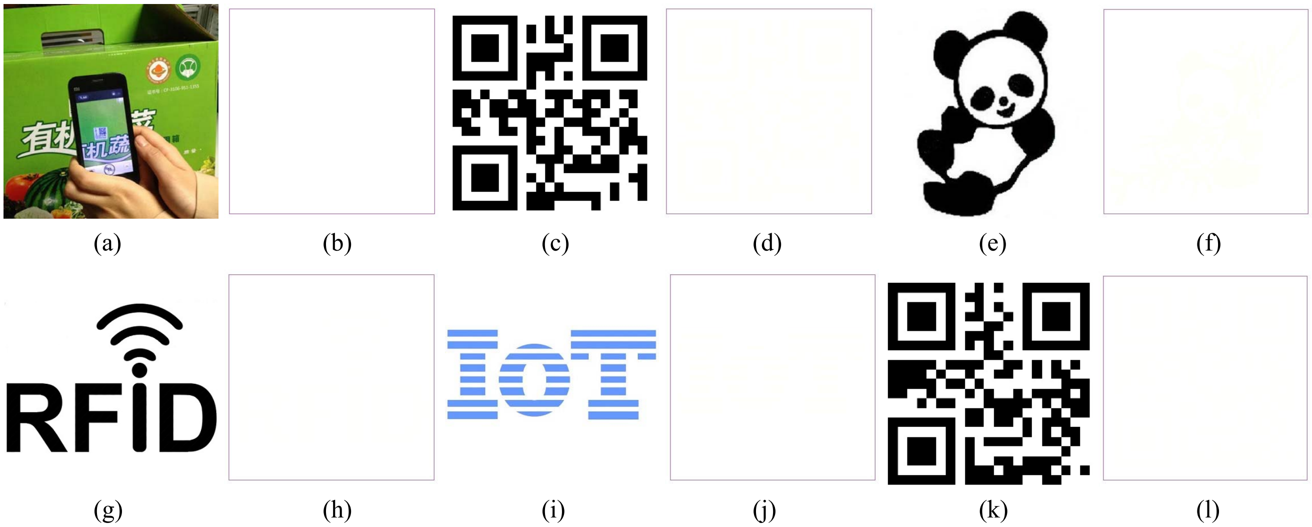


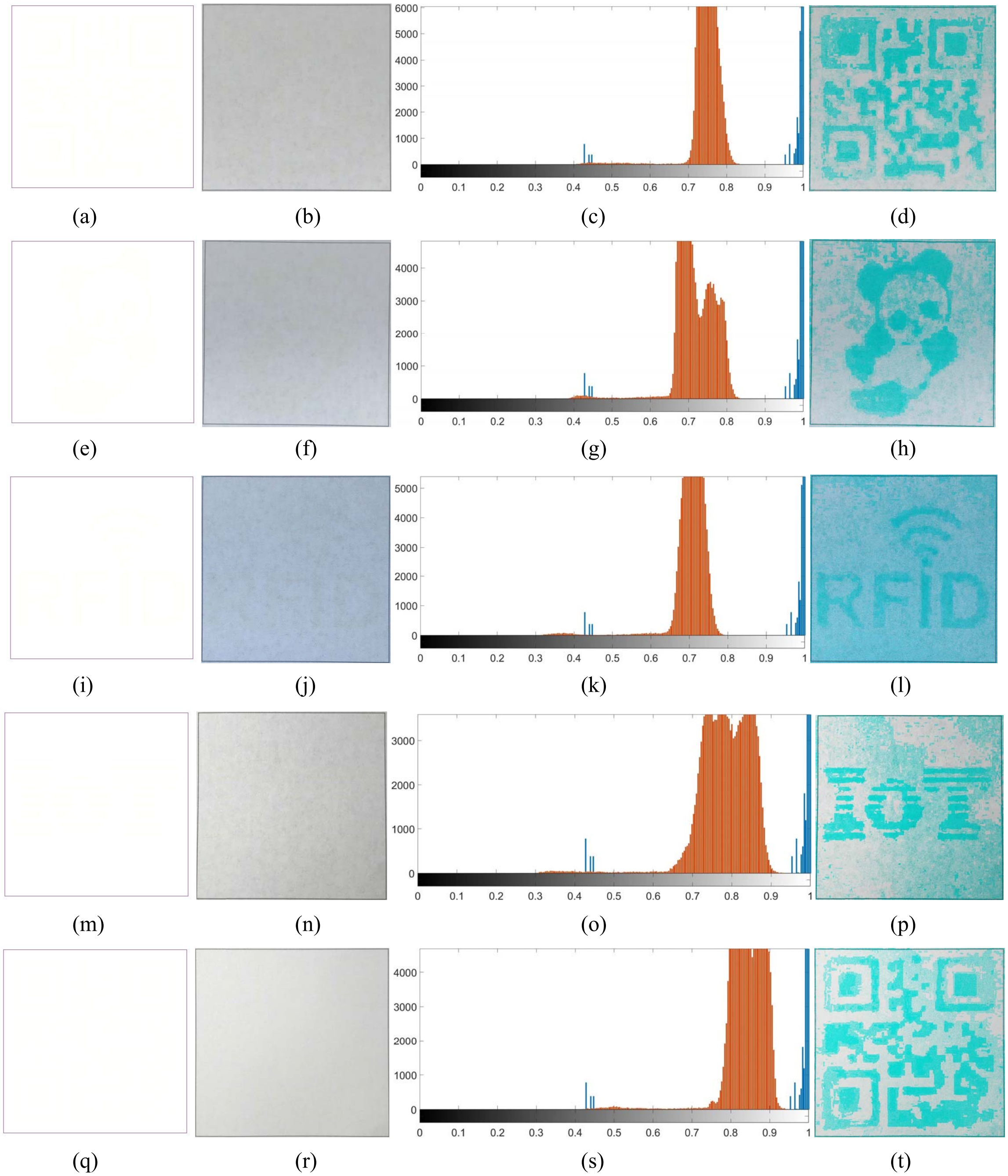
Fig. 6. Performance of FSS for pure white carrier image. (a) Real application scenario. (b) Original pure white carrier image. (c) First 2-D code. (d) (b) embedded with (c). (e) Panda. (f) (b) embedded with (e). (g) Symbol of RFID. (h) (b) embedded with (g). (i) Symbol of IoT. (j) (b) embedded with (i). (k) Second 2-D code. (l) (b) embedded with (k).

if the statistical properties of the original carrier image and the corresponding electronic embedded image are prior stole, the statistical properties of the corresponding captured pending printed image still cannot be considered. The random chromatic aberration, noise jamming, and distortion of the captured pending printed image compared with the corresponding electronic embedded image can further help to defense against statistics attack.

Example 3: To illustrate the capability of defending against rotation and distortion attack, without loss of generality, a printed matter of Fig. 4(a) in Example 2 is selected to evaluate performance of FBS for printed matter in IoT, which is shown in Fig. 5.

In Example 3, the ambient light illumination is also equal to 100–550 Lux. Fig. 5(a), (c), and (e) are the different captured pending printed images corresponding to Fig. 4(a), respectively. Fig. 5(b), (d), and (f) are the detection produced by FBS from (a) from Fig. 5(a), (c), and (e), respectively.

Fig. 5 indicates that no matter what the rotation angle is implemented and how much the distortion of captured pending printed image is achieved, it cannot eliminate local minimums or maximums in a neighborhood of a variational



(a) (b) (c) (d)

(e) (f) (g) (h)

(i) (j) (k) (l)

(m) (n) (o) (p)

(q) (r) (s) (t)

Fig. 7. Performance of FBS for pure white image. (a) Fig. 6(d). (b) Captured image of (a). (c) Gray histogram of both (a) and (b). (d) Detected image from (b). (e) Fig. 6(f). (f) Captured image of (e). (g) Gray histogram of both (e) and (f). (h) Detected image from (f). (i) Fig. 6(h). (j) Captured image of (i). (k) Gray histogram of both (i) and (j). (l) Detected image from (j). (m) Fig. 6(j). (n) Captured image of (m). (o) Gray histogram of both (m) and (n). (p) Detected image from (n). (q) Fig. 6(l). (r) Captured image of (q). (s) Gray histogram of both (q) and (r). (t) Detected image from (r).

function $V(x, y)$, which can be efficiently detected by FBS. In Fig. 5(b), (d), and (f), although the rotation angle is relative larger and the distortion is relative heavier, the detected hidden secret images of three clerical script of Chinese, i.e., Pu, implemented by FBS are relatively very distinct. From Fig. 5, it can be seen that the proposed FBS has the efficient capability of defending against rotation and distortion attack.

Example 4: To extend our analysis of performance of FSS for printed matter in IoT, this paper presents five extreme examples whose original carrier images are pure white image, i.e., the gray levels of all pixels of their original carrier images are equal to 255. In particular, without loss of generality, in (17), this paper sets the hiding intensity coefficient $\lambda = 0.0875$. The resolutions of an original carrier image $S(x, y)$ and a corresponding hidden secret image are equal to 418×418 and 376×376, respectively. The relative initial position of the hiding location of the original carrier region is at $(20, 20)$. Then, the results of the performance of FSS for printed matter in IoT are shown in Fig. 6.

Fig. 6(a) is the real application scenario of the anti-counterfeiting for product external packing in IoT. Fig. 6(c), (e), (g), (i), and (k) are five different hidden secret

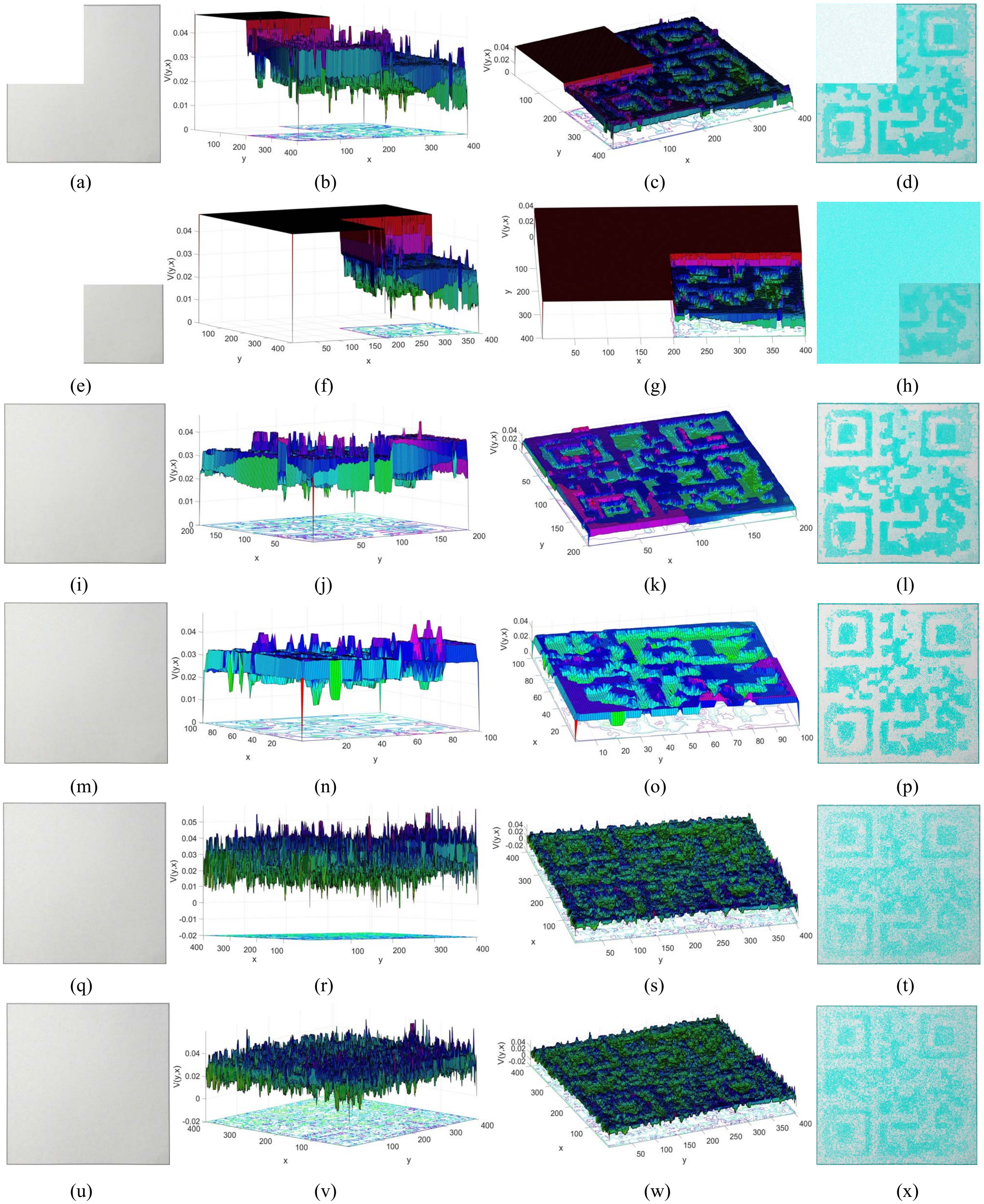


Fig. 8. Capability of FBS to defense against cropping attack, scaling attack, and noise attack. (a) Cut a quarter of Fig. 7(r). (b) Lateral view of (a). (c) Overlook of (a). (d) Detected image from (a). (e) Cut three quarters of Fig. 7(r). (f) Lateral view of (e). (g) Overlook of (e). (h) Detected image from (e). (i) Fifty percent scale drawing of Fig. 7(r). (j) Lateral view of (i). (k) Overlook of (i). (l) Detected image from (i). (m) Twenty-five percent scale drawing of Fig. 7(r). (n) Lateral view of (m). (o) Overlook of (m). (p) Detected image from (m). (q) Adds Gaussian white noise with mean 0 and variance 0.003 to Fig. 7(r). (r) Lateral view of (q). (s) Overlook of (q). (t) Detected image from (q). (u) Adds salt and pepper noise with noise density 0.01 to Fig. 7(r). (v) Lateral view of (u). (w) Overlook of (u). (x) Detected image from (u).

images. Fig. 6(d), (f), (h), (j), and (l) are the embedded images implemented by FSS from [Fig. 6(b) and (c)], [Fig. 6(b) and (e)], [Fig. 6(b) and (g)], [Fig. 6(b) and (i)], and [Fig. 6(b) and (k)], respectively.

In Fig. 6(d), (f), (h), (j), and (l), it can be seen that even though the original carrier images are pure white images, the hidden secret images embedded by FSS in the corresponding carrier images are hardly perceptible.

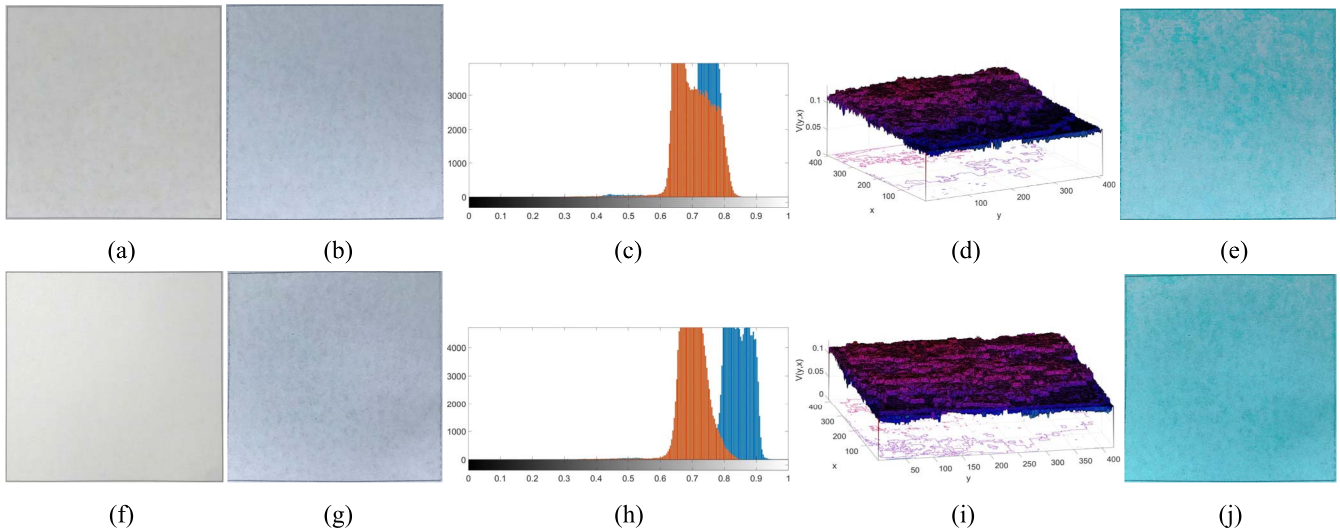


Fig. 9. Capability of FBS to defense against color copy attack. (a) Fig. 7(b). (b) Color copy of (a). (c) Gray histogram of both (a) and (b). (d) 3-D shaded surface of gray level of (b). (e) Detection produced by FBS from (b). (f) Fig. 7(r). (g) Color copy of (f). (h) Gray histogram of both (f) and (g). (i) 3-D shaded surface of gray level of (g). (j) Detection produced by FBS from (g).

The proposed FSS has an excellent information hiding ability.

Example 5: To extend our analysis of performance of FBS for printed matter in IoT, with identical parameter values in Example 2, this paper additionally performs experimental comparisons by using five captured pending printed image corresponding to Fig. 6(d), (f), (h), (j), and (l), which can be shown in Fig. 7.

In Example 5, the ambient light illumination is also equal to 100–550 Lux. Fig. 7(b), (f), (j), (n), and (r) are the captured pending printed image corresponding to Fig. 7(a), (e), (i), (m), and (q), respectively. Fig. 7(d), (h), (l), (p), and (t) are the detected hidden secret image produced by FBS from Fig. 7(b), (f), (j), (n), and (r), respectively.

From Fig. 7(b), (f), (j), (n), and (r), it can be seen that even though the original carrier images are pure white images, the hidden secret images embedded in the corresponding captured pending printed image are nearly invisible. There is some extent of slight chromatic aberration between Fig. 7(a), (e), (i), (m), and (q) and Fig. 7(b), (f), (j), (n), and (r), respectively. Moreover, in Fig. 7(c), (g), (k), (o), and (s) brownish red lines and blue ones denote the gray histograms of a captured pending printed image and the corresponding electronic embedded image, respectively. In Fig. 7(c), (g), (k), (o), and (s), the gray histogram of a captured pending printed image is almost different from that of the corresponding electronic embedded image. In addition, Fig. 7(d), (h), (l), (p), and (t) show that the hidden secret image can be easily detected by FBS from a captured pending printed image.

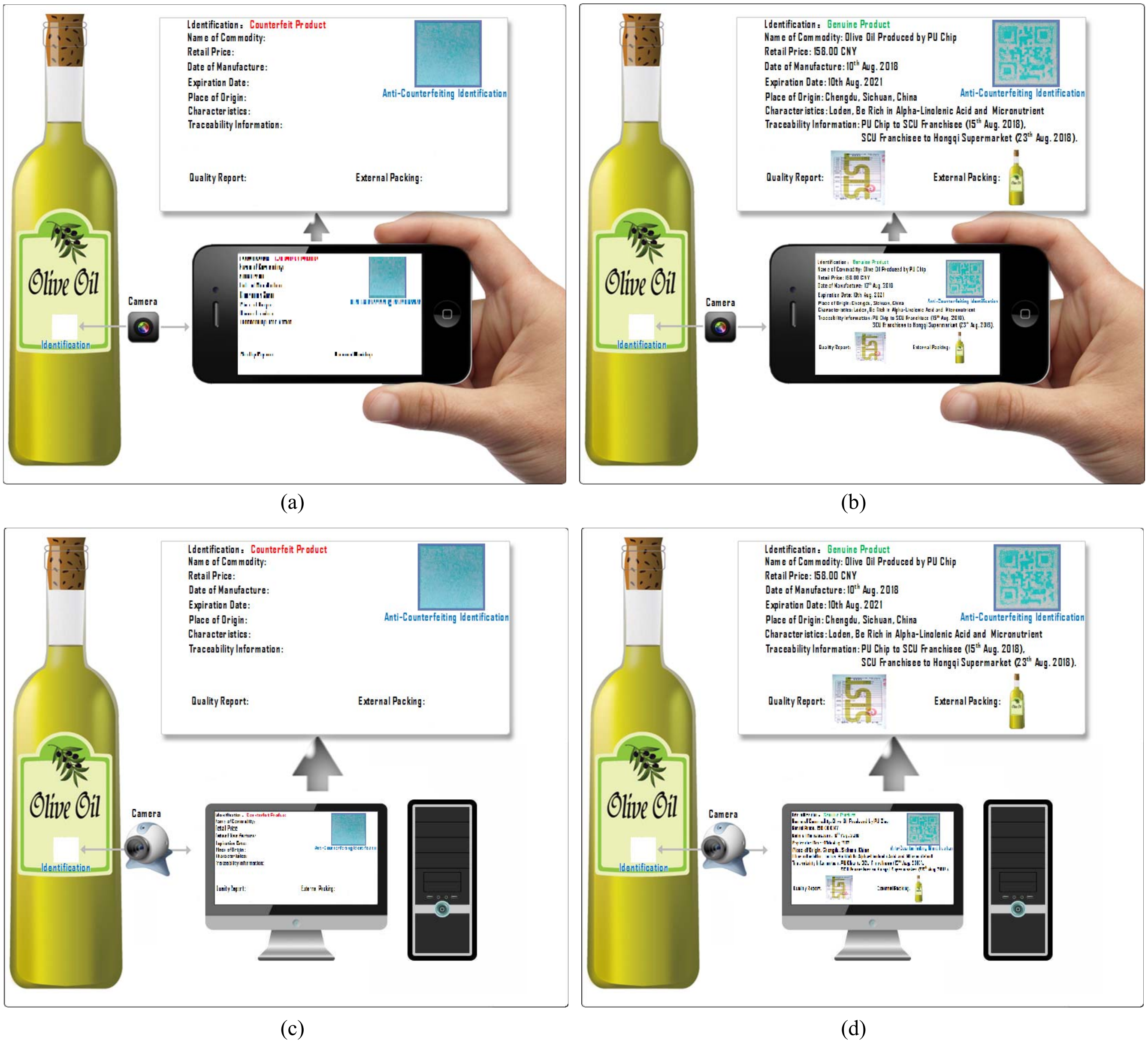
Example 6: To further illustrate the capability of defending against cropping attack, scaling attack, and noise attack, without loss of generality, a printed matter of Fig. 7(q) in Example 5 is selected to evaluate performance of FBS for printed matter in IoT, which is shown in Fig. 8.

In Example 6, the ambient light illumination is also equal to 100–550 Lux. Fig. 8(b), (f), (j), (n), (r), and (v) are the lateral views of the 3-D shaded surface of the gray level of Fig. 8(a), (e), (i), (m), (q), and (u), respectively. Fig. 8(c), (g), (k), (o), (s), and (w) are the overlook of the 3-D shaded surface of the gray level of Fig. 8(a), (e), (i), (m), (q), and (u), respectively. Fig. 8(d), (h), (l), (p), (t), and (x) are the detected hidden secret image produced by FBS from Fig. 8(a), (e), (i), (m), (q), and (u), respectively.

Fig. 8(c), (g), (k), (o), (s), and (w) show that after cropping attack, scaling attack, and noise attack, the local minimums or maximums in a neighborhood of a variational function $V(x, y)$ are still preserved, which can be efficiently detected by FBS. Fig. 8(d), (h), (l), (p), (t), and (x) show that no matter how much the cropping percentage of the captured pending printed image is, how much the scaling ratio of the captured pending printed image is, and what type the adding noise to the captured pending printed image is, the hidden secret image of the 2-D code shown in Fig. 6(k) can be efficiently detected by FBS. The proposed FBS has the efficient capability of defending against cropping attack, scaling attack, and noise attack.

Example 7: To further illustrate the capability of defending against color copy attack, without loss of generality, two printed matters of Fig. 7(a) and (q) in Example 5 is employed to evaluate performance of FBS for printed matter in IoT, which is shown in Fig. 9.

There are heavy chromatic aberrations between Fig. 9(a) and (b) and Fig. 9(f) and (g), respectively. In Fig. 9(c) and (h), brownish red lines and blue ones denote the gray histograms of a color copy of printed image and the corresponding captured pending printed image, respectively. In Fig. 7(c) and (h), the gray histogram of a color copy of printed image is almost different from that of the corresponding captured pending printed image. In addition, from aforementioned discussion, it can be seen that the visual sensitivity to blue light is much lower than



Ldentification: Counterfeit Product
Name of Commodity:
Retail Price:
Date of Manufacture:
Expiration Date:
Place of Origin:
Characteristics:
Traceability Information:
Anti-Counterfeiting Identification
Quality Report: External Packing:

(a)

Ldentification: Genuine Product
Name of Commodity: Olive Oil Produced by PU Chip
Retail Price: 158.00 CNY
Date of Manufacture: 10th Aug. 2018
Expiration Date: 10th Aug. 2021
Place of Origin: Chengdu, Sichuan, China
Characteristics: Loden, Be Rich in Alpha-Linolenic Acid and Micronutrient
Traceability Information: PU Chip to SCU Franchisee (15th Aug. 2018),
SCU Franchisee to Hongqi Supermarket (23th Aug. 2018).
Anti-Counterfeiting Identification
Quality Report: External Packing:

(b)

(c)

(d)

Fig. 10. Effective security traceability platform with anti-counterfeiting capability for commodities. (a) Counterfeit product detected by mobile phone. (b) Genuine product detected by mobile phone. (c) Counterfeit product detected by desk computer. (d) Genuine product detected by desk computer.

those to green light and red light, and opposite opponent colors are never perceived together. There is no yellowish blue. Then, slight changes of B value in the RGB color space of an original carrier image are hardly perceptible to copying machine. In Fig. 9(d) and (i), after color copy attack, the local minimums or maximums in a neighborhood of a variational function $V(x, y)$ cannot be preserved. Therefore, in Fig. 9(e) and (j), there is not any information of the hidden secret image of 2-D code can detected by FBS. The proposed FBS has the efficient capability of defending against color copy attack.

V. Conclusion

Traditional digital steganography is not printable. Within the limits of our knowledge, until now, there are not a well-established steganography and a corresponding steganalysis for printed matter in IoT, which should receive desired attention. The application of fractional calculus to the steganography and steganalysis for printed matter in IoT is an emerging field of research that has seldom received desired attention. The properties of the fractional calculus of a signal are quite different from those of its integer-order calculus. Fractional calculus has been applied to image processing mainly because of its inherent strength in terms of long-term memory, nonlocality, and weak singularity. The fractional differential can nonlinearly maintain the low-frequency contour features in smooth areas of an image, and nonlinearly enhance the high-frequency edges and textural details in those areas in which frequent and less obvious changes in the gray level occur. Therefore, to overcome the aforementioned technical limitation of traditional digital steganography, this paper introduces a novel conceptual formulation of an FSS and an FBS for printed matter. The efficient capability of hiding secret information of FSS and that of detecting secret information of FBS are two important advantages that lead to the superiority of the proposed approach for defending against statistics attack, rotation and distortion attack, cropping attack, scaling attack, noise attack, and color copy attack. The main contribution of this paper is the first preliminary attempt of a feasible achievement of a spatial steganography and a blind steganalysis for printed matter.

Note that IoT-specific application scenarios of FSS and FBS for printed matter are extensive, such as the anti-counterfeiting and tamper detection for the product external packing of commodities, paper documents, paper currencies, paper cheques, calligraphies, paintings, signatures, and so on. In addition, FSS and FBS can even be used to perform the spy work for data security comprising data authenticity, data confidentiality, and data integrity. For example, for retail business and logistics service, the malicious attackers achieve to counterfeit commodities through duplicating the certification labels on the product external packing, which brings forth many potential challenges specifically in the field of the true or false identification during commodity transfer phases in IoT. However, these fakes are hard to be identified directly by the traditional digital steganography, digital steganalysis, intelligent algorithms, and image processing algorithms. For this reason, security traceability system with anti-counterfeiting capability in IoT is a great concern in critical infrastructures, such as the smart home, smart city, smart healthcare, smart industry, etc. Propelled by the ongoing progresses in wireless technology, in IoT, an effective security traceability platform for commodities can be implemented with anti-counterfeiting capability by employing mobile device, desk computer, FSS, and FBS, as illustrated in Fig. 10.

In Fig. 10, a large amount of traceability information on commodities can be produced and communicated by the mobile phone and desk computer in IoT. In this IoT environment, because mobile phone and desk computer serve as a gateway for traceability services, their counterfeit detection capability plays a crucial role. To prevent the aforementioned counterfeiting attacks, FSS is applied to achieve the certification label on the product external packing of an olive oil bottle, while FBS is applied to program an anti-counterfeiting detector installed in the operating system of a mobile phone or a desk computer. Therefore, as shown in Fig. 10(a) and (c), if the hidden information produced by FSS cannot be detected by a mobile phone or a desk computer, end users will be warned that the pending verification manufacture is a counterfeit product. On the contrary, as shown in Fig. 10(b) and (d), proposed the hidden information embedded by FSS can be extracted, the detecting merchandise will be informed as a genuine product. Whereafter, a mobile phone or a desk computer will communicate with servers in IoT, and feedback the corresponding traceability information of this detecting commodity.

The aforementioned discussion has also highlighted additional problems that need to be further studied. For example, at first, further research is required to accelerate the computation of FBS that is closely related to the computational strength and potential of mobile device. As aforementioned discussion, FBS is essentially a fractional-order ant colony algorithm. Thus, the numerical implementation of an FBS is achieving multimodal function optimization in iterative algorithm, which is time-consuming. Furthermore, benchmark tests for desk computer and notebook computer are readily available, but there are a few benchmarks available for the processor of mobile device, which makes the fundamental understanding of the computational limitation of the graphics processing unit of mobile device to be insufficient. Second, the aforementioned 2-D FSS and FBS could be extended be the 3-D ones, which could be applied the anti-counterfeiting of the 3-D-printed objects. In a similar way to the 2-D FSS, to better achieve the imperceptibility of the hidden secret information, the 3-D one could utilize both the self-similar complex textures in a 3-D neighborhood and the opponent channel of blue versus yellow to implement the added material (plastics and metal alloys) corresponding to successive cross-sections of a 3-D model. 3-D printing does not only remove many of the constraints imposed by traditional manufacturing processes but also employ the extra-dimensional information entropy, which enhance the anti-attack capability and robustness of FSS. The authors wish to focus their future scope of research work in these directions.

References

[1] J. Fridrich, M. Goljan, and D. Soukal, "Searching for the Stego-key," in *Proc. SPIE Security Steganography Watermarking Multimedia Contents VI*, vol. 5306, 2004, pp. 70–82.

[2] T.-Y. Liu and W.-H. Tsai, "A new steganographic method for data hiding in microsoft word documents by a change tracking technique," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 1, pp. 24–30, Mar. 2007.

[3] C. G. Girling, "Covert channels in LAN's," *IEEE Trans. Softw. Eng.*, vol. SE-13, no. 2, pp. 292–296, Feb. 1987.

[4] M. Wolf, "Covert channels in LAN protocols," in *Proc. Workshop LANSEC Eur. Inst. System Security*, Karlsruhe, Germany, Apr. 1989, pp. 89–101.

[5] K. Ahsan and D. Kundur, "Practical data hiding in TCP/IP," in *Proc. Workshop Multimedia Security ACM Multimedia*, Karlsruhe, Germany, Apr. 2002, pp. 89–101.

[6] W. Mazurczyk and K. Szczypiorski, "Steganography of VoIP streams," in *Proc. OTM Confederated Int. Conf. Move Meaningful Internet Syst.*, Monterrey, Mexico, Nov. 2008, pp. 1001–1018.

[7] S. Wendzel and J. Keller, "Low-attention forwarding for mobile network covert channels," in *Proc. 12th Joint IFIP TC6 TC11 Conf. Commun. Multimedia Security*, Ghent, Belgium, Oct. 2011, pp. 122–133.

[8] W. Mazurczyk, S. Wendzel, S. Zander, A. Houmansadr, and K. Szczypiorski, *Information Hiding in Communication Networks: Fundamentals, Mechanisms, and Applications*. Hoboken, NJ, USA: Wiley, 2016.

[9] B. R. R. Shetty, J. Rohith, V. Mukund, H. Rohan, and R. Shanta, "Steganography using sudoku puzzle," in *Proc. Int. Conf. Adv. Recent Technol. Commun. Comput.*, Kottayam, India, Oct. 2009, pp. 27–28.

[10] S. Wendzel, W. Mazurczyk, and G. Haas, "Steganography for cyber-physical systems," *J. Cyber Security Mobility*, vol. 6, no. 2, pp. 105–126, 2017.

[11] N. Tuptuk and S. Hailes, "Steganography for cyber-physical systems," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun.*, May 2015, pp. 236–242.

[12] R. Das and P. Chatterjee, "Securing data transfer in IoT employing an integrated approach of cryptography & steganography," in *Proc. Int. Conf. High Perform. Compilation Comput. Commun.*, Kuala Lumpur, Malaysia, Mar. 2017, pp. 17–22.

[13] F. Djebbar and N. Abu-Ali, "Lightweight noise resilient steganography scheme for Internet of Things," in *Proc. IEEE Glob. Commun. Conf.*, Singapore, Dec. 2017, pp. 1–6.

[14] A. K. Bairagi, R. Khondoker, and R. Islam, "An Efficient steganographic approach for protecting communication in the Internet of Things IoT critical infrastructures," *Inf. Syst. Security*, vol. 25, nos. 4–6, pp. 197–212, 2016.

[15] S. R. Kim, J. N. Kim, S. T. Kim, S. Shin, and J. H. Yi, "Anti-reversible dynamic tamper detection scheme using distributed image steganography for IoT applications," *J. Supercomput.*, vol. 74, no. 9, pp. 4261–4280, 2018.

[16] M. Elhoseny *et al.*, "Secure medical data transmission model for IoT-based healthcare systems," *IEEE Access*, vol. 6, pp. 20596–20608, 2018.

[17] A. Soni, J. Jain, and R. Roshan, "Image steganography using discrete fractional Fourier transform," in *Proc. Int. Conf. Intell. Syst. Signal Process.*, Gujarat, India, Mar. 2013, pp. 97–100.

[18] C. Y. Roy and M. K. Goel, "Review on image steganography," *Indian J. Sci. Technol.*, vol. 9, no. 47, pp. 1–5, 2016, doi: 10.17485/ijst/2016/v9i47/106446.

[19] F. Bacon, *The Proficience and Advancement of Learning Divine and Humane*. Oxford, U.K.: Oxford Univ. Press, 1605.

[20] V. Chu. (2009). *ASCII Art Steganography*. [Online]. Available: http://www.vincentchu.com/asciiartsteganography.html

[21] K. B. Oldham and J. Spanier, *The Fractional Calculus: Integrations and Differentiations of Arbitrary Order*. New York, NY, USA: Academic, 1974.

[22] N. Özdemir and D. Karadeniz, "Fractional diffusion-wave problem in cylindrical coordinates," *Phys. Lett. A*, vol. 372, no. 38, pp. 5968–5972, 2008.

[23] Y. Povstenko, "Solutions to the fractional diffusion-wave equation in A wedge," *Fractional Calculus Appl. Anal.*, vol. 17, no. 1, pp. 122–135, 2014.

[24] R. C. Koeller, "Applications of the fractional calculus to the theory of viscoelasticity," *J. Appl. Mech.*, vol. 51, no. 2, pp. 294–298, 1984.

[25] Y. A. Rossikhin and M. V. Shitikova, "Applications of fractional calculus to dynamic problems of linear and nonlinear hereditary mechanics of solids," *Appl. Mech. Rev.*, vol. 50, no. 1, pp. 15–67, 1997.

[26] S. Manabe, "A suggestion of fractional-order controller for flexible spacecraft attitude control," *Nonlin. Dyn.*, vol. 29, nos. 1–4, pp. 251–268, 2002.

[27] I. Podlubny, I. Petráš, B. M. Vinagre, P. O'Leary, and L. Dorčák, "Analogue realizations of fractional-order controllers," *Nonlin. Dyn.*, vol. 29, nos. 1–4, pp. 281–296, 2002.

[28] Y. F. Pu, "Measurement units and physical dimensions of fractance-part I: Position of purely ideal fractor in Chua's axiomatic circuit element system and fractional-order reactance of fractor in its natural implementation," *IEEE Access*, vol. 4, pp. 3379–3397, 2016.

[29] Y.-F. Pu, "Measurement units and physical dimensions of fractance-part II: Fractional-order measurement units and physical dimensions of fractance and rules for fractors in series and parallel," *IEEE Access*, vol. 4, pp. 3398–3416, 2016.

[30] T. J. Freeborn, "A survey of fractional-order circuit models for biology and biomedicine," *IEEE Trans. Emerg. Sel. Topics Circuits Syst.*, vol. 3, no. 3, pp. 416–424, Sep. 2013.

[31] Y.-F. Pu and X. Yuan, "Fracmemristor: Fractional-order memristor," *IEEE Access*, vol. 4, pp. 1872–1888, 2016.

[32] Y.-F. Pu, X. Yuan, and B. Yu, "Analog circuit implementation of fractional-order memristor: Arbitrary-order lattice scaling fracmemristor," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 65, no. 9, pp. 2903–2916, Sep. 2018.

[33] Y. F. Pu, W. X. Wang, J. L. Zhou, Y. Y. Wang, and H. D. Jia, "Fractional differential approach to detecting textural features of digital image and its fractional differential filter implementation," *Sci. China F Inf. Sci.*, vol. 51, no. 9, pp. 1319–1339, 2008.

[34] Y. F. Pu *et al.*, "Fractional partial differential equation denoising models for texture image," *Sci. China Inf. Sci.*, vol. 57, no. 7, pp. 1–19, 2014.

[35] Y.-F. Pu, J.-L. Zhou, and X. Yuan, "Fractional differential mask: A fractional differential-based approach for multiscale texture enhancement," *IEEE Trans. Image Process.*, vol. 19, no. 2, pp. 491–511, Feb. 2010.

[36] Y.-F. Pu *et al.*, "A fractional-order variational framework for retinex: Fractional-order partial differential equation-based formulation for multi-scale nonlocal contrast enhancement with texture preserving," *IEEE Trans. Image Process.*, vol. 27, no. 3, pp. 1214–1229, Mar. 2018.

[37] Y.-F. Pu *et al.*, "Fractional extreme value adaptive training method: Fractional steepest descent approach," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 26, no. 4, pp. 653–662, Apr. 2015.

[38] Y.-F. Pu, Z. Yi, and J.-L. Zhou, "Fractional Hopfield neural networks: Fractional dynamic associative recurrent neural networks," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 28, no. 10, pp. 2319–2333, Oct. 2017.

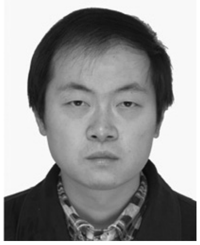
[39] Y. F. Pu, Z. Yi, and J. L. Zhou, "Defense against chip cloning attacks based on fractional Hopfield neural networks," *Int. J. Neural Syst.*, vol. 27, no. 4, 2017, Art. no. 1750003.

[40] T. Young, "Bakerian lecture: On the theory of light and colours," *Philosoph. Trans. Roy. Soc. London*, vol. 92, pp. 12–48, Jan. 1802.

[41] M. Foster, *A Text-book of Physiology*. London, U.K.: Lea Bros. & Co., 1891.

[42] A. K. Moorthy and A. C. Bovik, "Blind image quality assessment: From natural scene statistics to perceptual quality," *IEEE Trans. Image Process.*, vol. 20, no. 12, pp. 3350–3364, Apr. 2011.

[43] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: From error measurement to structural similarity," *IEEE Trans. Image Process.*, vol. 13, no. 4, pp. 600–612, Jan. 2004.

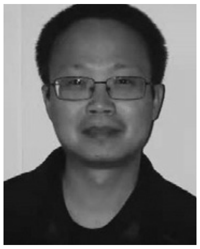


Yi-Fei Pu received the Ph.D. degree from the College of Electronics and Information Engineering, Sichuan University, Chengdu, China, in 2006.

He is a Full Professor and a Doctoral Supervisor with the College of Computer Science, Sichuan University, the Chief Technology Officer of Chengdu PU Chip Science and Technology Company, Ltd., Chengdu, and was elected into the Thousand Talents Program of Sichuan Province and the Academic and Technical Leader of Sichuan Province. He has authored or co-authored as a lead author approximately 20 papers indexed by SCI in journals such as the *International Journal of Neural Systems*, the IEEE TRANSACTIONS ON IMAGE PROCESSING, the IEEE TRANSACTIONS ON NEURAL NETWORKS AND LEARNING SYSTEMS, the IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—I: REGULAR PAPERS, the IEEE INTERNET OF THINGS JOURNAL, the *IEEE Intelligent Transportation Systems Magazine*, IEEE ACCESS, *Mathematic Methods in Applied Sciences*, and *Science in China Series F: Information Sciences*, and *Science China Information Sciences*. He held several research projects, such as with the National Key Research and Development Program Foundation of China, National Nature Science Foundation of China, and Returned Overseas Chinese Scholars Project of the Education Ministry of China, and holds 13 China Inventive Patents as the first or single inventor. His current research interest includes application of fractional calculus and fractional partial differential equation to signal analysis, signal processing, image processing, circuits and systems, and machine intelligence.

Ni Zhang received the Ph.D. degree from the Southwestern University of Finance and Economics, Chengdu, China, in 2012.

She is an Associate Research Librarian of the Library, Sichuan University, Chengdu. She has studied application fractional calculus on signal analysis and processing. She has hosted or has taken part in four research projects. She has authored or co-authored over ten papers, of which five were indexed by SCI, and four were indexed by EI. Her current research interests include application artificial intelligence, especially semantic information retrieve, on law.



Huai Wang received the M.S. degree from the College of Electronics and Information Engineering, Sichuan University, Chengdu, China, in 2004.

He is an Associate Chief Technology Officer with Chengdu PU Chip Science and Technology Company, Ltd., Chengdu. His current research interests include the application of fractional calculus to image processing and signal processing.