EURASIP Journal on Image
and Video Processing

RESEARCH Open Access

Iterative learning control for image feature extraction with multiple-image blends

Yinjun Zhang[1,2], Yinghui Li[1*] and Jianhuan Su[2]

Abstract

In this paper, a novel method of image extraction is proposed. Firstly, the image information is embedded into the parameters of the chaotic system, and then the image is overlapped and embedded to complete the image hiding. This process is equivalent to a dynamic system with unknown time-varying parameters. Secondly, the D-type iterative learning control algorithm is used to extract the information hidden in the image, because iterative learning can be used to estimate the time-varying parameter system completely in the time interval. Finally, the numerical simulation shows that the algorithm can effectively extract the hidden information under various attacks.

Keywords: Iterative learning control, Image extracting, Image hiding

1 Introduction

With the rapid development of Internet technology, it has provided great convenience for the dissemination of digital information products. On the other hand, copyright protection has become increasingly important. Information hiding and digital watermarking as an important method of intellectual property protection have attracted more and more attention.

In machine learning, in pattern recognition, and in image processing, feature extraction starts from an initial set of measured data and builds derived values (features) intended to be informative and non-redundant, facilitating the subsequent learning and generalization steps, and in some cases, leading to better human interpretations. Feature extraction is related to dimensionality reduction.

When the input data to an algorithm is too large to be processed and it is suspected to be redundant (e.g., the same measurement in both feet and meters, or the repetitiveness of images presented as pixels), then it can be transformed into a reduced set of features (also named a feature vector). Determining a subset of the initial features is called feature selection [1]. The selected features are expected to contain the relevant information from the input data, so that the desired task can be performed by using this reduced representation instead of the complete initial data.

Feature extraction involves reducing the amount of resources required to describe a large set of data. When performing analysis of complex data, one of the major problems stems from the number of variables involved. Analysis with a large number of variables generally requires a large amount of memory and computation power; also, it may cause a classification algorithm to over fit to training samples and generalize poorly to new samples. Feature extraction is a general term for methods of constructing combinations of the variables to get around these problems while still describing the data with sufficient accuracy. Many machine learning practitioners believe that properly optimized feature extraction is the key to effective model construction.

One very important area of application is image processing, in which algorithms are used to detect and isolate various desired portions or shapes (features) of a digitized image or video stream. It is particularly important in the area of optical character recognition.

Results can be improved using constructed sets of application-dependent features, typically built by an expert. One such process is called feature engineering. Alternatively, general dimensionality reduction techniques are used such as (1) independent component analysis, (2) Isomap, (3) kernel PCA, (4) latent semantic analysis, (5) partial least squares, (6) principal

* Correspondence: 18107786221@163.com
[1]Aeronautics and Astronautics Engineering Institute, Air Force Engineering University, Xi’an 710038, Shanxi Province, China
Full list of author information is available at the end of the article

component analysis, (7) multifactor dimensionality reduction, (8) nonlinear dimensionality reduction, (9) multilinear principal component analysis, (10) multilinear subspace learning, (11) semidefinite embedding, and (12) autoencoder.

Space technology [2, 3] and transform domain technology [4, 5] are the main methods of digital image hiding and embedding. From the airspace algorithm point of view, the LSB (least significant bits) method is a typical algorithm [6]. The method converts the spatial pixel values of the original carrier image from binary to decimalism and replaces each bit of information in the binary with the least significant bit in the corresponding carrier, and finally, the binary data containing secret information is converted to decimal pixel, in order to regain the secret image. Although the method has good concealment, so that the human eye is difficult to detect, it has poor robustness.

The transform domain method is relatively stable, and the image hidden by the transform domain method has a certain resistance to image compression, filtering, rotation, shearing, and noise. Discrete cosine transform (DCT) [7], discrete Fourier transform (DFT) [8], and discrete wavelet transform (DWT) [9, 10] are the main transform domain methods in recent years. We construct a unified form of the boundary value solving problem by constructing the matching function, and finally, using the conventional spectral method to solve is an important method in the domain of transform domain [10]. In the process of exploring image-hiding algorithms, some scholars have proposed an iterative hybrid image-hiding encryption algorithm [11]. The main idea of the algorithm is to embed an image into another image. The image is repeatedly embedded into a set of image, accordingly to adjust the iteration parameters to achieve the invisibility of the image. The algorithm provides a new way for better selection of the mixing parameters, but it shows weak robustness of the system due to the multiple product amplification of the mixed image change value. Due to the weak robustness caused by the error multi-amplification in [12], Urvoy [13] proposed an iterative hybrid algorithm for image modification that uses a partial image that does not contain a watermark to modify the image containing the watermark. Thus, we can eliminate the error from the image. However, in the face of random attacks such as Gaussian noise, the quality of the watermark we extract is poor. In order to improve

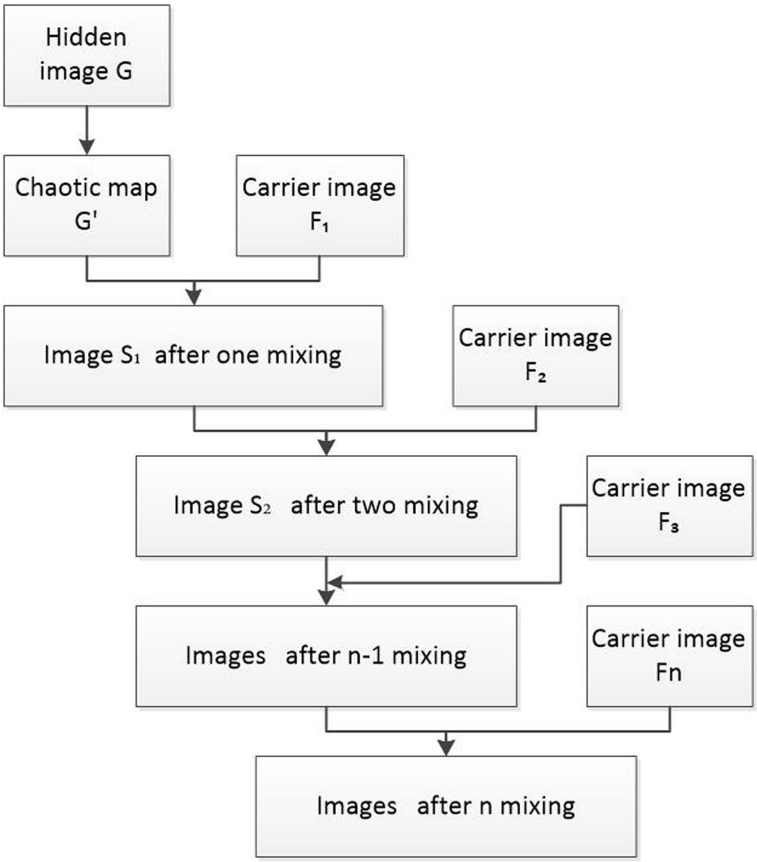

Fig. 1 Image encryption and its embedded process

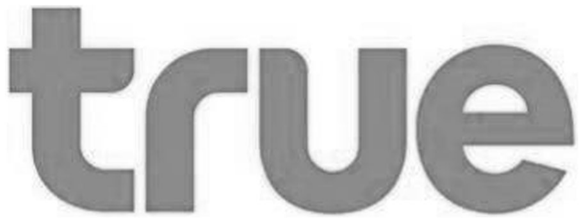

Fig. 2 Hidden image

the stability of the watermarking system, the literature [14, 15] proposed JADE blind separation watermarking algorithm. This method used an iterative hybrid method to embed the image and used the hidden image and the carrier image as different signals. By separating the matrix to determine whether there is hidden information, there is no need to know the exact location of the embedded image. When the two signals that need to be separated have a strong correlation, the method cannot separate the related signals well.

In this paper, we proposed the image extraction method based on iterative learning algorithm, which is applied to the full estimation of time-varying parameters in finite time intervals under certain convergence conditions. For the repeated mixed images, a new image extraction method is proposed in this paper. Iterative learning identification technology is used to reconstruct the image information signals. For the class of chaotic map and iterative hybrid encryption image system, an iterative learning identification law is constructed. Under the conditions of given learning law and initial state of the system, the sufficient conditions for learning gain convergence are deduced, and the convergence of the system is proved. Using iterative learning identification method to estimate the time-varying parameters completely in finite time interval, we can achieve completely reconstruction of image information in digital image watermarking system.

Remarks: Here are some general mathematical symbols used in this paper. $L^2(\Omega)$ (or short in L^2) represents a kind of Ω function space consisted by all measureable functions and it is bounded, satisfying $u_p = \left\{ \int_{\Omega} |u(x)|^p dx \right\}^{1/p} < \infty \ (1 \leq p \leq \infty)$. $L^p(\Omega)$is Banach space, $L^2(\Omega)$ is Hilbert space.

For the n dimensional vector $u = (u_1^T, u_2^T, \cdots, u_i^T)$, where the norm of definition is $\|u\| = \left(\sum_{i=1}^{n} u_i^2 \right)^{1/2}$. If $u_i(x) \in L^2, \ i = 1, \ 2, \ \cdots, \ n$ then $Q(x) = (Q_1(x), Q_2(x), L, Q_n(x)) \in R^n \cap L^2$ and $\|Q\|_{L^2} = \left\{ \int_{\Omega} (Q^T(x)Q(x))^2 dx \right\}^{1/2}$.

For the function $f(x, t) : \Omega \times [0, T] \rightarrow R^n$, $f(gt) \in R^n \cap L^2$, $t \in [0, T]$, define its (L^2, λ) norm as follows $\|f\|_{(L^2,\lambda)} = \sup_{0 \leq t \leq T} \left\{ \left(\|f\|_{L^2}^2 \right) e^{-\lambda t} \right\}$.

2 Digital image encryption

Chaotic cryptology includes two integral opposite parts: chaotic cryptography and chaotic cryptanalysis. Chaotic cryptography is the application of the mathematical chaos theory to the practice of the cryptography, the study or techniques used to privately and securely transmit information with the presence of a third party or adversary. The use of chaos or randomness in cryptography has long been sought after by entities wanting a new way to encrypt messages. However, because of the lack of thorough, provable security properties and low acceptable performance, chaotic cryptography has encountered setbacks [1, 16–18].

In order to use chaos theory efficiently in cryptography, the chaotic maps should be implemented such that the entropy generated by the map can produce required confusion and diffusion. Properties in chaotic systems and cryptographic primitives share unique characteristics that allow for the chaotic systems to be applied to cryptography [19]. If chaotic parameters, as

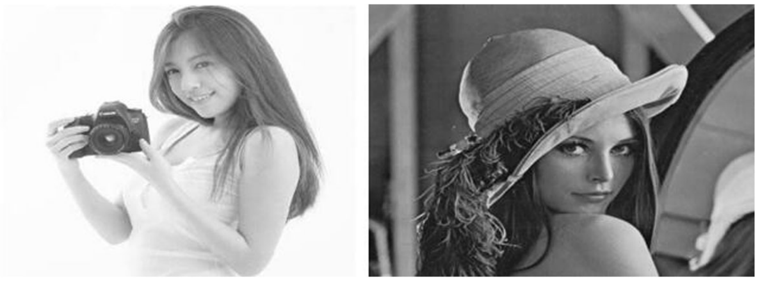

Fig. 3 Carrier image

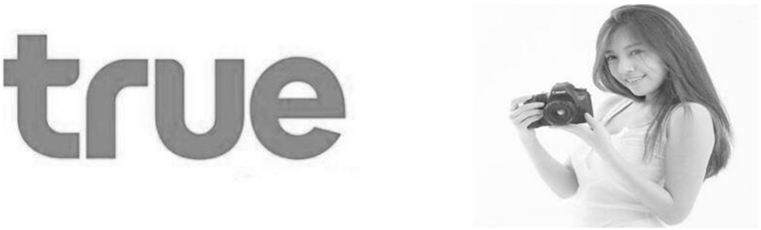

Fig. 4 Embedded carrier image and extracted hidden image

well as cryptographic keys, can be mapped symmetrically or mapped to produce acceptable and functional outputs, it will make it next to impossible for an adversary to find the outputs without any knowledge of the initial values. Since chaotic maps in a real life scenario require a set of numbers that are limited, they may, in fact, have no real purpose in a cryptosystem if the chaotic behavior can be predicted. One of the most important issues for any cryptographic primitive is the security of the system. However, in numerous cases, chaotic-based cryptography algorithms are proved unsecure [17, 20–22]. The main issue in many of the cryptanalyzed algorithms is the inadequacy of the chaotic maps implemented in the system [23, 24].

The concept of chaos cryptography or in the other words chaos-based cryptography can be divided into two major groups: the asymmetric [25, 26] and symmetric [27–29] chaos-based cryptography. The majority of the symmetric chaos-based algorithms are based on the application of discrete chaotic maps in their process [27, 30].

Bourbakis and Alexopoulos [31] in 1991 proposed supposedly the earliest fully intended digital image encryption scheme which was based on SCAN language. Later on, with the emergence of chaos-based cryptography, hundreds of new image encryption algorithms, all with the aim of improving the security of digital images, were proposed [21]. However, there were three main aspects of the design of an image encryption that was usually modified in different algorithms (chaotic map, application of the map, and structure of algorithm). The initial and perhaps the most crucial point was the chaotic map applied in the design of the algorithms [32–36]. The speed of the cryptosystem is always an important parameter in the evaluation of the efficiency of a cryptography algorithm; therefore, the designers were initially interested in using simple chaotic maps such as tent map, and the logistic map [19, 37]. However, in 2006 and 2007, the new image encryption algorithms based on more sophisticated chaotic maps proved that application of chaotic map with higher dimension could improve the quality and security of the cryptosystems [2, 3, 35, 38, 39].

In this paper, we use logistic encryption method to encrypt the digital image. The logistic chaotic map is described as follows:

$$x(t+1) = \mu x(t)(1 - x(t)), x(t) \in (0,1) \quad (1)$$

when $3.5699456\cdots \leq \mu \leq 4$, the unpredictability of the sequence $x(t)$ generated by logistic chaotic maps. If the same initial value is given, a random sequence will be generated, under the mapping of the parameter A. If a different initial value is given, different data sequences will be generated, but the correlation between the data sequences is almost zero. The original image G is marked as $\theta(t)$. In order to achieve the invisibility of the image, we superpose and mix the known image sequence

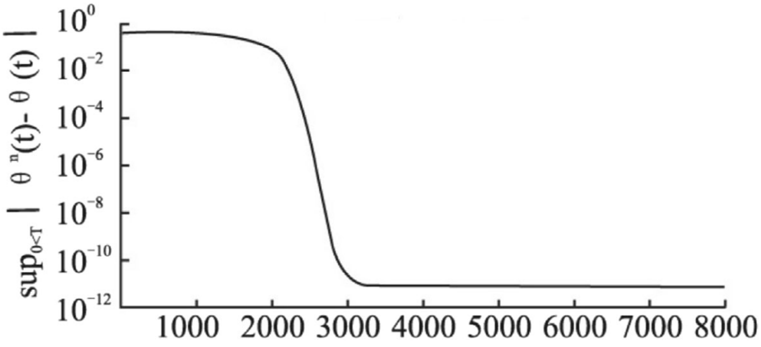

Fig. 5 Iterative output error

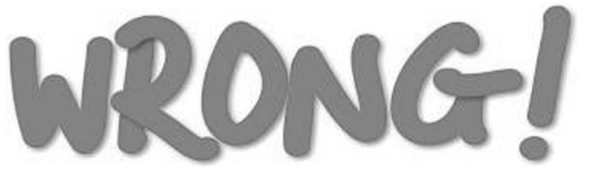

Fig. 6 Hidden image

with the parameter μ, namely μ(t) = λ + θ(t); at the same time, the Eq. (1) can be written as

$$x(t+1) = (\lambda + \theta(t))x(t)(1-x(t)), x(t)\in(0,1) \tag{2}$$

Thus, the chaotic sequence {x(t), t = 1,2,3,...} is the desired encrypted image G′, denoted here as x(t).

3 Method—multiple image blends

Assume that the image F is a pair of M × N digital images, G′ needs to be hidden images, then a superimposed mixed image S can be described as

$$\mathrm{S} = \alpha \mathrm{F} + (1-\alpha)\mathrm{G}' \tag{3}$$

α is adjustable mixing parameter, and F is carrier image. S is an image sequence produced after a superposition. According to Eq. (3), we know the 1 − α tends to 0, when mixing parameter α tends to 1, then the produced image sequence S=F. However, when the adjustable parameter α tends 0, the image sequence of superposition S will tend the hidden image G′. From the Eq. (3), we also know that when the value of the parameter α is closer to 1, the image G′ is hidden as much as possible. It is not easy to be detected, but it also increases the difficulty of the extraction.

Assume that the carrier images $\mathrm{F_i}(i = 1, 2, \cdots, n)$ are different M × N digital images and the mixing parameters are α_i | $\alpha_\mathrm{i} \in [0, 1]$, i = 1, 2, ⋯, n. According to the hybrid algorithm of image, firstly, we mix the image F1, G′, and α_1 to get S1 = α_1F1 + (1 − α_1)S1; secondly, we mix the image F2, G′, and α_2 to get S2 = α_2F2 + (1 − α_2) G′, and so on. Finally, mix the images to get Sn = α_nFn + (1 − α_n)Sn − 1; Sn is called the digital image group which is a mixture of N images.

The mixed image satisfies the following relation:

$$\begin{cases} \mathrm{S}_1(t) = a_1\mathrm{F}_1(t) + (1-a_1)x(t) \\ \mathrm{S}_2(t) = a_2\mathrm{F}_2(t) + (1-a_2)\mathrm{S}_1(t) \\ \vdots \\ \mathrm{S}_n(t) = a_n\mathrm{F}_n(t) + (1-a_n)\mathrm{S}_{n-1}(t) \end{cases} \tag{4}$$

so:

$$\mathrm{S}_n = \alpha_n\mathrm{F}_n + \beta_n\alpha_{n-1}\mathrm{F}_{n-1} + \cdots + \beta_n\beta_{n-1}\cdots\beta_{n-i}\alpha_{n-i}\mathrm{F}_{n-i} + \cdots + \beta_n\beta_{n-1}\cdots\beta_2\beta_1\mathrm{G}'$$

where $\beta_i = 1 - \alpha_\mathrm{i}$, i = 1, 2, ⋯, n. When α_i tends to 1, the better the effect of watermark embedding, the worse the effect of watermark extraction. We use the logistic map to produce these iterative parameters. Selected parameter μ′ and initial value α1.

$$\alpha_{i+1} = \mu'\alpha_i(1-\alpha_i) \tag{5}$$

According to Eq. (5), we can get a chaotic sequence α_i and use α_i as the parameter sequence for each image superposition and mixing. In order to avoid the correlation between the mixed images, the initial value α_1 of the parameter μ′ in Eq. (5) cannot be the same as the parameter μ(t) and the initial value x(0) in Eq. (1).

Image encryption and its embedded process are shown in Fig. 1.

4 The iterative learning control for image hidden with multi-blending

We use the image's multiple hybrids embedding technology to embed image information into the time-varying parameters of the digital image system and establish a mathematical model for the digital image system. The

Fig. 7 Carrier image

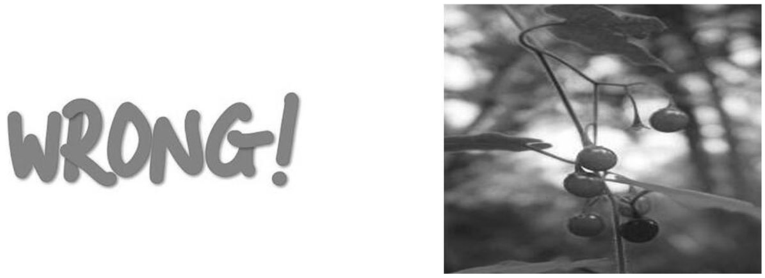

Fig. 8 Embedded carrier image and extracted hidden image

image information is regarded as a finite time, and the iterative learning identification method is applied to the image system. Variable parameters are estimated to achieve complete reproduction of image information.

We mark the initial image G as $\theta(t)$, then the encryption image G' as $x(t)$ sequence. Carrier image group $F_i(i=1,2,\cdots,n)$ is ω_i and the hybrid image S_i is $y(t)$; the system is described as

$$\begin{cases} x(t+1)=f(x(t),\theta(t),t) \\ y^1(t)=h_1(x(t),t) \\ y^2(t)=h_2\left(y^1(t),t\right) \\ \cdots \\ y^n(t)=h_n\left(y^{n-1}(t),t\right) \end{cases} \tag{6}$$

where $t\in\{0,1,2,\cdots,N\}$, $x(t)\in R^n$, $\theta(t)\in R^1$, $y^1(t)\in R^1$, $y(t)\in R^1$ are nonlinear function. $f(x(t),\theta(t),t)$ is the function of initial encryption image. The nonlinear function $h_1(x(t),t)$ represents an iterative mixed function of the encrypted image and carrier image, and $h_n(y^{n-1}(t),t)$ represents the mixed function of n iterations.

The iterative learning control system for estimating $\theta(t)$ is:

$$\begin{cases} x_k(t+1)=f(x_k(t),\theta_k(t),t) \\ y_k^1(t)=h_1(x_k(t),t) \\ y_k^2(t)=h_2\left(y_k^1(t),t\right) \\ \cdots \\ y_k^n(t)=h_n\left(y_k^{n-1}(t),t\right) \end{cases} \tag{7}$$

where k is iterative times and we use the same initial value. We suppose there exist f partial derivative $A_k(t)$, $B_k(t)$ about x, θ, h_1 partial derivative $C_k(t)$ about x and h_i partial derivative $D_{ki}(t)$ about y.

We use the D-type learning law:

$$\begin{cases} \theta_k(t)=\mathrm{sat}(\vartheta_k(t)) \\ \vartheta_{k+1}(t)=\mathrm{sat}(\vartheta_k(t))+L(t)\left[e_k(t+1)-e_k(t)\right] \end{cases} \tag{8}$$

where $\mathrm{sat}(\cdot)$ is the saturation function, $L(t)$ is the learning gain, and $e_k(t)=y^n-y_k^n$.

Theorem 1 *For the system (7) and learning law, if there exist*

$$\left\|1-L(t)\prod\nolimits_{i=2}^{n}D_{ki}(t+1)C_k(t+1)B_k(t)\right\|\le\rho<1 \tag{9}$$

then when $k\to\infty$, $\theta(t)$ converges to $\theta_k(t)$ interval $\{0, 1,\cdots,N\}$.

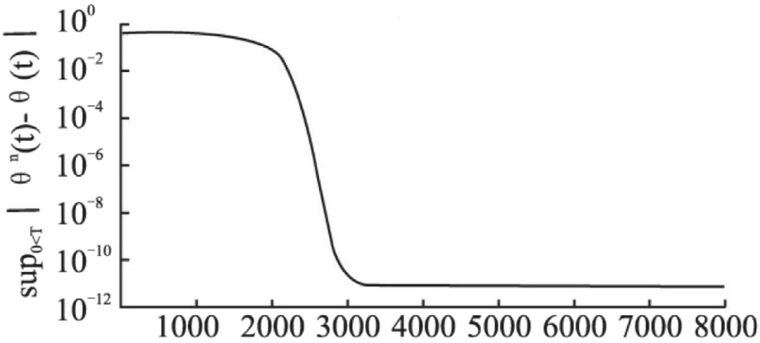

Fig. 9 Iterative output error

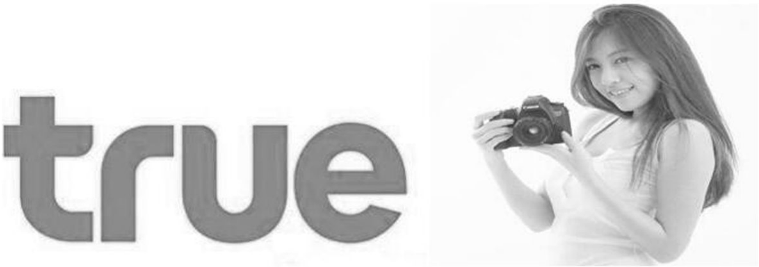

Fig. 10 Attacked with Gaussian noise and extracted hidden image (Example 1)

Proof
Remark $\delta x_k(t) = x_d(t) - x_k(t)$, $\delta\theta_k(t) = \theta_d(t) - \theta_k(t)$

$$\begin{aligned}\delta x_k(t) &= f(x_d(t-1), \theta_d(t-1), t-1) - f(x_k(t-1), \theta_k(t-1), t-1)\\ &\quad + f(x_d(t-1), \theta_k(t-1), t-1) - f(x_d(t-1), \theta_k(t-1), t-1)\end{aligned}$$

According to the differential mean value theorem, we have

$$\begin{aligned}& f(x_d(t-1), \theta_d(t-1), t-1) - f(x_k(t-1), \theta_k(t-1), t-1)\\ &= A_k(t-1)\delta x_k(t) f(x_d(t-1), \theta_d(t-1), t-1) - f(x_d(t-1), \theta_k(t-1), t-1)\\ &= B_k(t-1)\delta\theta_k(t)\delta x_k(t) = A_k(t-1)\delta x_k(t-1) + B_k(t-1)\delta\theta_k(t-1)\end{aligned} \tag{10}$$

Taking the norm of Eq. (9)

$$\begin{aligned}&\|\delta x_k(t) \le c_A^t \|\delta x_k(0)\| + c_A^{t-1} c_B \|\delta\theta_k(0)\| + c_A^{t-2} c_B \|\delta\theta_k(1)\\ &\| + \cdots + c_B \|\delta\theta_k(t-1)\end{aligned} \tag{11}$$

Because the initial state is the same at each iteration, $\delta x_k(0) = 0$. The (10) can be written

$$\|\delta x_k(t)\| \le \sum_{j=0}^{t-1} c_A^{t-j-1} c_B \|\delta\theta_k(j)\| \tag{12}$$

Multiplied by the two sides $c_A^{-\lambda t}$, yields

$$\|\delta x_k(t)\|_\lambda \le \sup \sum_{j=0}^{t-1} \left(c_B c_A^{t-j-1} c_A^{-\lambda t} \|\delta\theta_k(j)\| \right) \le \frac{c_B}{c_A \left(c_A^{\lambda-1} - 1 \right)} \tag{13}$$

Suppose $c > \max\{c_A, \overline{1}\}$, yields

$$\|\delta x_k(t)\|_\lambda \le \frac{c_B}{c_A(c^{\lambda-1} - 1)} \|\delta\theta_k(t)\|_\lambda \tag{14}$$

By (8), we have

$$\begin{aligned}\delta\vartheta_{k+1}(t) &= \delta\theta_k(t) - L(t)(e_k(t+1) - e_k(t))\\ &= \delta\theta_k(t) - L(t) \Bigg\{ \Bigg[h_n \Big(y^{n-1}((t+1), t+1 \Big)\\ &\quad - h_n y_k^{n-1}(t+1), t+1 \Big) \Bigg] - \Bigg[h_n (y^{n-1}((t), t)\\ &\quad - h_n y_k^{n-1}(t), t) \Bigg] \Bigg\}\end{aligned} \tag{15}$$

Remark

$$A_k(t) = \frac{\partial f(x_k(t), \theta_k(t), t)}{\partial x_d(t)} \mid x_k(t) = \xi_k(t)$$

where $\xi_k(t) = (1 - \sigma_3)x(t) + \sigma_3 x_k(k)$, $0 < \sigma_3 < 1$

$$B_k(t) = \frac{\partial f(x_k(t), \theta_k(t), t)}{\partial \theta_k(t)} \mid \theta_k(t) = \eta_k(t)$$

where $\eta_k(t) = (1 - \sigma_4)x(t) + \sigma_4 x_k(k)$, $0 < \sigma_4 < 1$

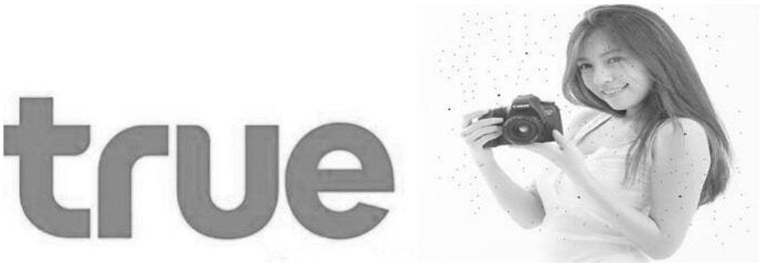

Fig. 11 Attacked with salt and pepper noise and extracted hidden image (Example 1)

$D_{kn}(t) = \frac{\partial h_n(y,t)}{\partial y} \mid y = \xi_{kn}(t)$
where $\xi_{kn}(t) = (1 - \sigma_n)y^{n-1}(t) + \sigma_n y^{n-1}(t)$, $0 < \sigma_n < 1$

$$h_n(y^{n-1}((t+1), t+1) - h_n\left(y_k^{n-1}(t+1), t+1\right)$$
$$= D_{kn}(t+1)(h_{n-1}(y^{n-2}((t+1), t+1) - h_{n-1}$$
$$\left(y_k^{n-2}(t+1), t+1\right)\Big) \tag{16}$$

$$h_n\left(y^{n-1}(t), t\right) - h_n\left(y_k^{n-1}(t), t\right)$$
$$= D_{kn}(t)(h_{n-1}\left(y^{n-2}((t+1), t+1) - h_{n-1}\right.$$
$$\left(y_k^{n-2}(t), t\right)\Big) \tag{17}$$

$$\delta\vartheta_{k+1}(t) = \delta\theta_k(t) - L(t)[\textstyle\prod_{i=2}^{n} D_{ki}(t+1)C_k(t+1)B_k(t)$$
$$\left(f(x_d(t), \theta_d(t), t) - f(x_k(t), \theta_k(t), t) - \prod_{i=2}^{n} D_{ki}(t)C_k(t)\right.$$
$$\delta x_k(t)\Big] \tag{18}$$

By definition of $A_k(t)$ and $B_k(t)$, (18) can be written

$$\delta\vartheta_{k+1}(t) = \left[1 - L(t)\prod_{i=1}^{n} D_{ki}(t+1)C_k(t+1)B_k(t)\right]\delta\theta_k(t) - L(t)$$
$$\left[\prod_{i=1}^{n} D_{ki}(t)C_k(t) - \prod_{i=1}^{n} D_{ki}(t+1)C_k(t+1)A_k(t)\right]\delta x_k(t) \tag{19}$$

From Eq. (7), we have

$$\delta\vartheta_{k+1}(t) = \rho\delta\theta_k(t) + L\left[\prod_{i=1}^{n} D_{ki}(t)C_k(t) - \prod_{i=1}^{n} D_{ki}(t+1)\right.$$
$$\left. C_k(t+1)A_k(t)\right]\delta x_k(t) \tag{20}$$

Remark
$M_k(t) = L\left[\prod_{i=1}^{n} D_{ki}(t)C_k(t) - \prod_{i=1}^{n} D_{ki}(t+1)C_k(t+1)A_k(t)\right]$
So (19) can be written

$$\delta\vartheta_{k+1}(\mathrm{t}) = \rho\delta\theta_k(t) + M_k(t)\delta x_k(t) \tag{21}$$

Suppose $M_k(t) \leq M$, we take λ norm of (21).

$$\left\|\delta\overline{\vartheta}_{k+1}(t)\right\|_\lambda \leq \rho\|\delta\theta_k(t)\|_\lambda + M\|\delta x_k(t)\|_\lambda \tag{22}$$

Introducing (14) into (22), yields

$$\left\|\delta\overline{\vartheta}_{k+1}(t)\right\|_\lambda \leq \rho\|\delta\theta_k(t)\|_\lambda + \frac{Mc_B}{c_A(c^{\lambda-1}-1)}\|\delta\theta_k(t)\|_\lambda \tag{23}$$

If there exist enough λ, then
$\lim_{k\to\infty} \|\delta\theta_k(t)\|_\lambda = 0$

Table 1 Adding the Gaussian noise attack with Example 1

Gaussian noise	VGN = 0.001	VGN = 0.01	VGN = 0.02
NC	0.9935	0.9781	0.9680
PSNR	25.673	24.823	22.081

The steps of using an iterative learning method to reproduce the hidden images are as follows:

1. We find the superimposed mixed image $y(t)$, and the initial estimate θ0(t) with the given arbitrary image sequence of multiple carrier wi(t) (i = 1,2,…,n), where $t \in \{1, 2, \quad, N\}$.
2. Set initial state $x_k(0) = x^0$, substituting θk(t) into the iterative learning control system, and obtain Sk(t) by solving.
3. Calculate the output error ek(t).
4. Using the iterative learning law to calculate θk + 1(t).
5. The given error $J_k = \sup_{t\in\{0,1,2,\cdots N\}}\|\delta\theta_k(t)\|$, if ek($t$) < Jk, then the system will stop iteration; otherwise, set $k = k + 1$, go to step 2).

The image information is hidden in time-varying parameter θk(t) obtained by the iterative learning method. A set of image sequences is known, and then the hidden images are restored according to the pixel ratio of the image.

5 Results and discussions

For mixed images and restored hidden images, we can use the peak signal-to-noise ratio PSNR and normalized cross-correlation coefficient NC to measure the objective fidelity of the image. The peak signal-to-noise ratio of the original carrier image F and image S containing hidden information is measured.

PSNR is:

$$\mathrm{PSNR} = 101g\left(\frac{M \times N \times 255^2}{\sum_{i=1}^{M}\sum_{j=1}^{N}(\mathrm{F}(i,j) - \mathrm{S}(i,j))^2}\right) \tag{24}$$

The peak signal-to-noise ratio PSNR is used as a measure of the objective fidelity of the image. The larger the value, the higher the fidelity of the image mixture.

Normalized cross correlation (NC) measures the degree of similarity between the extracted image and the original image. It is defined as:

Table 2 Adding the salt and pepper noise attack with Example 1

Salt and pepper noise	INSP = 0.001	INSP = 0.01	INSP = 0.02
NC	0.9932	0.9721	0.9603
PSNR	26.543	25.829	22.321

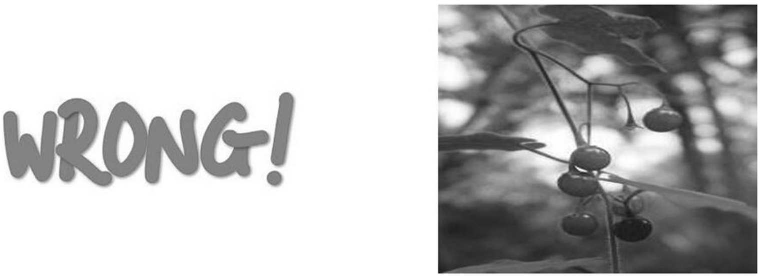

Fig. 12 Attacked with Gaussian noise and extracted hidden image (Example 2)

$$\mathrm{NC} = \frac{\sum_{i=1}^{M\times M} x(t) \times \hat{x}(t)}{\sum_{i=1}^{M\times M} x(t)^2} \tag{25}$$

where $x(t)$ and $\hat{x}(t)$ denote pixel value sequence of the original image and pixel value sequence of extracted image.

In this experiment, we use Camera (256*256) and Lena (256*256) as the two carrier images, and the binary image "true" (32*32) as the image to be hidden.

The state of the digital image embedding system is as follows:

$$\begin{cases} x(t+1) = (\lambda + \theta(t))x(t)(1-x(t)) \\ y_1(t) = \alpha_1 w_1(t) + (1-\alpha_1)x(t) \\ y_2(t) = \alpha_2 w_2(t) + (1-\alpha_2)y_1(t) \\ y(t) = y_2(t) \end{cases}$$

Example 1. In the experiment, the hidden image "true" is first embedded in the carrier image Lena. Then, the mixed image is embedded into the carrier image Camera again, and finally we obtain the mixture images. Taking $\lambda = 3.568$, the initial $x_k(0) = 0.5$. Original image $\theta(t)$ is binary image, the carrier image $w_1(t)$ and $w_2(t)$ are two pixel points of the same gray image, and the images obtained after two times of superposition and mixing are y (t).

Taking $\lambda = 3.568$, $\alpha_1 = 0.52$, according to the chaotic sequence generated by the Eq. (5), $\{\alpha_i\}$, we choose the required experimental parameter sequence $\{\alpha_1,\alpha_2\}$., the given learning gain is:

$$L_k(t) = \frac{1}{(\beta_1\beta_2)x_k(t)(1-x_k(t))}$$

where $\beta_i = 1 - \alpha_i$, $i = 1, 2$

Figure 2 is the hidden image "true" used during the experiment, and Fig. 3 is the carrier image Camera and Lena. Firstly, the hidden image "true" needs to be embedded in the first carrier image Lena, and then the resulting mixed image is further embedded into the second carrier image Camera. Figure 4 is the final mixed image Camera and extracted hidden image using an iterative learning method. Experimental results show that this method can completely recover hidden images.

To verify the performance of the algorithm, we define the index function as

$$J_k = \sup_{t\in\{1,2,\cdots,N\}} |\delta\theta_k(t)|$$

We reconstruct the error convergence process of hidden image "true" by iterative learning algorithm. From Fig. 5, it can be seen that when the iterative times reach to 3000, the identified image and original image error has reached 10^{-12}. The experimental results show that the method effectively reconstructs the finite length information.

Example 2. In the experiment 2, the "wrong" is hidden image. Cherry and Lena are carrier images, then we take the hidden image embeds into the carrier images and obtain the mixture images finally. Taking $\lambda = 4.256$, the initial $x_k(0) = 0$. The rest of the conditions are the same as the Example 1.

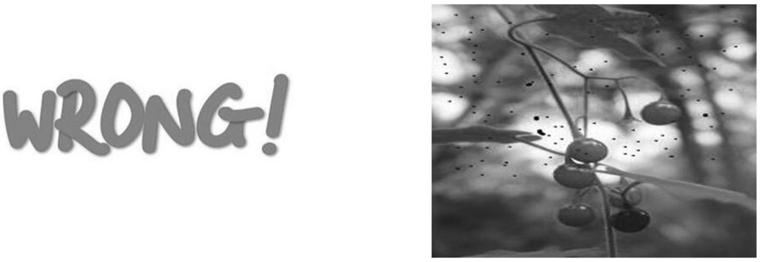

Fig. 13 Attacked with salt and pepper noise and extracted hidden image (Example 2)

Table 3 Adding the Gaussian noise attack with Example 2

Gaussian noise	VGN = 0.001	VGN = 0.01	VGN = 0.02
NC	0.9892	0.9821	0.9790
PSNR	25.351	24.723	22.109

By the chaotic sequence produced by Eq. (5), {αi}, the required experimental parameter sequences that we choose are $\{\alpha_1,\alpha_2\}$ and the given learning gain is:

$L_k(t)=\frac{1}{(\beta_1\beta_2)x_k(t)(1-x_k(t))}$

where $\beta_i = 1 - \alpha_i$, $i = 1, 2$

Figure 6 is the hidden image "wrong" used during the experiment, and Cherry and Lena are the carrier images in Fig. 7. Firstly, we embed the "wrong" image into the Cherry and obtain a mixed image. Secondly, we embed the mixed image into the Lena image. Figure 8 is the final mixed image Cherry and extracting hidden image by the iterative learning way. Experimental results illustrate that the way that we use can completely reconstruct the hidden image.

We use the same index function as experiment 1:

$$J_k = \sup_{t\in\{1,2,\cdots,N\}} |\delta\theta_k(t)|$$

We use the same algorithm to reconstruct the convergence process of hidden image "wrong." We know the iterative error has reached 10–14 with the iterative times reach to 3000 from Fig. 9. The simulation shows the algorithm can effectively reconstruct the finite length information.

The anti-attack results of the test algorithm are as follows:

1. Anti-attack test adding Gauss noise and salt and pepper noise

Adding Gauss noise and salt and pepper noise to the mixed image, the Gauss noise variance VGN is 0.001, 0.01, and 0.02, respectively. Noise intensity of salt and pepper (INSP) is 0.001, 0.01, and 0.02.

Figures 10 and 11 show the mixed image and the extracted image after the attack. The similarity NC between the original image and the extracted image after the attack are shown in Table 1. The peak signal-to-noise ratio PSNR of the original mixed image and the mixed image after the attack is shown in Table 2.

Table 4 Adding the salt and pepper noise attack with Example 2

Salt and pepper noise	INSP = 0.001	INSP = 0.01	INSP = 0.02
NC	0.9895	0.9801	0.9721
PSNR	25.921	24.823	23.321

2. Anti-attack test with compressed

The JPEG image compression method is a compression attack for the mixed image. The smaller the compression factor *Q*, the higher the compression, that is, the greater the pixel loss. In Experiment 1 and Experiment 2, we separately select different compression factors *Q* to extract the hidden images respectively. When *Q* = 10, the compression ratio is already very large. From Figs. 10, 11, 12, and 13, it can be seen that the "true" image proposed by the iterative learning identification method still has a high correlation NC (0.78) and better PSNR. It shows that the algorithm has better robustness for JPEG compression attack. The robustness of algorithms for JPEG compression attack are shown in (Tables 3 and 4).

6 Conclusions

In this paper, we proposed the image extraction problem by using iterative learning algorithm. This method is to embed the hidden image into several different carrier images. Finally, the iterative learning is used to fully track the parameters of the image information, and the hidden image is reproduced. The parameters of the iterative learning law are updated with the change of time, which shows that the algorithm has better self-adaptability. Both experimental results show that when the mixed image with hidden information is attacked, the iterative learning recognition method can still recover the hidden image, and the ordinary reversible image solving method cannot restore the hidden image. The experimental data also proves the anti-attack of the algorithm.

Abbreviations

INSP: Noise intensity of salt and pepper; NC: Normalized cross correlation; PSNR: Peak signal to noise ratio; VGN: Gauss noise variance

Acknowledgements

The authors thank the editor and anonymous reviewers for their helpful comments and valuable suggestions.

Funding

The work was supported by the Hechi University Foundation (XJ2016ZD004), Hechi University Youth Teacher Foundation (XJ2017QN08), the Projection of Environment Master Foundation (2017HJA001, 2017HJB001), the important project of the New Century Teaching Reform Project in Guangxi (2010JGZ033), and Guangxi Youth teacher Foundation (2018KY0495).

Availability of data and materials

We can provide the data.

Authors' contributions

All authors contributed equally and significantly in writing this article. All authors read and approved the final manuscript. Yinghui Li is the corresponding author.

Authors' information

Yingjun Zhang was born in Xinjiang in 1984. He received the M.S. degree in control theory and control engineering from Guangxi Technology University in 2011. He is pursuing the Ph.D. in Air Force Engineering University. His research interests are in fault diagnosis control and iterative learning control.

Yinghui Li (corresponding author) was born in Guangxi in 1966. She received the Ph.D. from Shanghai JiaoTong University. Now she is a professor in Air Force Engineering University. Her research interests include nonlinear control, motor control, and dynamics control.

Jianhuan Su was born in Guangxi in 1967. He received the M.S. from Chongqin University. Now he is a professor in Hechi University. His research interests include single process, nonlinear control.

Ethics approval and consent to participate

Approved.

Consent for publication

Approved.

Competing interests

The authors declare that they have no competing interests. And all authors have seen the manuscript and approved to submit to your journal. We confirm that the content of the manuscript has not been published or submitted for publication elsewhere.

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Author details

[1]Aeronautics and Astronautics Engineering Institute, Air Force Engineering University, Xi'an 710038, Shanxi Province, China. [2]School of Physics and Electrical Engineering, Hechi University Yizhou, No.42 Rd. Longjiang, Yizhou 546300, Guangxi, China.

Received: 13 July 2018 Accepted: 14 September 2018
Published online: 03 October 2018

References

1. E. Alpaydin, *Introduction to Machine Learning* (The MIT Press, London, 2010), p. 110 ISBN 978-0-262-01243-0. Retrieved 4 Feb 2017
2. Akhshani A, Mahmodi H, Akhavan A. *A Novel Block Cipher Based on Hierarchy of One-Dimensional Composition Chaotic Maps[C]//*. IEEE International Conference on Image Processing. IEEE, (Chicago, USA, 2007), pp. 1993-1996
3. Xie, Eric Yong, et al. *On the cryptanalysis of Fridrich's chaotic image encryption scheme[J]*.Signal Processing. 132(2), 150-154 (2017)
4. M.D. Swanson, Multimedia data-embedding and watermarking technologies. Proc. IEEE **86**(6), 1064–1087 (1998)
5. J. Zhao, E. Koch, A generic digital watermarking model. Comput. Graph. **22**(4), 397–403 (1998)
6. M.S. Fu, O.C. Au, Data hiding watermarking for halftone images. IEEE Trans. Image Process. **11**(4), 909–930 (2002)
7. W. Bender, D. Gruhl, Techniques for data hiding. IBM Syst. J **35**(4), 313–336 (1996)
8. C.H. Lee, Y.K. Lee, An adaptive digital image watermarking technique for copyright protection. IEEE Trans. Consum. Electron. **45**(4), 1005–1015 (1999)
9. N. Nikolaidis, I. Pitas, Robust image watermarking in the spatial domain. Signal Process **66**(3), 385–403 (1998)
10. H.-p. Hu, L. Shuang-hong, Z.-x. Wang, A method for generating chaotic key stream. Chinese J Comput **7**(3), 408–414 (2004)
11. Liu R Z, Tan T N. Watermarking for digital images[C]//. International Conference on Signal Processing. **2**, 944-947 (2002)
12. M.A. Suhail, Digital watermarking-based DCT and JPEG model. IEEE Trans. Instrum. Meas. **52**(5), 1640–1647 (2003)
13. M. Urvoy, Perceptual DFT watermarking with improved detection and robustness to geometrical distortions. IEEE Trans. Inf. Forensics Secur. **9**(7), 1108–1119 (2014)
14. Y. Ishikawa, Optimization of size of pixel blocks for orthogonal transform in optical watermarking technique. J. Disp. Technol **8**(9), 505–510 (2012)
15. Y. Xu, S. Dong, B. Xuhui, Zero-error convergence of iterative learning control using quantized error information. IMA J. Math. Control. Inf. **34**(3), 1061–1077 (2016)
16. Y. Chen, X. Liao, Cryptanalysis on a modified Baptista-type cryptosystem with chaotic masking algorithm. Phys. Lett. A **342**(5–6), 389–396 (2005)
17. E.Y. Xie, C. Li, S. Yu, J. Lü, On the cryptanalysis of Fridrich's chaotic image encryption scheme. Signal Process. **132**, 150–154 (2017)
18. A. Akhavan, A. Samsudin, A. Akhshani, Cryptanalysis of an improvement over an image encryption method based on total shuffling. Opt. Commun. **350**, 77–82 (2015)
19. A. Akhavan, A. Samsudin, A. Akhshani, Cryptanalysis of an image encryption algorithm based on DNA encoding. Opt. Laser Technol **95**, 94–99 (2017)
20. M.S. Baptista, Cryptography with chaos. Phys. Lett. A **240**(1–2), 50–54 (1998)
21. S. Li, X. Zheng, Cryptanalysis of a chaotic image encryption method. 2002 Proc. IEEE Int. Symp. Circuits Syst. Proceedings (Cat. No.02CH37353). 2: II–708–II–711 **2**, 708–711 (2002)
22. G. Alvarez, S. Li, Some basic cryptographic requirements for chaos-based cryptosystems. Int. J. Bifurcation Chaos **16**(8), 2129–2151 (2006)
23. E. Solak, C. Çokal, O.T. Yildiz, T. Biyikoğlu, Cryptanalysis of Fridrich's chaotic image encryption. Int. J. Bifurcation Chaos **20**(5), 1405–1413 (2010)
24. Kwok H S, Tang W K S. *A fast image encryption system based on chaotic maps with finite precision representation[J]*. Chaos Solitons & Fractals. **32**(4), 1518-1529 (2007)
25. C. Li, Cracking a hierarchical chaotic image encryption algorithm based on permutation. Signal Process. **118**, 203–210 (2016)
26. L. Kocarev, M. Sterjev, A. Fekete, G. Vattay, Public-key encryption with chaos. Chaos: an interdisciplinary. J. Nonlinear Sci. **14**(4), 1078–1082 (2004)
27. L. Kocarev, J. Makraduli, P. Amato, Public-key encryption based on Chebyshev polynomials. Circuits Systems Signal Process **24**(5), 497–517 (2005)
28. A. Akhavan, A. Samsudin, A. Akhshani, A symmetric image encryption scheme based on combination of nonlinear chaotic maps. J. Franklin Inst. **348**(8), 1797–1813 (2011)
29. Y. Mao, G. Chen, *Handbook of Geometric Computing* (Springer, Heidelberg, 2005), pp. 231–265
30. S. Behnia, A. Akhshani, H. Mahmodi, A. Akhavan, A novel algorithm for image encryption based on mixture of chaotic maps. Chaos Solitons Fractals **35**(2), 408–419 (2008)
31. S. Behnia, A. Akhshani, H. Mahmodi, A. Akhavan, Chaotic cryptographic scheme based on composition maps. Int. J. Bifurcation Chaos. **18**(1), 251–261 (2008)
32. N. Bourbakis, C. Alexopoulos, Picture data encryption using scan patterns. Pattern Recogn **25**(6), 567–581 (1992)
33. S. Behnia, A. Akhshani, S. Ahadpour, H. Mahmodi, A. Akhavan, A fast chaotic encryption scheme based on piecewise nonlinear chaotic maps. Phys. Lett. A **366**(4–5), 391–396 (2007)
34. M. Ghebleh, A. Kanso, A robust chaotic algorithm for digital image steganography. Commun. Nonlinear Sci. Numer. Simul. **19**(6), 1898–1907 (2014)
35. Q. Liu, P.-y. Li, M.-c. Zhang, Y.-x. Sui, H.-j. Yang, A novel image encryption algorithm based on chaos maps with Markov properties. Commun. Nonlinear Sci. Numer. Simul. **20**(2), 506–515 (2015)
36. S. Behnia, A. Akhshani, A. Akhavan, H. Mahmodi, Applications of tripled chaotic maps in cryptography. Chaos Solitons Fractals **40**(1), 505–519 (2009)
37. A. Kanso, M. Ghebleh, An efficient and robust image encryption scheme for medical applications. Commun. Nonlinear Sci. Numer. Simul. **24**(1–3), 98–116 (2015)
38. H.S. Kwok, W.K.S. Tang, A fast image encryption system based on chaotic maps with finite precision representation. Chaos Solitons Fractals **32**(4), 1518–1529 (2007)
39. A. Akhavan, H. Mahmodi, A. Akhshani, in *Computer and Information Sciences – ISCIS 2006. Lecture Notes in Computer Science*. A new image encryption algorithm based on one-dimensional polynomial chaotic maps (Springer, Heidelberg, 2006), pp. 963–971