Multimedia Tools and Applications (2024) 83:20861–20887
https://doi.org/10.1007/s11042-023-16240-w

# Chaotic coyote optimization algorithm for image encryption and steganography

**Huawei Tong[1,2] · Tianyou Li[1,2] · Youyun Xu[1,2] · Xinzhong Su[1,2] · Guopeng Qiao[1,2]**

Received: 21 March 2022 / Revised: 29 May 2023 / Accepted: 4 July 2023 /
Published online: 4 August 2023


**Abstract**
It is significant to ensure the communication networks and information security, and balancing simplicity and complexity is still a real issue that is the key to improve the effectiveness of a scheme in many applications scenarios.Current researches focusing on the security of digital images and putting barriers to protect sensitive data still have room for improvement. Herein,the aim of this paper is twofold. Firstly, we propose a color image encryption method by utilizing Chaotic Coyote Optimization Algorithm to solve the key selection problem for minimizing the correlation between adjacent pixels of the cipher image, where three color channels are processed to enhance its security against various attacks. Secondly, we design a color image Steganography scheme that has ability to defend common types of the image attacks. In the design stage of embedding, the Chaotic Coyote Optimization Algorithm and a special designed strategy are implemented together to handle the problem of location selection to lower the distortion in all components of the embedded image. According to the simulation results, the proposed image encryption method is efficient and robust considering the performance indexes: correlation coefficient, information entropy, number of pixels change rate, unified average changing intensity, and histogram. Meanwhile, the image Steganography approach also provides satisfying effect compared with other methods in the literature, based on indicators of peak signal-to-noise ratio and structural similarity.

✉ Youyun Xu
yyxu@njupt.edu.cn

Huawei Tong
2021010111@njupt.edu.cn

Tianyou Li
314634357@qq.com

Xinzhong Su
suxinz20@163.com

Guopeng Qiao
1020010219@njupt.edu.cn

[1] College of Telecommunications and Information Engineering, Nanjing University of Posts and Telecommunications, No.66, new model road, Nanjing 210003, Jiangsu, China

[2] National Engineering Research Center of Communications & Networking, No.66, new model road, Nanjing 210003, Jiangsu, China

**Keywords** Metaheuristic · Encryption · Steganography · Image processing · Information security

## 1 Introduction

Information security is very important in digital world and communication networks needed to ensure under the control.Especially a considerable number of devices, i.e., computers, mobile phones, smart watches, or other smart Internet of Things devices, have become very essential for our daily life. That is, lifestyle has entirely changed by using those devices, which provide remarkable experiences for everyone and cater to their requirements, meanwhile granting the fact that there has be a tremendous increase in personal and industry data in recent years.

From an industrial economy to a digital society at full speed and with breakthrough information technologies, one of the major risk that governments, businesses, and individuals alike facing, is cyberattacks emerged across the globe. It is a big fact that the intractability of this issue challenges people in ways that no hazard has faced before. Innovators always assure confidentiality and integrity of crucial information and running process of the new and improved technology, but it's hard not to be skeptic when faced with reality. All this notwithstanding, guaranteeing the safe processing and storing of industry data, personal healthcare and sensitive information is a necessary move to align the stability and growth of information technologies. From healthcare data breach to hotel management booking platform data leak, there is a lot of trouble the ignorant of communication networks and information security issues can cause, none of which was intended when to make design rules the first time. To be better said, communication networks and information security is a key topic frequently discussed and must not be ignored, even if smart devices Internet connected are helping works and activities more effortless and trouble-free in various areas. In particular, image encryption and Steganography have been applied in numerous realms, including wireless communications, medical imaging, and multimedia systems, after images becoming one of the most usable forms of information [11]. For instance, in the healthcare scenario, the image of iris can be used to assess an individual's general health based on the analyze of color, patterns, and various other properties [10].

Image encryption is one of information security topics, which encountered at least once over communication networks and online [8]. Digital images need to be protected against unauthorized users due to carrying essential information in many scenes. With the advances in TV and mobile applications, encrypted images are transmitted with the thirst and focus [11]. And also it should has power to defend other illegal activities, e.g., hacking, copying, and using information maliciously [16]. Image encryption is the paradigm where scrambling a message or original piece of information with math to make it illegible, then store or transmit it along to the receiver who will take appropriate action to unscramble it for directly reading. For ensuring the security of the sensitive images, encryption is an effective way to against third parties snooping around [36, 42], with the substitution strategy to change on the plaintext and obtain a ciphered image finally. Thus, image encryption has become a major issue in communication networks and information security [12, 22].

At the other side, Steganography is also a special branch of information security, which performs a greater role in a variety of fields [28], being used as a powerful solution to the issue of content authentication and copy-right protection [32]. Normally, Steganography is a practice or technique of hiding secret messages or information inside of another item. Cryptography technology paves the way for development of Steganography in digital times,

which has a long history of human utilization. Those two, differs greatly in their function that cryptography conceals the content of secret file, but steganography implants information and does not permit a third party becomes aware of the existence of embedded messages if they use the human eye [6, 15, 23]. Steganography methods not only hide the original message into a carrier, but also keep the changes are imperceptible. A collection of applications in the field of Steganography, signals that it is much needed for law enforcement, individual's information secure, network security, banking, national intelligence missions, military bodies etc [9, 17]. Generally, Steganography is classified into five types: text, image, audio, video, and network Steganography. Image Steganography takes the lead in multimedia communication [18].

Optimization strategies of algorithm or scheme are important to handle the problems in the procedures of image encryption and Steganography. Generally, the technologies for solving optimization problems can be classified into two types that deterministic algorithms and non-deterministic also named stochastic algorithms. To search the global optimal, it is tough that make deterministic algorithm to explore the whole lot of possible candidate solutions on condition that search space is bounded by practical constraints, discrete problems, and problems comprising multitudinous local optimal solutions. Metaheuristic is a useful approach for obtaining a sufficiently good solution in economics, operations research and engineering problems, which cannot be disentangled by conventional means in the environment where nearly limitless computing power can be provided [31]. The term metaheuristic matches up almost identically to the mean of global search technique or all novel nature-inspired optimization algorithms which are extremely effective, supremely versatile and enable to drive vigorously for optimality.

The term of "Artificial Intelligence (AI)" is a branch of computer science worked on making computers behave like humans, which is created by John McCarthy in 1956 at Massachusetts Institute of Technology in the USA. Expert systems, Games playing, natural language, robotics and soft computing are belonged to AI. Soft computing or Computational Intelligence can be split into four areas of research: Fuzzy Systems, Stochastic Algorithms, Neural Networks, and Machine Learning [25]. The stochastic algorithms include heuristics and metaheuristics algorithms.

At the moment, problems lie in image encryption and Steganography are making correlation coefficient more lower, and providing more higher robustness and lower distortion of embedded image, respectively. And we want to extend the application of [40] which is the our past work. Therefore, we propose two methods based on a metaheuristic algorithm named Chaotic Coyote Optimization Algorithm to solve thoses problems to achieve a higher level of quality, which is also the goal in this paper.

The main contributions and insights of this paper are listed as follows:

1. We propose a new color image encryption method to overcome the low efficiency of the present schemes, which is designed subtly on basis of Chaotic Coyote Optimization Algorithm and named EN-CCOA. The EN-CCOA achieves satisfactorily and effectively in reducing the correlation coefficient, where the setting is more straightforward with fewer parameters and it runs easier and faster.
2. We propose a new color image Steganography method based on the Chaotic Coyote Optimization Algorithm (ST-CCOA) to embed secret data more effective. We design two acceleration factors to avoid wasting lots of time selecting the location for hiding and realize the fast convergence. And we find out the best initial value of those two factors over repeated trials.

3. The proposed EN-CCOA and ST-CCOA methods perform better than the other algorithms in terms of some commonly used evaluation metrics. In addition, our proposed methods have the capability for resisting the image attacks.

Accordingly, the rest of this paper is structured as follows. After a systematic literature reviewing, some existing algorithms for image encryption and Steganography has been discussed in Section 2. Chaotic Coyote Optimization Algorithm is formulated and its entire logic is approximately described by the pseudocode in Section 3. In Section 4, we propose the EN-CCOA method to deal with the color image encryption problem, Meanwhile, for the color image Steganography, the design of ST-CCOA method is introduced. The Section 5 displays the data and analyzes the simulation results. Section 6 presents a brief conclusion at the end of this paper.

## 2 Background and related works

Numerous researchers, for their idea to work, find the insufficient of image encryption firstly, and then use some effective methods to perfect it. Most recent developments are based on the swarm intelligence algorithms and chaotic system, the performance can be as regarded as satisfactory.

In Wireless Sensor Networks, Shankar and Elhoseny [36] have done some works to enhance the enryption quality for transmitting digital images, which including Light Weight Ciphers algorithm in encryption and Opposition-based Particle Swarm Optimization (PSO) algorithm in key optimization. Managing medical images, especially when storing on cloud sever and transmitting via Internet of Things, which is a component of the complicated security issue. For improving encryption and avoiding falling into local optimum, due to the properties of chaos, like high sensitivity of initial state,a new image cipher putting together from a chaotic system mixing two chaotic maps was proposed in [3]. That chaos-based cipher has the better complexity, and its chaotic parameter range is wide than counterparts, thus having power to against many attacks. A color image cryptosystem is proposed in [7], depending on dynamic DNA encryption and four-wing hyperchaotic system, which resist plaintext attacks well. In order to address the defect that chaos-based cryptosystems's dynamical behaviors are not complex enough, Hua et al. [14] combined two chaotic maps together and applied it into image encryption. It is clear that based on chaotic system, image encryption is widely researched [35, 41, 44]. Zeng and Wang [47] proposed a hyperchaotic encryption system which combines PSO algorithm and cellular automata (CA). Their system has increased the complexity and diversity of the particles in PSO, and enriched the security. Ahmad et al. [2] proposed an image encryption scheme based on PSO and used chaotic map for generating key. In [42], an image encryption algorithm by using multi-objective PSO for selecting sub-key sequence, implementing encryption based on DNA encoding and Logistic map, is proposed and has been verified its satisfactory performance.

There are many researchers struggle to fix and improve Steganography technologies. Large number of methods for Steganography have been used to meet some specific demand. Several works have given our some indicators which help us to change our idea into facts, including building a list of searches related to both Steganography and its specific approaches.

In [39], Swain applied least significant bit and quotient value differencing to boost the image capacity and ensured the message can not be detected. For e-healthcare, a new data hiding scheme that embeds fall-related clinical information was introduced in [32], whose

capacity is high and being reversed is supported at the end. Kadhim's group proposed an improved method that employs Dual-Tree Complex Wavelet Transform and Machine learning based optimization algorithms to make image Steganographic system more powerful [18]. By implementing Recurrent Neural Networks, Yang et al. [46] proposed an enhanced linguistic Steganography approach achieving high embedding efficiency. Atawneh et al. [4] proposed a diamond encoding scheme for reducing the distortion added to the images to improve the embedding efficiency in the discrete wavelet transform Steganography. In [28], through analyzing the uncorrelated color space, an adaptive least significant bit substitution method to make image's visual quality more intact. The channel-dependent payload partition strategy is proposed in [22] to improve the ability of against detection, which is based on amplifying the modification probabilities of channels. For processing batch images, an encryption algorithm is proposed based on the Cipher Block Chaining mode, which can be applied in parallel computing [38]. By using a controlled-NOT gate and the two most and least significant qubits, a quantum Steganography approach is put forward in [1]. Based on quaternion Hadamard transform and Schur decomposition, Li et al. [20] designed a novel color image watermarking scheme to improve the robustness against attacks. For smart city application, an image watermarking method by implementing synergetic neural networks is proposed in [21]. In the process of content confidentiality of medical images, a biomedical data concealment procedure is presented with Sudoku based scrambling on biomedical image and Queen Traversal pattern for locating the pixels over the image [5]. Snasel et al. [37] used PSO to strengthen the ability of embedding secret messages and applied AVX instructions to accelerate data parallel operations. For improving the peak signal-to-noise ration and the mean square error, a method based on PSO With sparse representation for image Steganography is proposed in [30]. PSO is implemented to find the best pixels where embedding the hidden data, has been verified its robustness and statistical undetectability in [26, 27]. And an image Steganography approach with Integer Wavelet Transform and PSO is proposed by Muhuri et al. [29]. In [19], an image Steganography scheme is introduced, which utilized the modulus function, PSO, and pixel-value differencing, and its performance is also be confirmed. Based on Cuckoo Search, an approach for hiding audio file into JPEG image is proposed [13], which has the ability of finding the most suitable solution for minimizing the distortion in cover image.

In conclusion, color image encryption and Steganography approaches have satisfactory performance on the basis of the swarm intelligence algorithms.

## 3 CCOA: a brief overview

Chaotic Coyote Optimization Algorithm (CCOA) [40] is an advanced swarm intelligence algorithm that enhances the performance of the Coyote Optimization Algorithm (COA) designed by Pierezan and Coelho [34]. The structure and mathematical modeling of CCOA are comprehensively described in this section.

CCOA belongs to metaheuristic algorithms and tackles the optimization problem in a reasonable amount of time. Metaheuristic is defined in such a way that, an approach that devises an interaction between the local strengthening programs and the superior level stratagems to create a process to capable of flying from local optima and achieving a robust search of solution space. Swarm intelligence explores and simulates in depth the behaviors of social animals without a centralized control agent in native environment. Swarm intelligence can be seen as composed by a set of individuals that interact with each other posing intelligence

as easy as falling off a log [25]. This way, the usage of those individuals is very suitable to deal with complex global optimization problem. Hence, it has been used in some fields of engineering and makes them capable of unravelling the challenging real-world issues.

Inspired by the species called Canis latrans, the mechanism of CCOA is divided into social structure, population exchange, cultural tendency and interaction, birth and dead procedure. The biggest difference between CCOA and other swarm algorithms is that the concept of social conditions and its update process are employed or not. More specifically, each coyote depends on its social condition to find the best solution of an optimization problem.

Social structure is introduced to imply the adaptability of each agent, and during initialization, for all population, which is calculated as

$$S_c^{p,t} = \vec{x} = (x_1, x_2, \ldots, x_D), \tag{1}$$

where $S_c^{p,t}$ defines the social condition of $c$th coyote in $p$th pack in the $t$th instant of time, $D$ means the search space dimension, and $\vec{x}$ is the decision variables of an optimization problem.

In the search space, no one goes through any competition without a good social condition, which is obtained by

$$S_{c,d}^{p,t} = L_d + C_d \times (U_d - L_d), \tag{2}$$

where, $C_d$ is a chaotic number lie in the range of [0, 1] in $d$th dimension, $U_d$ and $L_d$ represent the upper and lower bounds of decision variable, respectively.

In the world of coyotes, adapting to the surroundings is more about social conditions than anything. Thus, fitness value is easily calculated by using the (3).

$$F_c^{p,t} = fun\_fitness(S_c^{p,t}). \tag{3}$$

Several researches indicates that each pack has two alphas in the real world, but considering computational complexity, CCOA only select the best one (i.e., the coyote has the best adaptability) as an alpha in every pack. That means, the process of selection can be finished according to (4).

$$Alpha^{p,t} = \{S_c^{p,t} \| arg_{c=\{1,2,\ldots,N_{coy}\}} \min fun\_fitness(S_c^{p,t})\}, \tag{4}$$

where, $N_{coy}$ is the number of coyotes in a pack.

Note that, all information including social conditions are linked and shared to make a pack stronger. Thus, the formula for computing cultural tendency $Q$ is given below:

$$Q_d^{p,t} = \begin{cases} R_{0.5\times(N_{coy}+1),d}^{p,t}, & N_{coy} \text{ is odd} \\ (R_{0.5\times N_{coy},d}^{p,t} + R_{0.5\times(N_{coy}+1),d}^{p,t})/2, & N_{coy} \text{ is even} \end{cases}, \tag{5}$$

where, $R$ is the ranked social conditions of all coyotes, and $Q_d^{p,t}$ denotes the median social conditions of all coyotes in $p$th pack in $d$th dimension in the $t$th instant of time.

In terms of the number of packs and coyotes inside pack, which are chosen in advance ahead of running, the probability of the event that coyote leave its pack and enter another is evaluated as follows:

$$P_e = \frac{N_{coy}^2}{200}, \tag{6}$$

in which, $N_{coy}$ denotes the number of coyotes in a pack.

We define the association probability $P_g$ and scatter probability $P_s$, which are specially served as assistants to escort the cultural diversity of each pack of coyotes,

$$P_g = \frac{1 - P_s}{2}. \tag{7}$$

If $D$ denotes the dimension of search space, $P_s$ in (7) can be formulated by

$$P_s = 1/D. \tag{8}$$

To better facilitate the benign competition and develop of coyote pack, birth and death strategy is employed that assume the newborn coyote is generated and initialized by mixing the social conditions of its parents (randomly chosen), which is applied as in (9).

$$New^{p,t} = \begin{cases} S^{p,t}_{f,d}, & r_d < P_s \text{ or } d = d_1 \\ S^{p,t}_{m,d}, & r_d \geq P_s + P_g \text{ or } d = d_2 \\ R_d, & \text{otherwise} \end{cases}, \tag{9}$$

where, $f$ and $m$ (the coyotes which are randomly chosen) represent father and mother of this newborn,respectively and, $r_d$ is a number generated randomly in between the interval (0,1), $R_d$ is a random number inside the decision variable bound of the $d$th dimension, $d_1$ and $d_2$ are random dimensions of the optimization problem.

Two influences, including alpha influence that the cultural difference between a coyote (randomly chosen) and the alpha, and pack influence that the cultural difference between a random coyote and its corresponding pack's cultural tendency, have been taken into consideration. Due to the fact that coyotes of this species are completely under those two influences, this process is realized as below, where $c_1$ and $c_2$ are random coyotes in $p$th pack in the $t$th instant of time.

$$\lambda_1 = Alpha^{p,t} - S^{p,t}_{c_1}, \tag{10}$$

$$\lambda_2 = Q^{p,t} - S^{p,t}_{c_2}, \tag{11}$$

in which, $\lambda_1$ represents the alpha influence, $\lambda_2$ represents the pack influence, $Alpha^{p,t}$ and $Q^{p,t}$ are the alpha coyote and the cultural tendency in $p$th pack in the $t$th instant of time, respectively.

For see the adaptability as their great adventure, changing social condition has been forced upon each individual coyote, so that coyotes can do everything they can to make it more efficient to tackle the survival problems. The value is updated by using (12).

$$NewS^{p,t}_c = S^{p,t}_c + C_1 \times \lambda_1 + C_2 \times \lambda_2, \tag{12}$$

where, $C_1$ and $C_2$ are chaotic numbers inside (0,1).

Then, the new fitness value is computed using (3).

$$NewF^{p,t}_c = fun\_fitness(S^{p,t}_c). \tag{13}$$

Here,there is a simple rule which can be performed in the phase of rejuvenating the whole current social condition, described as follows.

$$S^{p,t+1}_c = \begin{cases} NewS^{p,t}_c, & NewF^{p,t}_c < F^{p,t}_c \\ S^{p,t}_c, & \text{otherwise} \end{cases}. \tag{14}$$

Being in the environment which for all coyotes is fundamental need to live their best lives. After running this algorithm, the best coyote will be found—the one settles in to anything

**Algorithm 1** Coyote Optimization Algorithm.

```
input  : population each pack, number of packs
         maximum total population
output : best coyote: B
// which is adjust best to the surroundings
foreach coyote do
    initialize social condition (2);
    calculate fitness value (3);
repeat
    foreach pack do
        select alpha (4);
        work out social tendency (5);
        foreach coyote in this pack do
            update social condition (12);
            obtain fitness value (13);
        Life (this pack) ;
    reassign packs ← Exchange (all coyotes) ;
    update global best B;
until greater than maximum total population;
def Life(pack) :
    calculate number of this pack β;
    γ ← generate and initialize new coyote;
    α ← adapted worse than γ to their environment;
    if β > 1 then
        coyote γ survives;
        the oldermost of α dies ;
        else if β = 1 then
            coyote γ survives;
            coyotes in α die;
        else coyote γ dies;
    return this pack;
def Exchange (coyotes) :
    calculate probability value P ;
    generate chaotic number c ;
    if c < P then
        some leave their pack and enter a new one;
    return new assign;
```

challenging and new surroundings (i.e., best solution which more effectively achieves the aim of problem to have maximum or minimum fitness value).

Finally, the complete CCOA algorithm is listed clearly in Algorithm 1, and in addition, a schematic diagram of the natural mechanism that CCOA mimic is drawn as shown in Fig. 1.

## 4 The proposed methods

### 4.1 Color image encryption method based on CCOA (EN-CCOA)

A standout amongst the most vital data, which is in the process of sending over communication networks to one or more receivers, is the digital images that is essential in social platform and medical environment. In this way, using a image encryption method is requisite for

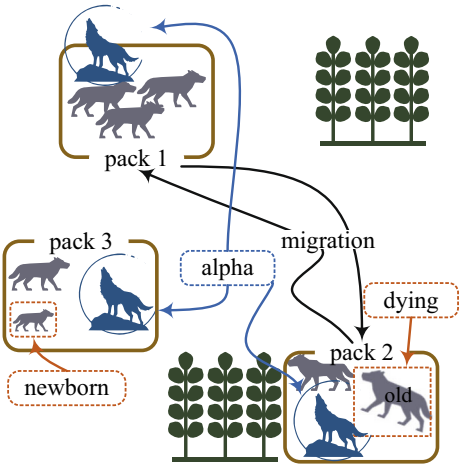


**Fig. 1** Schematic diagram of coyote optimization algorithm shows that each pack including an alpha and some coyotes. Some mechanisms of coyotes as in migration, birth and death,are marked noticeably

safeguarding industrial, commercial and individual private data. The basic structure of the color image encryption and decryption process is shown in Fig. 2. A RGB (red, green, and blue) image can be divided into three components, including red, green, and blue component, and each component is encrypted by implementing a encryption method. Then, these three encryption parts are merged together into the cipher image. It's imperative to realize that the key for encryption and decryption must be shared via the private communication channel for achieving maximum security, and the cipher image can be transmitted through the public communication networks at the same time.

Bit depth is the concept of image which relates to the quality of image files. That is, the number of information image file carries refers to bit depth which significantly impacts on overall image file size. In general, the bit depth of images is 8-bit (each pixel is 8 bits deep so construct 256 color palettes) or 24-bit (has three channels, and 8 bits per channel, they are red, green, and blue color respectively) that are highly related to a certain extent. The higher the bit depth of a picture file, it supports a strongly preferable set of colors and can be dealt with more severe editing even if it has lost some of the quality and details. The RGB image file is constituted with those three primary colors which are represented by one byte

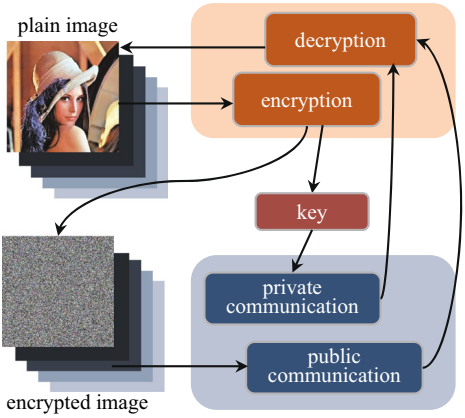


**Fig. 2** Structure of the color image encryption and decryption process

respectively, and each pixel is made up of those three bytes. Figure 3 shows that overwriting each pixel value in one color channel by implementing a proposed algorithm or method with some intended functions. That means, once the value of each pixel have been changed, a encrypted image will be obtained.

At issue here is how to encrypt RGB image files and how to design the effective method. Settle on designing the encryption method that is effective and proper for any RGB images, we therefore propose an image encryption method based on Chaotic Coyote Optimization Algorithm (CCOA) (see Section 3) and its pseudocode for encryption is shown in Algorithm 2, and the decryption is the inverse process of encryption. Contrary to image encryption, we are given the best coyote's social conditions, which is the best encryption solution, and are asked to be in accordance with the rules to find its original image. The complete method consists of all operations and strategies in CCOA. Splitting the original RGB image into three parts, that is, red, green, blue channels which will be encrypted respectively, and then initializing the CCOA by using the size of color channel. In each iteration, the alpha will be selected, and the social tendency of each pack will be calculated. Then, generating the key for image encryption with values of coyote's social condition, and updating the best solution by comparing the fitness value of each coyote. And, accordingly, the cipher image can be restored to its original pixels using the key generated in decryption procedure, which is the same as the one used in the process of encryption, generated in decryption procedure.

### 4.2 Color image Steganography method based on CCOA (ST-CCOA)

Embedding the data into the color image file that is as cover object is known as color image Steganography. Taking into consideration a large quantity of bits exist in the digital representation of an color image, image files are popularly used cover source. In addition, numerous ways are available to hide information inside a cover object, e.g. encrypt and scatter, redundant pattern encoding, masking and filtering, coding and cosine transformation, and least significant bit insertion.

As described in Section 4.1, the 24 bit color depth image is 3 bytes per pixel, and from this, those bytes can be overwrote to hide other data. One attention-grabbing way is the use of least significant bit (LSB) of pixels in the image to store the specific sections or all of

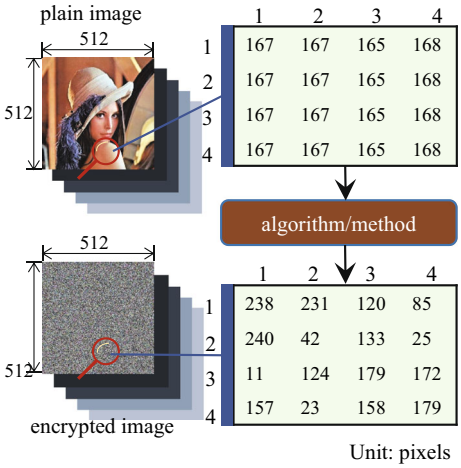


**Fig. 3** Schematic diagram of image encryption

**Algorithm 2** EN-CCOA.

```
input  : im: image file, population each pack, number of packs,
         maximum total population
output : encrypted image: E
im ← read(im.filename);
// im.matrix is M-by-N, contains pixel values
foreach coyote do
    coyote.social(1) ← random ∈ [1, im.size];
    coyote.social(2) ← ⌈coyote.social(1)/M⌉;
    c ← coy.social(1) mod N;
    if c = 0 then c ← N;
    key ← keyGet (coyote.social(2), c);
    coyote.matrix ← Encry (im.matrix, key);
    calculate fitness value;
repeat
    foreach pack do
        select alpha (4);
        work out social tendency (5);
        foreach coyote in this pack do
            coyote.social ← (12);
            c ← coyote.social(1) mod N;
            if c = 0 then c ← N;
            key ← keyGet (coyote.social(2), c);
            O ← Encry (coyote.matrix, key);
            coyote.matrix ← O;
            calculate fitness value;
        this pack ← call Life in Alg. 1;
    reassign packs ← call Exchange in Alg. 1;
    update global best E;
until greater than maximum total population;
def keyGet (row, column):
    [r, c] ← binary(row,column);
    key ← concatenate r and c;
    return key;
def Encry (matrix G, key): // G is M − by − N
    len ← length of key;
    x ← 1/2^len × (∑_{i=1}^{len} key(i) × 2^{len−i});
    foreach e in G do
        H(e) ← bitxor(⌊x × 256⌋, G(e));
        x ← 4 × (x − x^2);
    return H;
```

the secret information [24, 32, 33]. LSB means those bits which are at rightmost of a binary number. In one case, the binary code of decimal number 16 is “00010000”, whose LSB is ‘0’. After replacing ‘0’ with ‘1’, the decimal 17 that the binary of which is “00010001” can be got eventually. In such manner, hiding of secret messages inside of a carrier file is simpler and effective whilst building a same image as before.

When we talking about secret file, it could be audio files in Healthcare as a data collection method, or image transmission via smartphone on social media platform, or text files of any website that can communicate information [30]. Almost all types of those files and their uses have enhanced day-to-day quality of life for all netizens.

A image Steganography method based on Chaotic Coyote Optimization Algorithm (ST-CCOA) is proposed here. During the stage of design, we are considering the strategy for reducing the possibility of arranging multiple content in same location of the cover image, which would get the algorithm nowhere with the unbearable response time, only taking up precious time. As we conduct further research on CCOA, the (10) and (11) are rewritten with two acceleration factors, $\nu_1$ and $\nu_2$, which are used to stop avoiding wasting a lot of time selecting the location for hiding the secret messages and realize the acceleration of convergence. Thus,those two new equations are,

$$\lambda_1 = \nu_1 \times Alpha^{p,t} - S_{c_1}^{p,t}, \tag{15}$$

$$\lambda_2 = \nu_2 \times Q^{p,t} - S_{c_2}^{p,t}, \tag{16}$$

where, $c_1$ and $c_2$ are the random coyotes that are belong to $p$th pack in the $t$th instant of time, $\nu_1$ and $\nu_2$ are factors used to avoid the complex of computing too large and make the convergence much faster.

In this method, the initial value of those two factors being 200 straightaway decided on some comparison tests which shows it takes the least time. It is also worth pointing out that

$$\nu_1 = \nu_1 + 200, \tag{17}$$

$$\nu_2 = \nu_2 + 200. \tag{18}$$

The proposed ST-CCOA method obtains the best solution of optimization problem after 5032 iterations for lack of this strategy, however, the optimal solution requires 342 iterations to be stabilized by applying those two acceleration factors.

The flow chart of ST-CCOA is presented in Fig. 4 for describing more details and steps of hiding data. The input elements contain a digital image as cover object, a secret file as host object, number of bits embedded via LSB, and some parameters for running CCOA algorithm. Often, the secret file that supports several different types is serialized as binary stream which is always more easier to process image Steganography than others. In the ST-CCOA method, all parts of CCOA are used, and what's more, the new strategy takes aim at reducing computing time and quickening the speed of convergence is applied, which has been introduced above. First, we use one channel of a RGB color image, and divide the bitstream of the secret image into three parts. Next, we select the best coyote as the alpha in each pack using (4) and calculate the cultural tendency using (5). Then, we compute the location of hiding by implementing the substitute strategy in the Fig. 4. After this part of the bitstream has been hidden, we use (12), (15), and (16) to update the social conditions of coyotes and apply the birth and death process. When all packs use the steps as above, we reassign packs by using exchange strategy and update the global optimal solution. Finally, the results are combined to obtain the embedded image after repeating the above steps for all parts of the cover color image and the secret color image.

## 5 Simulation results

In this section, simulation experiments have been completed for the validation of the proposed EN-CCOA and ST-CCOA methods. Five standard test images are taken, including the 512 × 512 Color Airplane (F-16), the 512 × 512 Color House, the 512 × 512 Color Lena, the

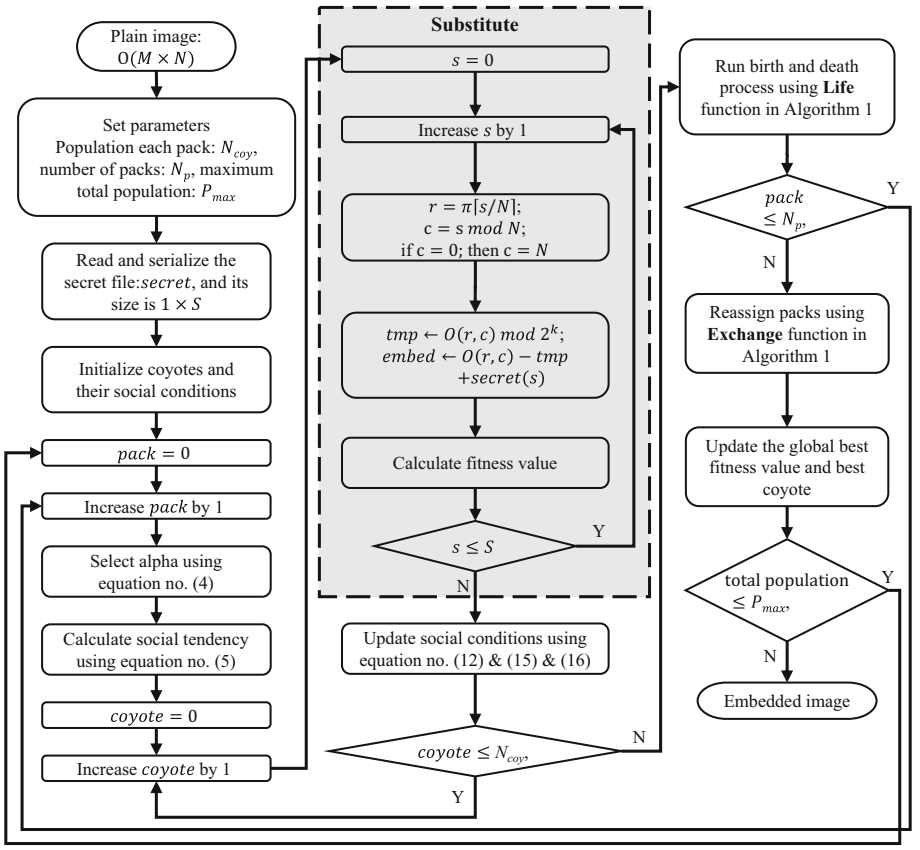


**Fig. 4** Flow chart of proposed ST-CCOA method

512 × 512 Color Mandrill (a.k.a. Baboon), and the 512 × 512 Color Peppers. In addition, the 256 × 256 Grayscale Clock is used as the secret file in the image Steganography scheme. All evaluation metrics employed are explained and their mathematical formulas are expressed. To present the simulation data more effective, that is, for organizing the right data at proper form with tables, we take the average of the red, green, blue components when calculating evaluation metrics to do a great job of filling rational need for quantifiable information.

### 5.1 EN-CCOA

With a focus on the perform in image encryption, three comparison algorithms or methods are implemented in this part, including Particle Swarm Optimization (PSO), Genetic Algorithm (GA), and Chaotic maps. Five comparison approaches are used to analyze the statistical characteristics of encrypted images,

In our simulation, the statistical term named correlation coefficient (CCF) is chosen as fitness function, greater value indicates the correlation between pixel values is stronger, and

CCF $\in [-1, 1]$, which is defined as below, where $A$ and $B$ are images, $\bar{A}$ and $\bar{B}$ are the mean of $A$ and $B$, respectively.

$$\mathrm{CCF} = \frac{\sum_m \sum_n (A_{mn} - \bar{A})(B_{mn} - \bar{B})}{\sqrt{\left(\sum_m \sum_n (A_{mn} - \bar{A})^2\right)\left(\sum_m \sum_n (B_{mn} - \bar{B})^2\right)}}, \tag{19}$$

where, $A_{mn}$ and $B_{mn}$ represent the pixel value of the image $A$ and $B$ in row $m$ and column $n$, respectively.

The effectiveness of setting parameters is essential to be enhanced for executing an algorithm, and therefore, some simulations have been done in the pretreatment. In our case, we choose 20 as the the number of packs and 15 as the number of coyotes in each pack according to experience. During the simulation, it is apparent that the fitness value is satisfactory enough after 44 iterations, and the best solution will be collected after 306 iterations. Considering the running time of the algorithm, the number of iterations in our simulations is 44, that is, the maximum population is 5260. The reason to set that number, the fitness value would not change significantly, even if the total population of coyotes increase greatly after it reaches 5260. Once the maximum population and the number of packs are determined, in order to improve the performance of our method, the number of coyotes in each pack is set to 20 according to the curve of fitness values. Depending on the above-mentioned tests and some literature, we supplied the specific parameters for simulations as the Table 1 shows.

From the Fig. 5, we can see that all five standard test images are encrypted by using the proposed EN-CCOA method and then decrypted successfully. The simulation displays the value of CCF among adjacent pixels in all five test images and its cipher images in Table 2. The mean values are close to 0 and even are negative numbers, which suggests that the points are distributed randomly on the whole space of the cipher images and its correlations are removed sufficiently. Meanwhile, the comparison results of correlation coefficients of other image encryption methods are also listed in Table 2, which also are fitness values for optimizing the process of image encryption. It can be observed the proposed EN-CCOA has a significant better performance than others in view of the CCF. The mean value of CCF of EN-CCOA is -0.0042, the mean value of CCF of the method in [2] based on PSO is 0.0061, the method based on GA algorithm's mean CCF value is 0.0467, and the mean value of the approach combining GA algorithm and chaotic maps is -0.0001 on the CCF index. Through these data, we can see that the EN-CCOA resulted in the lowest value means higher randomness, that is, it can effectively reduce the correlation of adjacent pixels in the original image.

In order to measure the amount of information in a digital image, information entropy is used that is an common and effective test criteria. It can be calculated as:

$$H(O) = \sum_{i=0}^{2^n-1} p(o_i) \log_2\left(\frac{1}{p(o_i)}\right), \tag{20}$$

where, $O$ is an image, $n$ is the number of bits per pixel, and $p(o_i)$ is the probability of the symbol $o_i$ in image $O$. Here, RGB image is used for test, so that $n = 8$ in each component and the theoretical value of $H(O)$ is 8.

The information entropy of the plain and cipher image are computed and have been tabulated in Table 2. It is reported that the obtained cipher images are just like random signals, according to the value of information entropy in all five tested images are very close to 8.In addition, the information entropy values obtained by applying other methods are also

**Table 1** Experiment sets for image encryption

| Algorithm | Item | Value |
|---|---|---|
| EN-CCOA | number of coyotes each pack | 20 |
| | number of packs | 20 |
| | maximum number of iterations | 44 |
| | initial value of chaotic map | 0.3 |
| GA | population size | 100 |
| | parent number | 50 |
| | mutation rate | 0.1 |
| | maximum number of generations | 100 |
| Ref. [2] | population size | 20 |
| | inertia weight | 1 |
| | inertia weight damping ratio | 0.99 |
| | personal learning coefficient | 1.5 |
| | global learning coefficient | 2 |
| | maximum number of iterations | 50 |
| Ref. [12] | the control parameters $a, b, c$ of Chen's chaotic map | 35,3,28 |
| | initial value of primary values $X_0$, $Y_0$, $Z_0$ of Chen's chaotic map | -9,-5,14 |
| | population size | 80 |
| | parent number | 40 |
| | mutation rate | 0.1 |
| | maximum number of generations | 100 |


**Fig. 5** Encryption and decryption simulation results of the proposed EN-CCOA method. 1(a)-5(a) are the original images, 1(b)-5(b) are the ciphered images,1(c)-5(c) are the decrypted images

**Table 2** Comparison of correlation coefficients (CCF) and information entropy with other methods

| Image | Ref. [2] | | GA | | Ref. [12] | | EN-CCOA | |
|---|---|---|---|---|---|---|---|---|
| | CCF | Entropy | CCF | Entropy | CCF | Entropy | CCF | Entropy |
| airplane | 0.0009 | 7.9993 | 0.0439 | 7.9542 | 0.0017 | 7.9989 | 0.0005 | 7.9993 |
| house | 0.0270 | 7.9934 | 0.0536 | 7.9850 | 0.0004 | 7.9987 | −0.0 028 | 7.9993 |
| lena | −0.0081 | 7.9993 | 0.0577 | 7.9949 | −0.0003 | 7.9990 | −0.0087 | 7.9994 |
| mandrill | 0.0130 | 7.9929 | 0.0342 | 7.9794 | −0.0001 | 7.9986 | 0.0039 | 7.9993 |
| peppers | −0.0024 | 7.9993 | 0.0440 | 7.9844 | −0.0020 | 7.9992 | −0.0141 | 7.9993 |
| Mean | 0.0061 | 7.9968 | 0.0467 | 7.9796 | −0.0001 | 7.9989 | −0.0042 | 7.9993 |

shown in Table 2. From the data, the average information entropy of PSO, GA, the method integrating GA and chaotic map, and EN-CCOA are 7.9968, 7.9796, 7.9989, and 7.9993, respectively. The results also reveal the proposed EN-CCOA method is more effective than others.

It is true that system sensitivity is a vital security valuation aspect of image schemes performance. Number of pixels change rate (NPCR) and Unified average changing intensity (UACI) are two sensitivity evaluation indexes widely used to analyze algorithms [45, 48], which focus on figuring out the difference between two images of same dimensions. The equation of NPCR is written as follows:

$$\mathrm{NPCR} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} D(i, j) \times 100\%, \tag{21}$$

where, $M$ and $N$ denote the size of image file, the term $D(i, j)$ is defined for referring to the relationships between two pixels, seen in (22). $\boldsymbol{O}_1$ and $\boldsymbol{O}_2$ are images.

$$D(i, j) = \begin{cases} 1, & \boldsymbol{O}_1(i, j) \neq \boldsymbol{O}_2(i, j) \\ 0, & \boldsymbol{O}_1(i, j) = \boldsymbol{O}_2(i, j) \end{cases}. \tag{22}$$

For expressing UACI, it is formulated in the following form, where, $\boldsymbol{O}_1$ and $\boldsymbol{O}_2$ are images with a size of $M \times N$.

$$\mathrm{UACI} = \frac{100\%}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{\|\boldsymbol{O}_1(i, j) - \boldsymbol{O}_2(i, j)\|}{255}. \tag{23}$$

The NPCR and UACI scores of each method in the simulation experiments are recorded in the Table 3, which provide the evident that our method obviously performs best on image encryption and decryption. It is well known that the ideal value of NPCR is 99.9064% and the theoretical value of UACI is 33.4635% [48]. The proposed EN-CCOA method scored higher than other methods both NPCR and UACI, that is 99.60% and 31.74%.

In an image, counting the number of pixels per pixel is involved in the analysis of histogram which indicates image's randomness content and firms the encryption method offers the satisfactory cipher images. In general, pixels values are distributed evenly in an cipher image that means encryption scheme performs effectively [2, 41]. The histogram of the original Airplane image and its corresponding cipher are shown in Fig. 6, and it is clear that the pixels

**Table 3** NPCR and UACI scores by different encryption methods

| Image | Ref. [2] | | GA | | Ref. [12] | | EN-CCOA | |
|---|---|---|---|---|---|---|---|---|
| | NPCR | UACI | NPCR | UACI | NPCR | UACI | NPCR | UACI |
| airplane | 99.61% | 32.65% | 96.17% | 31.11% | 99.52% | 32.31% | 99.61% | 32.67% |
| house | 98.45% | 29.99% | 96.05% | 28.48% | 99.51% | 31.28% | 99.60% | 30.97% |
| lena | 99.62% | 32.79% | 96.14% | 30.43% | 99.57% | 32.35% | 99.62% | 32.79% |
| mandrill | 98.45% | 28.78% | 96.10% | 26.86% | 99.56% | 30.16% | 99.56% | 29.90% |
| peppers | 99.61% | 32.26% | 96.10% | 30.06% | 99.55% | 29.36% | 99.61% | 32.35% |
| Mean | 99.15% | 31.30% | 96.11% | 29.39% | 99.54% | 31.09% | 99.60% | 31.74% |

of cipher image from all component are scattered. That is, the cipher Airplane image obtained by the proposed method has the ability to resist statistical attacks [42].

To test the capacity for preventing attacks of the cipher image four common attacks are used on the standard test image named airplane, and its result are listed in Table 4. The proposed EN-CCOA method performs better than others for Gaussian, and all methods perform at about the same level for Speckle, Poisson noise, and Salt & pepper noise.As shown in Fig. 7, 1(a) is the noisy image obtained by Speckle noise with mean = 0 and variance = 0.05; 2(a) is the noisy image obtained by Gaussian noise with mean = 0 and variance = 0.01; 3(a) is the noisy image obtained by Salt and pepper noise with density = 0.3; 4(a) is the noisy image obtained by Poisson noise with mean = 10; and 1(b) is the decrypted image of 1(a); 2(b) is the decrypted image of 2(a); 3(b) is the decrypted image of 3(a); and 4(b) is the decrypted image of 4(a). Altogether, combining those data and the analysis of Fig. 7, it is obviously that the proposed method can against those attacks effectively.

In summary, we quantify the color image encryption performance using five metrics and the four common attacks, and the results indicate that our proposed EN-CCOA method has the best performance.

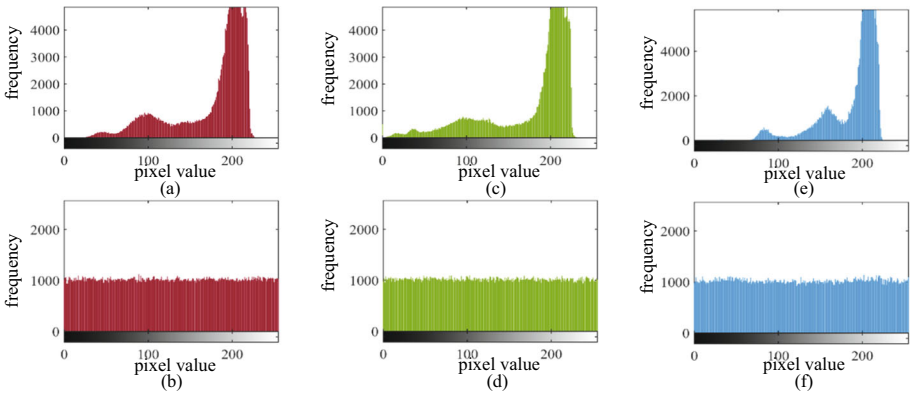


**Fig. 6** Histograms of the plain color image named Airplane and its cipher image.(a) Red component of the plain image, (b) Red component of the cipher image, (c) Green component of the plain image, (d) Green component of the cipher image, (e) Blue component of the plain image, (f) Blue component of the cipher image

**Table 4** Results of attacks for Airplane (512 × 512)

| Attack | Ref. [2] | GA | Ref. [12] | EN-CCOA |
|---|---|---|---|---|
| Speckle noise | 0.9280 | 0.9280 | 0.9282 | 0.9278 |
| Gaussian noise | 0.9392 | 0.9394 | 0.9389 | 0.9396 |
| Salt & pepper noise | 0.9484 | 0.9474 | 0.9480 | 0.9474 |
| Poisson noise | 0.9780 | 0.9782 | 0.9783 | 0.9781 |

### 5.2 ST-CCOA

Understanding a optimization problem's structure and objective is the most important step that is also complex for getting a firm handle on. The fitness function of an image Steganography focus predominantly on two aspects: how to render the cover image low distortion and meanwhile make robustness higher [13]. Like other popular researches, we use peak signal-to-noise ratio (PSNR) and structural similarity (SSIM) index. What's more, PSNR and SSIM are combined in our fitness function serviced for the proposed ST-CCOA to calculate the fitness value in each iteration.

First, when addressing picture processing, PSNR metric provides a decibel value to evaluate the difference between two images, and its numerical value can be obtained by computing the ratio of the image's maximum possible power to the mean square error (MSE) [13, 15, 32]. The larger the PSNR, the better the quality of the cipher image obtained via corresponding image encryption method. And, it is easy to understand that the related definitions are:

$$\mathrm{MSE} = \frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}[\boldsymbol{O_1}(i,j) - \boldsymbol{O_2}(i,j)]^2, \tag{24}$$

$$\mathrm{PSNR} = 10log_{10}(peakval^2\mathrm{MSE}(\boldsymbol{O}_1, \boldsymbol{O}_2)), \tag{25}$$

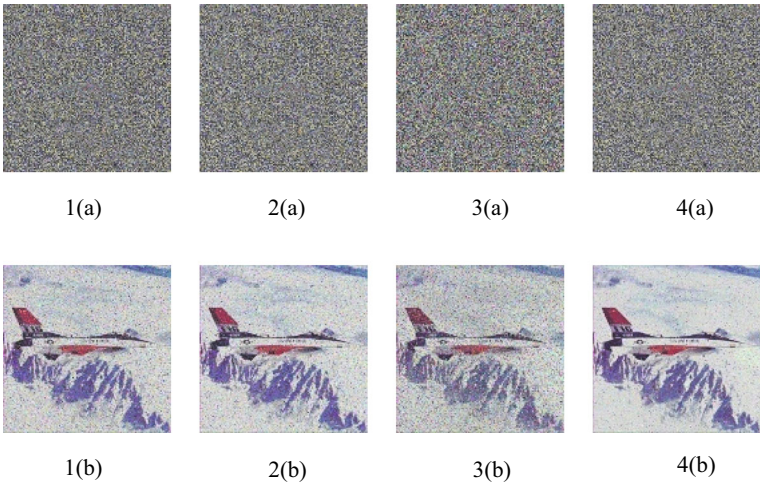


**Fig. 7** Attack results of the proposed image encryption method. 1(a)-4(a) are the noisy images acquired with some noise, and 1(b)-4(b) are the corresponding decrypted images

in which, $\boldsymbol{O_1}$ and $\boldsymbol{O_2}$ are $M \times N$ images, and $peakval$ is taken from the range of the image data type, i.e., for unit8, $peakval$ is $2^8 - 1 = 255$.

In this paper, we use the standard test images displayed in RGB color model, not like the grayscale-based encryption method contains only one color channel, so that providing the mean of PSNR as a evaluation index, as follows:

$$\text{MPSNR} = \frac{1}{M}\sum_{j=1}^{M}\text{PSNR}(\boldsymbol{O}_{1_j}, \boldsymbol{O}_{2_j}), \tag{26}$$

in which, $M$ is the number of the color channels, that is equals 3 in our simulations.

Second, the SSIM is widely used for measuring image perceived quality, that is, the similarity between the original image and the embedded image. The formulas for computing SSIM, are given below in details.

$$\text{SSIM} = l^{\alpha} \times c^{\beta} \times s^{\gamma}, \tag{27}$$

$$l = \frac{2\mu_{O_1}\mu_{O_2} + C_1}{\mu_{O_1}^2 + \mu_{O_2}^2 + C_1}, \tag{28}$$

$$c = \frac{2\sigma_{O_1}\sigma_{O_2} + C_2}{\sigma_{O_1}^2 + \sigma_{O_2}^2 + C_2}, \tag{29}$$

$$s = \frac{2\sigma_{O_1O_2} + C_3}{\sigma_{O_1}\sigma_{O_2} + C_3}, \tag{30}$$

where, $\boldsymbol{O_1}$ and $\boldsymbol{O_2}$ are images used in this operation, $\mu_{O_1}$ and $\mu_{O_2}$ are the statistical mean of pixels in those two images, $\sigma_{O_1}$ and $\sigma_{O_2}$ are the standard deviations, $\sigma_{O_1O_2}$ is the cross-covariance for images, $C_1$ and $C_2$ are constants avoid the statistical mean or standard deviations is very close to zero, and $C_3 = C_2/2$ is set as default. To make the expression of SSIM simpler, we set $\alpha$, $\beta$, and $\gamma$ to 1 [13, 32, 43].

Therefore, the specific form of SSIM is

$$\begin{aligned}\text{SSIM} &= l \times c \times s \\ &= \frac{(2\mu_{O_1}\mu_{O_2} + C_1)(2\sigma_{O_1O_2} + C_2)}{(\mu_{O_1}^2 + \mu_{O_2}^2 + C_1)(\sigma_{O_1}^2 + \sigma_{O_2}^2 + C_2)},\end{aligned} \tag{31}$$

and the range of it is [0,1]. When the value of SSIM is 1, it indicates that those two images are completely the same.

In practice,for evaluating the entire multi-dimensional image quality, we use the mean SSIM (MSSIM) index which is calculated by the following formula:

$$\text{MSSIM} = \frac{1}{M}\sum_{j=1}^{M}\text{SSIM}(\boldsymbol{O}_{1_j}, \boldsymbol{O}_{2_j}), \tag{32}$$

in which, $M$ is the number of color channels in the object image, $\boldsymbol{O}_{1_j}$ and $\boldsymbol{O}_{2_j}$ represent the $j$th color channel of the image $\boldsymbol{O}_1$ and $\boldsymbol{O}_2$, respectively. As mentioned earlier, the value is taken as 3 for $M$ in RGB image processing.

Finally, MPSNR and MSSIM are mixed together [13] to make a new function as the fitness function in the proposed ST-CCOA. That is,

$$\text{Fitness} = \delta \times (\text{MPSNR}/100) + (1 - \delta) \times \text{MSSIM}, \tag{33}$$

where, $\delta$ is the weight constant, and it euqals 0.5. During the execution of ST-CCOA method, each candidate solution generated as input is taken by the fitness function, and then it produces a fitness value as output to appraise how "good" the solution is with respect to the problem in consideration.

Based on LSB (see Section 4.2), five standard test RGB images as cover images are implemented our method to hide the bitstream of the secret file. And as same as the pretreatment in Section 5.1, some experiments have been set up to determine the parameters for running our proposed method ST-CCOA in image Steganography. In this case, we select 20 as the the number of packs and 15 as the number of coyotes in each pack according to experience. The fitness value is acceptable after 14 iterations, meanwhile, the best value of fitness is obtained after 342 iterations. Taking into account the algorithm speed the number of iterations is set to 14 in this proposed method, and the maximum population is set to 3060. In addition, on this basis, the number of coyotes is set to 15 according to the experiments results. The parameters which are required for running our proposed method ST-CCOA based on CCOA are listed in Table 5.

According to the simulation results, the illustrations of cover color images, secret color images, the embedded images and the extracted images are shown in Fig. 8. Meanwhile, Table 6 gives the PSNR and SSIM results after excuting the compared algorithms and our proposed method. It can be seen from the data that the ST-CCOA method has larger PSNR and SSIM results and greater security level. The values of PSNR of ST-CCOA method are all above 48 dB, by contrast, the methods based on PSO, CS, and GA algorithm obtain the lower values of PSNR and SSIM. What's more, the results of the fitness values are also tabled in Table 6, where five different standard test images were used for comparison with other

**Table 5** Experiment sets for image Steganography

| Algorithm | Item | Value |
|---|---|---|
| ST-CCOA | number of coyotes each pack | 15 |
| | number of packs | 20 |
| | maximum number of iterations | 14 |
| | initial value of chaotic map | 0.3 |
| GA | population size | 100 |
| | parent number | 50 |
| | mutation rate | 0.1 |
| | maximum number of generations | 100 |
| | minimal cost | 1.0E-6 |
| PSO | population size | 20 |
| | inertia weight | 1 |
| | inertia weight damping ratio | 0.99 |
| | personal learning coefficient | 1.5 |
| | global learning coefficient | 2 |
| | maximum number of iterations | 20 |
| CS [13] | number of nests | 20 |
| | probability of building a new nest | 0.25 |
| | maximum number of iterations | 20 |

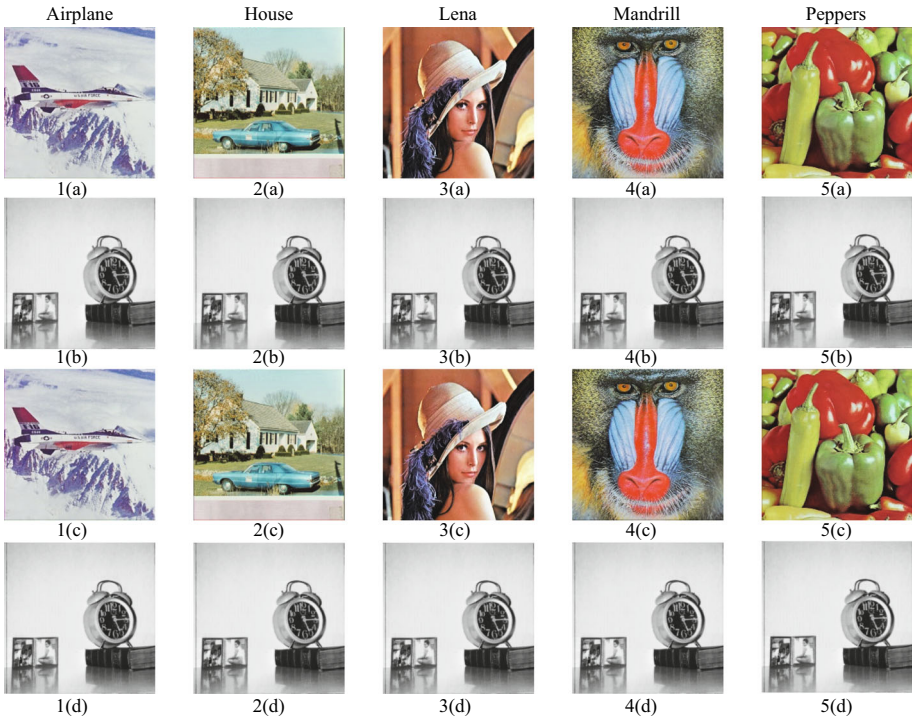


**Fig. 8** Five standard test images and their corresponding marked version utilizing the proposed ST-CCOA approach. 1(a)-5(a) are the original images, 1(b)-5(b) are the secret images, 1(c)-5(c) are the embedded images, 1(d)-5(d) are the extracted images

methods. The average PSNR values of PSO, CS, GA, and ST-CCOA are 43.2954, 43.2957, 43.2348, and 48.1125, respectively. For the SSIM metric, the results of these methods are 0.9810, 0.9810, 0.9806, and 0.9937. According to the analysis, there is no doubt that the proposed ST-CCOA method exhibits better performance than PSO, CS, and GA for all standard test images.

During the process of transmission, the embedded image can be damaged or corrupt, therefore, we arrange some attacks to validate the performance of the ST-CCOA method in the simulation, including crop, Salt and pepper, Gaussian, and Speckle noise. The property index of those attacked images are listed in Table 7. And in Fig. 9, 1(a) is the Stego image with 1/16 data loss at the top-left corner; 2(a) is the noisy image that is produced by Salt and pepper noise with density $= 0.05$; 3(a) is the noisy image produced by Gaussian noise with mean $= 0$ and variance $= 0.000001$; 4(a) is the noisy image produced by Speckle noise with mean $= 0$ and variance $= 0.000003$; and 1(b) is the secret image extracted from 1(a); 2(b) is the secret image extracted from 2(a); 3(b) is the secret image extracted from 3(a); 4(b) is the secret image extracted from 4(a). From Table 7, PSNR values are calculated between the secret image named Clock and the extracted image and are larger than 14 dB. Additionally, the PSNR value is 20.73 dB, the SSIM value is 0.4686, and the fitness value is 0.3379 for Salt and pepper noise. It is delightful that the recovered image is still legible in Fig. 9. In the meantime, PSO method performs better than ST-CCOA for crop and Speckle noise; the CS method resists better than ST-CCOA for crop attack; and GA approach has poor performance for Gaussian and Speckle noise. All those data reports the evidence that

**Table 6** PSNR, SSIM and fitness value results for different images

| Image | ST-CCOA | | | PSO | | | CS [13] | | | GA | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | PSNR | SSIM | Fitness | PSNR | SSIM | Fitness | PSNR | SSIM | Fitness | PSNR | 'SSIM | Fitness |
| airplane | 48.1294 | 0.9913 | 0.7363 | 43.2973 | 0.9744 | 0.7037 | 43.2960 | 0.9744 | 0.7037 | 43.2393 | 0.9740 | 0.7032 |
| house | 48.1202 | 0.9939 | 0.7376 | 43.3161 | 0.9826 | 0.7079 | 43.3217 | 0.9826 | 0.7079 | 43.2681 | 0.9823 | 0.7075 |
| lena | 48.1391 | 0.9930 | 0.7372 | 43.3176 | 0.9793 | 0.7062 | 43.3151 | 0.9793 | 0.7062 | 43.2568 | 0.9789 | 0.7057 |
| mandrill | 48.1359 | 0.9977 | 0.7395 | 43.3200 | 0.9931 | 0.7131 | 43.3226 | 0.9931 | 0.7131 | 43.2557 | 0.9929 | 0.7127 |
| peppers | 48.0378 | 0.9924 | 0.7364 | 43.2258 | 0.9755 | 0.7039 | 43.2233 | 0.9755 | 0.7039 | 43.1540 | 0.9750 | 0.7033 |
| **Mean** | 48.1125 | 0.9937 | 0.7374 | 43.2954 | 0.9810 | 0.7070 | 43.2957 | 0.9810 | 0.7070 | 43.2348 | 0.9806 | 0.7065 |

**Table 7** Results of attacks for Airplane (512 × 512)

| Attack | | Crop | Salt& pepper noise | Gaussian noise | Speckle noise |
|---|---|---|---|---|---|
| ST-CCOA | PSNR | 17.3038 | 20.7320 | 19.2345 | 14.2138 |
| | SSIM | 0.3306 | 0.4686 | 0.3530 | 0.1649 |
| | Fitness | 0.2518 | 0.3379 | 0.2727 | 0.1535 |
| PSO | PSNR | 17.6041 | 20.8268 | 18.8510 | 14.2058 |
| | SSIM | 0.3334 | 0.4671 | 0.3366 | 0.1657 |
| | Fitness | 0.2547 | 0.3377 | 0.2626 | 0.1539 |
| CS [13] | PSNR | 17.5500 | 20.7100 | 18.9981 | 14.2151 |
| | SSIM | 0.3336 | 0.4647 | 0.3448 | 0.1642 |
| | Fitness | 0.2546 | 0.3359 | 0.2674 | 0.1532 |
| GA | PSNR | 17.5501 | 20.7337 | 18.8651 | 14.3186 |
| | SSIM | 0.3396 | 0.4695 | 0.3381 | 0.1644 |
| | Fitness | 0.2575 | 0.3384 | 0.2634 | 0.1529 |

the proposed ST-CCOA method has appealing performance to resist attacks, even it is no better than other methods on the whole.

## 6 Conclusion

This work contributes to existing knowledge of image processing and information security by presenting EN-CCOA and ST-CCOA methods, which are designed on basis of the Chaotic Coyote Optimization Algorithm (CCOA). And in the process of image encryption, the key

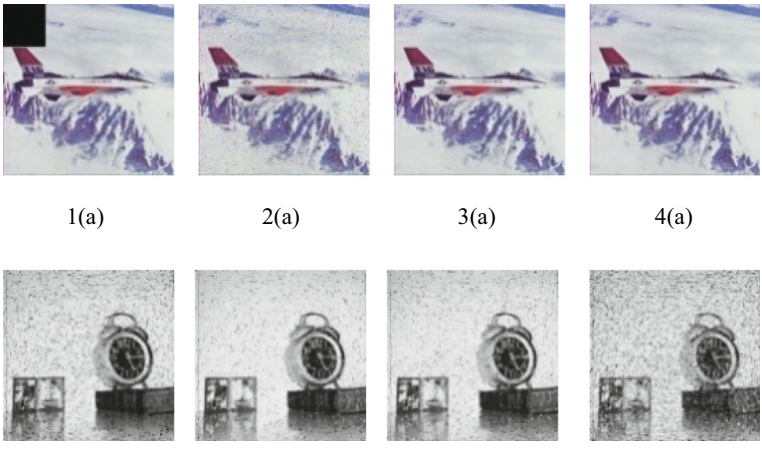


**Fig. 9** Attack results of the proposed ST-CCOA method.1(a)-4(a) are the images being attacked, and 1(b)-4(b) are the secret images extracted from the corresponding images

is generated and optimized with the efficient mechanisms of CCOA, which is composed of the social condition update, birth and death, and migration strategies. So that being put it into practice sufficient, the corresponding simulation results express the high sensitivity and security of EN-CCOA method. By making compromise between the running time and the performance, we find that the maximum number of iterations should be set to 44 in our case. In the meanwhile, for executing the ST-CCOA more effectively, the specific locations of embedding are selected and then optimized with the CCOA and our designed strategy, which contains two acceleration factors has the capability to reduce the response time in selecting location for the color image Steganography. That is, the convergence speed of the ST-CCOA is more increased with the aid of our designed strategy. Based on some comparison tests for reducing the run time, we set the initial value of the designed strategy to 200. Then, the maximum number of iterations is set to 14 to achieve a compromise between the run time and high performance in our case. Once the locations are determined in the cover image, the bitstream of the secret image file is embedded according to the optimization solution. The results show that the proposed ST-CCOA method is effective and accomplishes the state of the art performance. Moreover, the image attack tests have been done in the simulation experiment, which demonstrate that the ability to defend against attack is also contained in both of our two methods.

In other words, the proposed EN-CCOA and ST-CCOA methods produce reliable results and warrant a broad generalizability for some special goals. For future works, we will focus on improving the robustness of those two methods for resisting more serious occasional attacks in communication process. The possible further improvements that may be achieved by making some adjustment in algorithm structure. And we may consider extending the proposed scheme and the enhanced algorithm to other applications in the area of wireless communications.

**Acknowledgements** This document is the results of the research project funded by the National Key Research and Development Program of China under Contract No. 2016YFE0200200, Postgraduate Research & Practice Innovation Program of Jiangsu Province No. KYCX22_0937, the National Natural Science Funds of China under Contract No. 61701253 and 61801240.

## Declarations

All authors certify that they have no affiliations with or involvement in any organization or entity with any financial interest or non-financial interest in the subject matter or materials discussed in this manuscript.

## References

1. Abd El-Latif AA, Abd-El-Atty B, Hossain MS, Rahman MA, Alamri A, Gupta BB (2018) Efficient Quantum Information Hiding for Remote Medical Image Sharing. IEEE access?: practical innovations, open solutions 6:21075–21083. https://doi.org/10.1109/ACCESS.2018.2820603
2. Ahmad M, Alam M, Umayya Z, Khan S, Ahmad F (2018) An image encryption approach using particle swarm optimization and chaotic map. International Journal of Information Technology 10. https://doi.org/10.1007/s41870-018-0099-y
3. Alawida M, Samsudin A, Teh JS, Alkhawaldeh RS (2019) A new hybrid digital chaotic system with applications in image encryption. Signal Processing 160:45–58. https://doi.org/10.1016/j.sigpro.2019.02016
4. Atawneh S, Almomani A, Al Bazar H, Sumari P, Gupta B (2017) Secure and Imperceptible Digital Image Steganographic Algorithm Based on Diamond Encoding in DWT Domain. Multimedia Tools and Applications 76(18):18451–18472. https://doi.org/10.1007/s11042-016-3930-0
5. Bala Krishnan R, Rajesh Kumar N, Raajan NR, Manikandan G, Srinivasan A, Narasimhan D (2022) An Approach for Attaining Content Confidentiality on Medical Images Through Image Encryption with

Steganography. Wireless Personal Communications 127(2):979–995. https://doi.org/10.1007/s11277-021-08477-1
6. Boroumand M, Chen M, Fridrich J (2019) Deep Residual Network for Steganalysis of Digital Images. IEEE Transactions on Information Forensics and Security 14(5):1181–1193. https://doi.org/10.1109/TIFS.2018.2871749
7. Chai X, Fu X, Gan Z, Lu Y, Chen Y (2019) A color image cryptosystem based on dynamic DNA encryption and chaos. Signal Processing 155:44–62. https://doi.org/10.1016/j.sigpro.2018.09.029
8. Chuman T, Sirichotedumrong W, Kiya H (2019) Encryption-Then-Compression Systems Using Grayscale-Based Image Encryption for JPEG Images. IEEE Transactions on Information Forensics and Security 14(6):1515–1525. https://doi.org/10.1109/TIFS.2018.2881677
9. Dalal M, Juneja M (2021) Steganography and Steganalysis (in digital forensics): a Cybersecurity guide. Multimedia Tools and Applications 80(4):5723–5771. https://doi.org/10.1007/s11042-020-09929-9
10. Divya CD, Gururaj HL, Rohan R, Bhagyalakshmi V, Rashmi HA, Domnick A, Flammini F (2021) An Efficient Machine Learning Approach to Nephrology through Iris Recognition. Discover Artificial Intelligence 1(1):10. https://doi.org/10.1007/s44163-021-00010-4
11. El-Samie FEA, Ahmed HEH, Elashry IF, Shahieen MH, Faragallah OS, El-Rabaie E-SM, Alshebeili SA (2013) Image Encryption: A Communication Perspective, 1st edn. CRC Press, Boca Raton
12. Ghazvini M, Mirzadi M, Parvar N (2020) A modified method for image encryption based on chaotic map and genetic algorithm. Multimedia Tools and Applications 79(37):26927–26950. https://doi.org/10.1007/s11042-020-09058-3
13. Gupta A, Chaudhary A (2018) A metaheuristic method to hide MP3 sound in JPEG image. Neural Computing and Applications 30(5):1611–1618. https://doi.org/10.1007/s00521-016-2759-9
14. Hua Z, Zhou Y, Huang H (2019) Cosine-transform-based chaotic system for image encryption. Information Sciences 480:403–419. https://doi.org/10.1016/j.ins.2018.12.048
15. Hussain M, Wahab AWA, Idris YIB, Ho ATS, Jung K-H (2018) Image steganography in spatial domain: A survey. Signal Processing: Image Communication 65:46–66. https://doi.org/10.1016/j.image.2018.03.012
16. Itier V, Puteaux P, Puech W (2020) Recompression of JPEG Crypto-Compressed Images Without a Key. IEEE Transactions on Circuits and Systems for Video Technology 30(3):646–660. https://doi.org/10.1109/TCSVT.2019.2894520
17. Kadhim IJ, Premaratne P, Vial PJ, Halloran B (2019) Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research. Neurocomputing 335:299–326. https://doi.org/10.1016/j.neucom.2018.06.075
18. Kadhim IJ, Premaratne P, Vial PJ (2020) High capacity adaptive image steganography with cover region selection using dual-tree complex wavelet transform. Cognitive Systems Research 60:20–32. https://doi.org/10.1016/j.cogsys.2019.11.002
19. Li Z, He Y (2018) Steganography with pixel-value differencing and modulus function based on PSO. Journal of Information Security and Applications 43:47–52. https://doi.org/10.1016/j.jisa.2018.10.006
20. Li J, Yu C, Gupta BB, Ren X (2018) Color Image Watermarking Scheme Based on Quaternion Hadamard Transform and Schur Decomposition. Multimedia Tools and Applications 77(4):4545–4561. https://doi.org/10.1007/s11042-017-4452-0
21. Li D, Deng L, Bhooshan Gupta B, Wang H, Choi C (2019) A Novel CNN Based Security Guaranteed Image Watermarking Generation Scenario for Smart City Applications. Information Sciences 479:432–447. https://doi.org/10.1016/j.ins.2018.02.060
22. Liao X, Yu Y, Li B, Li Z, Qin Z (2020) A New Payload Partition Strategy in Color Image Steganography. IEEE Transactions on Circuits and Systems for Video Technology 30(3):685–696. https://doi.org/10.1109/TCSVT.2019.2896270
23. Ma Y, Luo X, Li X, Bao Z, Zhang Y (2019) Selection of Rich Model Steganalysis Features Based on Decision Rough Set a Positive Region Reduction. IEEE Transactions on Circuits and Systems for Video Technology 29(2):336–350. https://doi.org/10.1109/TCSVT.2018.2799243
24. Mielikainen J (2006) LSB matching revisited. IEEE Signal Processing Letters 13(5):285–287. https://doi.org/10.1109/LSP.2006.870357
25. Wang X, Zhao H, Wang M (2019) A new image encryption algorithm with nonlinear-diffusion based on Multiple coupled map lattices. Optics & Laser Technology 115, 42–57. https://doi.org/10.1016/j.optlastec.2019.02.009
26. Zeng J, Wang C (2021) A Novel Hyperchaotic Image Encryption System Based on Particle Swarm Optimization Algorithm and Cellular Automata. Security and Communication Networks 2021, 6675565. https://doi.org/10.1155/2021/6675565
27. Mohsin AH, Zaidan AA, Zaidan BB, Albahri OS, Albahri AS, Alsalem MA, Mohammed KI, Nidhal S, Jalood NS, Jasim AN, Shareef AH (2019) New Method of Image Steganography Based on Particle

Swarm Optimization Algorithm in Spatial Domain for High Embedding Capacity. IEEE Access 7:168994–169010. https://doi.org/10.1109/ACCESS.2019.2949622
28. Muhammad K, Sajjad M, Mehmood I, Rho S, Baik SW (2018) Image steganography using uncorrelated color space and its application for security of visual contents in online social networks. Future Generation Computer Systems 86:951–960. https://doi.org/10.1016/j.future.2016.11.029
29. Muhuri PK, Ashraf Z, Goel S (2020) A Novel Image Steganographic Method based on Integer Wavelet Transformation and Particle Swarm Optimization. Applied Soft Computing 92:106257. https://doi.org/10.1016/j.asoc.2020.106257
30. Nipanikar SI, Deepthi VH, Kulkarni N (2018) A sparse representation based image Steganography using Particle Swarm Optimization and wavelet transform. Alexandria Engineering Journal 57(4):2343–2356. https://doi.org/10.1016/j.aej.2017.09.005
31. Song W, Fu C, Tie M, Sham C-W, Liu J, Ma H-f (2022) A fast parallel batch image encryption algorithm using intrinsic properties of chaos. Signal Processing: Image Communication 102, 116628
32. Parah SA, Ahad F, Sheikh JA, Bhat GM (2017) Hiding clinical information in medical images: A new high capacity and reversible data hiding technique. Journal of Biomedical Informatics 66:214–230. https://doi.org/10.1016/j.jbi.2017.01.006
33. Pevny T, Bas P, Fridrich J (2010) Steganalysis by Subtractive Pixel Adjacency Matrix. IEEE Transactions on Information Forensics and Security 5(2):215–224. https://doi.org/10.1109/TIFS.2010.2045842
34. Li D, Deng L, Bhooshan Gupta B, Wang H, Choi C (2019) A Novel CNN Based Security Guaranteed Image Watermarking Generation Scenario for Smart City Applications. Information Sciences 479, 432-447. https://doi.org/10.1016/j.ins.2018.02.060
35. Roy A, Misra AP, Banerjee S (2019) Chaos-based image encryption using vertical-cavity surface-emitting lasers. Optik 176:119–131. https://doi.org/10.1016/j.ijleo.2018.09.062
36. Snasel V, Kromer P, Safarik J, Platos J (2020) JPEG steganography with particle swarm optimization accelerated by AVX. Concurrency and Computation: Practice and Experience 32(8):5448. https://doi.org/10.1002/cpe.5448
37. Snasel V, Kromer P, Safarik J, Platos J (2020) JPEG steganography with particle swarm optimization accelerated by AVX. Concurrency and Computation: Practice and Experience 32(8):5448. https://doi.org/10.1002/cpe.5448
38. Song W, Fu C, Tie M, Sham C-W, Liu J, Ma H-f (2022) A fast parallel batch image encryption algorithm using intrinsic properties of chaos. Signal Processing: Image Communication 102:116628
39. Swain G (2019) Very High Capacity Image Steganography Technique Using Quotient Value Differencing and LSB Substitution. Arabian Journal for Science and Engineering 44(4):2995–3004. https://doi.org/10.1007/s13369-018-3372-2
40. Tong H, Zhu Y, Pierezan J, Xu Y, Coelho LdS (2021) Chaotic Coyote Optimization Algorithm. Journal of Ambient Intelligence and Humanized Computing. https://doi.org/10.1007/s12652-021-03234-5
41. Wang X, Gao S (2020) Image encryption algorithm for synchronously updating Boolean networks based on matrix semi-tensor product theory. Information Sciences 507:16–36. https://doi.org/10.1016/j.ins.2019.08.041
42. Wang X, Li Y (2021) Chaotic image encryption algorithm based on hybrid multi-objective particle swarm optimization and DNA sequence. Optics and Lasers in Engineering 137:106393. https://doi.org/10.1016/j.optlaseng.2020.106393
43. Wang Z, Bovik AC, Sheikh HR, Simoncelli EP (2004) Image quality assessment: from error visibility to structural similarity. IEEE Transactions on Image Processing 13(4):600–612. https://doi.org/10.1109/TIP.2003.819861
44. Wang X, Zhao H, Wang M (2019) A new image encryption algorithm with nonlinear-diffusion based on Multiple coupled map lattices. Optics & Laser Technology 115:42–57. https://doi.org/10.1016/j.optlastec.2019.02.009
45. Pevny T, Bas P, Fridrich J (2010) Steganalysis by Subtractive Pixel Adjacency Matrix. IEEE Transactions on Information Forensics and Security 5(2):215–224. https://doi.org/10.1109/TIFS.2010.2045842
46. Yang Z-L, Guo X-Q, Chen Z-M, Huang Y-F, Zhang Y-J (2019) RNNStega: Linguistic Steganography Based on Recurrent Neural Networks. IEEE Transactions on Information Forensics and Security 14(5):1280–1295. https://doi.org/10.1109/TIFS.2018.2871746
47. Zeng J, Wang C (2021) A Novel Hyperchaotic Image Encryption System Based on Particle Swarm Optimization Algorithm and Cellular Automata. Security and Communication Networks 2021:6675565. https://doi.org/10.1155/2021/6675565
48. Zhang Y (2021) Statistical test criteria for sensitivity indexes of image cryptosystems. Information Sciences 550:313–328. https://doi.org/10.1016/j.ins.2020.10.026

# Terms and Conditions

Springer Nature journal content, brought to you courtesy of Springer Nature Customer Service Center GmbH ("Springer Nature").

Springer Nature supports a reasonable amount of sharing of research papers by authors, subscribers and authorised users ("Users"), for small-scale personal, non-commercial use provided that all copyright, trade and service marks and other proprietary notices are maintained. By accessing, sharing, receiving or otherwise using the Springer Nature journal content you agree to these terms of use ("Terms"). For these purposes, Springer Nature considers academic use (by researchers and students) to be non-commercial.

These Terms are supplementary and will apply in addition to any applicable website terms and conditions, a relevant site licence or a personal subscription. These Terms will prevail over any conflict or ambiguity with regards to the relevant terms, a site licence or a personal subscription (to the extent of the conflict or ambiguity only). For Creative Commons-licensed articles, the terms of the Creative Commons license used will apply.

We collect and use personal data to provide access to the Springer Nature journal content. We may also use these personal data internally within ResearchGate and Springer Nature and as agreed share it, in an anonymised way, for purposes of tracking, analysis and reporting. We will not otherwise disclose your personal data outside the ResearchGate or the Springer Nature group of companies unless we have your permission as detailed in the Privacy Policy.

While Users may use the Springer Nature journal content for small scale, personal non-commercial use, it is important to note that Users may not:

1. use such content for the purpose of providing other users with access on a regular or large scale basis or as a means to circumvent access control;
2. use such content where to do so would be considered a criminal or statutory offence in any jurisdiction, or gives rise to civil liability, or is otherwise unlawful;
3. falsely or misleadingly imply or suggest endorsement, approval , sponsorship, or association unless explicitly agreed to by Springer Nature in writing;
4. use bots or other automated methods to access the content or redirect messages
5. override any security feature or exclusionary protocol; or
6. share the content in order to create substitute for Springer Nature products or services or a systematic database of Springer Nature journal content.

In line with the restriction against commercial use, Springer Nature does not permit the creation of a product or service that creates revenue, royalties, rent or income from our content or its inclusion as part of a paid for service or for other commercial gain. Springer Nature journal content cannot be used for inter-library loans and librarians may not upload Springer Nature journal content on a large scale into their, or any other, institutional repository.

These terms of use are reviewed regularly and may be amended at any time. Springer Nature is not obligated to publish any information or content on this website and may remove it or features or functionality at our sole discretion, at any time with or without notice. Springer Nature may revoke this licence to you at any time and remove access to any copies of the Springer Nature journal content which have been saved.

To the fullest extent permitted by law, Springer Nature makes no warranties, representations or guarantees to Users, either express or implied with respect to the Springer nature journal content and all parties disclaim and waive any implied warranties or warranties imposed by law, including merchantability or fitness for any particular purpose.

Please note that these rights do not automatically extend to content, data or other material published by Springer Nature that may be licensed from third parties.

If you would like to use or distribute our Springer Nature journal content to a wider audience or on a regular basis or in any other manner not expressly permitted by these Terms, please contact Springer Nature at

onlineservice@springernature.com