Multimed Tools Appl (2017) 76:23517–23538
DOI 10.1007/s11042-016-4052-4

A novel cascade encryption algorithm for digital images based on anti-synchronized fractional order dynamical systems

P. Muthukumar[1,2] · P. Balasubramaniam[1] · K. Ratnavelu[2]

Received: 7 July 2015 / Revised: 15 July 2016 / Accepted: 6 October 2016 /
Published online: 19 November 2016

Abstract In this paper, an active control technique is employed for anti-synchronization between two identical fractional order reverse butterfly-shaped hyperchaotic systems. We have shown that the convergence rate of anti-synchronization error is very faster by increasing the value of an active controller gain. A new algorithm for image encryption and decryption is introduced and established by anti-synchronized fractional order dynamical systems. Experimental results show that the proposed encryption algorithm has high level security against various attacks. Further, it confirms that the new algorithm is more efficient compared to other existing algorithms.

Keywords Fractional order system · Hyperchaos · Anti-synchronization · Image encryption

1 Introduction

1.1 Research background

With the development of communication and social networking technologies, multimedia data such as images, video and audio are transmitted over the network more conveniently.

✉ P. Balasubramaniam
balugru@gmail.com

P. Muthukumar
muthukumardgl@gmail.com

K. Ratnavelu
kuru052001@gmail.com

[1] Department of Mathematics, Gandhigram Rural Institute-Deemed University, Dindigul, 624 302, Tamil Nadu, India

[2] Institute of Mathematical Sciences, Faculty of Science, University of Malaya, 50603 Kuala Lumpur, Malaysia

Consequently, the security of multimedia data becomes more and more important. A huge amount of digital data, which are either private or confidential, need to be protected against the misuse. Therefore, a well secured encryption algorithm is essential for secure communication. The security of multimedia data is receiving more and more attention due to the widespread transmission over various communication networks. Yet a potential risk of information security always exists during the processing and transmission of digital images over an open network. The properties of an ideal encryption scheme for data security such as confidentiality, integrity and authenticity have been drawn more attention by researchers in the field of image encryption. Therefore, designing good image encryption schemes has become a focal research topic. The conventional cryptographic algorithms like RSA (Rivest Shamir Adleman) and DES (Data Encryption Standard) are not effective for encryption of data owing to capacity of data, intrinsic characteristics of images, high redundancy and so on. Due to the main features of chaotic systems like sensitivity to initial conditions, ergodicity, simple analytic description and high complex behavior, cryptographic algorithms using chaotic systems are more effective and secure than traditional cryptographic algorithms. Further, chaotic system based encryption algorithms have several inherent features favorable to data security.

1.2 Literature overview

Over the past decades, several chaos based image encryption techniques have been widely investigated in the field of secure communication. In 1989, Matthews [23] developed the first chaotic stream encryption algorithm. After that, a symmetric image encryption algorithm using the two-dimensional standard Baker map has been proposed by Fridrich [8] in 1998. Lately, the chaotic Boolean bit function has been employed and applied to the image encryption in [14]. In [19], a color image encryption scheme has been designed by using chaos with the help of bijective function. Synchronization of two different six-dimensional hyperchaotic systems [36] has been utilized for image encryption. The total plain image characteristics, crossover operator and chaos have been applied for image encryption respectively in [9, 24]. The statistical properties of image encryption algorithm have been improved by multiple chaotic maps in [40]. A fast color image encryption scheme has been designed in [20] by one-time S-Box, which is generated by the complex chaotic system. DNA sequence and hyperchaotic system have been utilized for image encryption in [11].

In order to improve the security and efficiency performance, several image encryption algorithms have been designed by applying the theory of fractional calculus. The fractional differential equations are generalizations of classical differential equations and it gained popularity in the nonlinear dynamical systems. Many real world systems have been determined by fractional derivatives since they allow more flexibility in the model [15, 21, 42]. The study of chaotic dynamics of fractional order systems has been a hot topic in the field of nonlinear science. Furthermore, applications of control and synchronization of fractional order chaotic systems have been reported in many areas, for instance in medicine [1], telecommunications [32], robotics [7], secure communication and cryptography [3, 25–28, 30, 35]. Several types of control techniques and methodologies have been investigated for synchronizing fractional order systems such as feedback control technique [25], adaptive observer [41], active control method [4], non-fragile control [2], multi-scale synchronization technique [26], fast projective synchronization method [28], Lyapunov based control [17], hybrid phase synchronization [27] and sliding mode control [29]. Apart from synchronization, anti-synchronization is a dominating phenomenon in symmetrical oscillators. The ultimate aim of anti-synchronization is to study the opponent behavior of the master and slave systems so that the sum of their states will converge to zero asymptotically. Due to this reason, different control methods have been utilized for anti-synchronizing chaotic systems in [6, 13, 16, 31, 33].

A short overview of the recently proposed image encryption schemes [10, 12, 18, 26, 37, 39] build from fractional order dynamical systems are given hereafter. A color image encryption algorithm by using coupled-map lattices and a fractional order chaotic system has been proposed to enhance the security and robustness of the encryption algorithms with a permutation-diffusion structure in [37]. The scrambled image has been encrypted once again by the pseudorandom sequences generated from the combined fractional-order hyperchaotic systems in [10]. An encryption algorithm has been constructed in [12] by the fractional order hyperchaotic system which can effectively enhance the cryptosystem security. In [18], a color image encryption algorithm by combining the reality-preserving fractional DCT with chaotic mapping in HSI space has been presented. A new cryptosystem has been proposed for an image encryption by using synchronized fractional order King Cobra chaotic systems with the supports of multiple cryptographic assumptions in [26]. In [39], an image encryption algorithm has been presented where the original image is encoded by a nonlinear function of a fractional chaotic state. Further, these encryption algorithms are experimentally demonstrated which includes correlation analysis, histogram analysis, and key sensitivity analysis to verify the security level of the encryption scheme. Compared to integer order systems, the fractional order systems are found to have more complex dynamics because the fractional derivatives have complex geometrical interpretation due to their nonlocal character and high nonlinearity. Further, the derivative orders can be also used as secret keys as well, which will increase the key space of the cryptosystem. To the best of authors knowledge, few more encryption techniques are available in the literature using the fractional order chaotic systems. Therefore, for the purpose of high security, the construction of new image encryption algorithm by applying fractional order chaotic systems is very essential.

1.3 Our contribution

Based on the aforesaid studies, the anti-synchronization scheme for fractional order reverse butterfly-shaped hyperchaotic systems is investigated via active control technique. The necessary conditions are derived to achieve the anti-synchronization between two systems. Apart from existing image encryption algorithms, a new image encryption-decryption algorithm is introduced by utilizing anti-synchronized fractional order hyperchaotic systems and encryption (decryption) of encryption (decryption) techniques, which is entirely different from other existing image encryption techniques. Further, we have shown that the new algorithm has higher level security by various experimental analysis tests and comparison results.

In Section 2, some basic theories of fractional calculus are given. In Section 3, the fractional order reverse butterfly-shaped hyperchaotic system is described. The process of anti-synchronization between two identical fractional order reverse butterfly-shaped hyperchaotic systems using active control technique is elaborately studied in Section 4. Section 5 contributes to the applications: a new image encryption algorithm is described by the anti-synchronized scheme. The experimental analysis of the proposed algorithm is presented in Section 6. The performance analysis and the security of the proposed algorithm are compared in Section 7. The conclusions of this paper are drawn in Section 8.

2 Preliminaries

In this paper, we have used the Caputo fractional differential operator since the Caputo's derivative of a constant is zero and it has conventional initial conditions.

Definition 1 [5] The Caputo fractional derivative is defined as

$$D^{\alpha} f(t) = \frac{1}{\Gamma(n-\alpha)} \int_{a}^{t} (t-\tau)^{-\alpha+n-1} f^{(n)}(\tau) d\tau, \tag{1}$$

where $n = [\alpha] + 1$, $[\alpha]$ is the integer part of α, D^{α} is called the α-order Caputo differential operator, Γ is the usual Gamma function given by and

$$\Gamma(z) = \int_{0}^{\infty} e^{-t} t^{z-1} dt. \tag{2}$$

Further it is noted that $\Gamma(z+1) = z\Gamma(z)$.

Theorem 1 [22] *The following autonomous fractional order system*

$$D^{\alpha} x(t) = Ax(t),\ x(0) = x_0, \tag{3}$$

where $0 < \alpha \leq 1,\ x \in \mathbb{R}^n$ *is asymptotically stable if and only if*

$$|\arg(eig(A))| > \frac{\alpha\pi}{2}. \tag{4}$$

Also, the system (3) *is stable if and only if* $|\arg(eig(A))| \geq \frac{\alpha\pi}{2}$ *and those critical eigenvalues that satisfy* $|\arg(eig(A))| = \frac{\alpha\pi}{2}$ *have geometric multiplicity one.*

Theorem 2 [34] *A necessary condition for the system* (3) *to remain chaotic is keeping at least one eigenvalue* λ *in the unstable region. This means*

$$\alpha > \frac{2}{\pi} \arctan\left(\frac{|Im(\lambda)|}{Re(\lambda)}\right). \tag{5}$$

3 Description of fractional order hyperchaotic system

Consider the fractional form of the reverse butterfly-shaped hyperchaotic system described in [38],

$$\begin{aligned} D^{\alpha} x_1 &= a(x_2 - x_1) + x_4, \\ D^{\alpha} x_2 &= bx_1 + kx_1x_3, \\ D^{\alpha} x_3 &= -cx_3 - hx_1x_2, \\ D^{\alpha} x_4 &= x_1x_3 - dx_2, \end{aligned} \tag{6}$$

where $0 < \alpha \leq 1, x = (x_1, x_2, x_3, x_4)^T \in \mathbb{R}^4$ is the state variable and a, b, c, d, h, k are the parameters of the system (6). D^{α} is the α-order differential operator in the sense of Caputo [5]. The authors in [38] have been shown that the integer order ($\alpha = 1$) system (6) behave hyperchaos for the parameters $a = 10, b = 40, c = 2.5, d = 2, h = 1$ and $k = 16$.

Throughout this manuscript, we have fix the same parameters $a = 10, b = 40, c = 2.5, d = 2, h = 1$ and $k = 16$ for the fractional order system (6). According to Theorem

1, the fractional order system is stable for every $\alpha \le 0.9606$. The system (6) exhibit chaos with two positive Lyapunov exponents when the fractional order $\alpha > 0.9606$ according to Theorem 2. Therefore, the system (6) is called as a fractional order reverse butterfly-shaped hyperchaotic system and the corresponding hyperchaotic attractors when $\alpha = 0.97$ are depicted in Fig. 1.

4 Anti-synchronization of two identical fractional order hyperchaotic systems

In this section, an active control technique is applied to achieve anti-synchronization between two identical fractional order reverse butterfly-shaped hyper chaotic systems.

Consider the fractional order system (6) as a master system and the following identical system of (6) as a slave system

$$\begin{aligned} D^{\alpha} y_1 &= a(y_2 - y_1) + y_4 + u_1, \\ D^{\alpha} y_2 &= by_1 + ky_1 y_3 + u_2, \\ D^{\alpha} y_3 &= -cy_3 - hy_1 y_2 + u_3, \\ D^{\alpha} y_4 &= y_1 y_3 - dy_2 + u_4, \end{aligned} \tag{7}$$

where $0 < \alpha \le 1$, $y = (y_1, y_2, y_3, y_4)^T \in \mathbb{R}^4$ is the state variable, $u = (u_1, u_2, u_3, u_4)^T$ is the active control function to be determined later so that both systems (6) and (7) are anti-synchronized successfully.

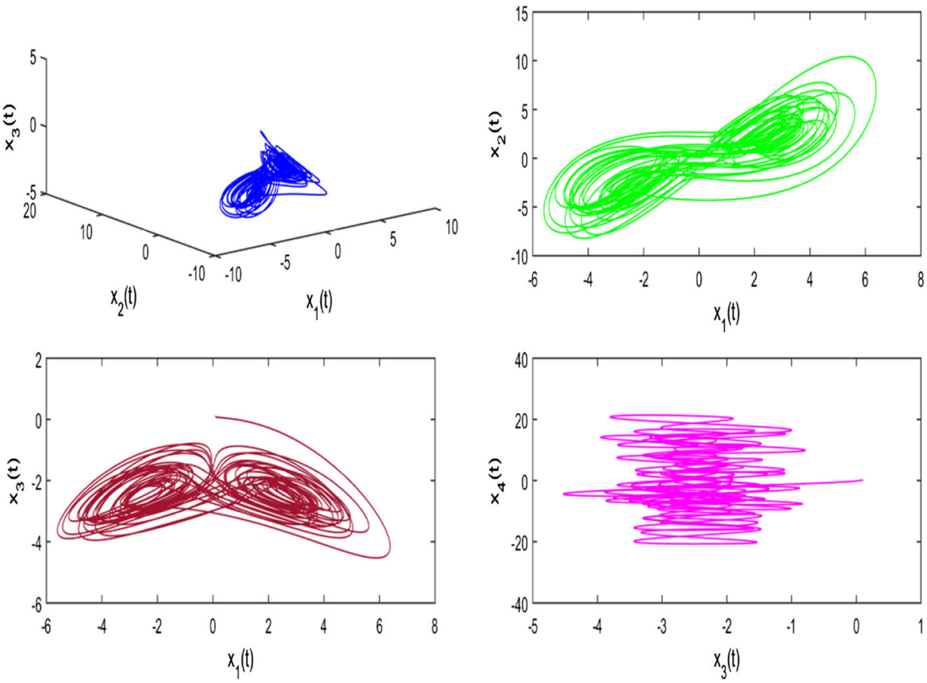

Fig. 1 Hyperchaotic attractors of the system (6) when $\alpha = 0.97$

To investigate the anti-synchronization between the systems (6) and (7), we define the synchronization error states as $e_i = y_i + x_i$ for $i = 1, 2, 3, 4$. The ultimate aim is to select the active control function u such that

$$\lim_{t\to\infty} \|e_i(t)\| = \lim_{t\to\infty} \|y_i(t) + x_i(t)\| = 0, \ \ i = 1, 2, 3, 4. \tag{8}$$

Then, the fractional order error dynamical system between the systems (6) and (7) is described by

$$\begin{aligned} D^\alpha e_1(t) &= a(e_2 - e_1) + e_4 + u_1, \\ D^\alpha e_2(t) &= be_1 + k(y_1y_3 + x_1x_3) + u_2, \\ D^\alpha e_3(t) &= -ce_3 - h(y_1y_2 + x_1x_2) + u_3, \\ D^\alpha e_4(t) &= -de_2 + y_1y_3 + x_1x_3 + u_4. \end{aligned} \tag{9}$$

Theorem 3 *The fractional order mater system* (6) *and the slave system* (7) *are globally asymptotically anti-synchronized with the following active control functions*

$$\begin{aligned} u_1(t) &= v_1 - ae_2 - e_4, \\ u_2(t) &= v_2 - be_1 - k(y_1y_3 + x_1x_3), \\ u_3(t) &= v_3 + h(y_1y_2 + x_1x_2), \\ u_4(t) &= v_4 + de_2 - y_1y_3 - x_1x_3, \end{aligned} \tag{10}$$

where v_i is a linear function of e_i such that $v_i < 0$ for $i = 1, 2, 3, 4$.

Proof The fractional order error dynamical system (9) together with active control functions u_i defined in (10) yields

$$\begin{aligned} D^\alpha e_1(t) &= v_1 - ae_1, \\ D^\alpha e_2(t) &= v_2, \\ D^\alpha e_3(t) &= v_3 - ce_3, \\ D^\alpha e_4(t) &= v_4. \end{aligned} \tag{11}$$

Since by hypothesis, without loss of generality, we assume that $v_i(t) = -l_ie_i$ where $l_i > 0$ is the gain of v_i as well as active control functions u_i for $i = 1, 2, 3, 4$.

Then, the system (11) can be written as

$$\begin{aligned} D^\alpha e_1(t) &= -(l_1 + a)e_1, \\ D^\alpha e_2(t) &= -l_2e_2, \\ D^\alpha e_3(t) &= -(l_3 + c)e_3, \\ D^\alpha e_4(t) &= -l_4e_4. \end{aligned} \tag{12}$$

The Jacobian matrix J of fractional order error dynamical system (12) is

$$J = \begin{pmatrix} -(l_1 + a) & 0 & 0 & 0 \\ 0 & -l_2 & 0 & 0 \\ 0 & 0 & -(l_3 + c) & 0 \\ 0 & 0 & 0 & -l_4 \end{pmatrix} \tag{13}$$

The eigenvalues $\lambda_i, i = 1, 2, 3, 4$ of (13) are $\lambda_1 = -(l_1 + a)$, $\lambda_2 = -l_2$, $\lambda_3 = -(l_3 + c)$ and $\lambda_4 = -l_4$. Since $l_i > 0$ for every i, $a = 10$ and $c = 2.5$, then all eigenvalues are less than zero. Further, the value of $|\arg(\lambda_i)|$ is equal to π for $i = 1, 2, 3, 4$. Thus, the asymptotically stable condition (4) is satisfied for the fractional order error dynamical system (12). Consequently, the error states e_i are tend to zero as $t \to \infty$. Therefore, the proposed active control function is fulfilled the requirement (8). Hence, anti-synchronization between the master system (6) and the slave system (7) is achieved successfully. □

4.1 Numerical simulations

Consider the initial values of the master system (6) and the slave system (7) respectively by $(x_1(0), x_2(0), x_3(0), x_4(0)) = (0.1, 0.1, 0.1, 0.1)$ and $(y_1(0), y_2(0), y_3(0), y_4(0)) = (-1, -1, 1, 1)$. For convenience, we fix the fractional order $\alpha = 0.98$ and the controller gain l_i is selected as $l_i = l > 0$ for $i = 1, 2, 3, 4$.

In simulations, the state trajectories between the systems (6) and (7) are depicted in Figs. 2, 3 and 4 for $l = 0.5$, $l = 5$ and $l = 15$ respectively. Further, the corresponding time response of anti-synchronization error states are depicted in Figs. 5, 6 and 7 respectively. From Figs. 5–7, we observed that the convergence rate of anti-synchronization errors are gradually decreased in the fractional order $\alpha = 0.98$ by increasing the value of controller gain l. Thus, we conclude that anti-synchronization is achieved faster by increasing the control gain.

In the following section, these anti-synchronized fractional order reverse butterfly-shaped hyperchaotic systems are utilized to develop an encryption and decryption algorithm for digital images.

5 Proposed encryption-decryption algorithm

In this section, a new encryption algorithm for an image without any key exchange is introduced by anti-synchronized fractional order reverse butterfly-shaped hyperchaotic systems with the support of the discrete logarithm problem and it can be described as follows.

Assume that two cryptographic entities Alice and Bob. Let Alice be a sender and Bob be a receiver. Also, assume that the master system (6) as a sender system and the slave system (7) as a receiver system. Both Alice and Bob agree on the fractional order $\alpha > 0.9606$ and $l > 0$ at time $t > t_0$ where t_0 is a time if anti-synchronization errors between the systems (6) and (7) are tend to zero from t_0 onwards for given values of α and l.

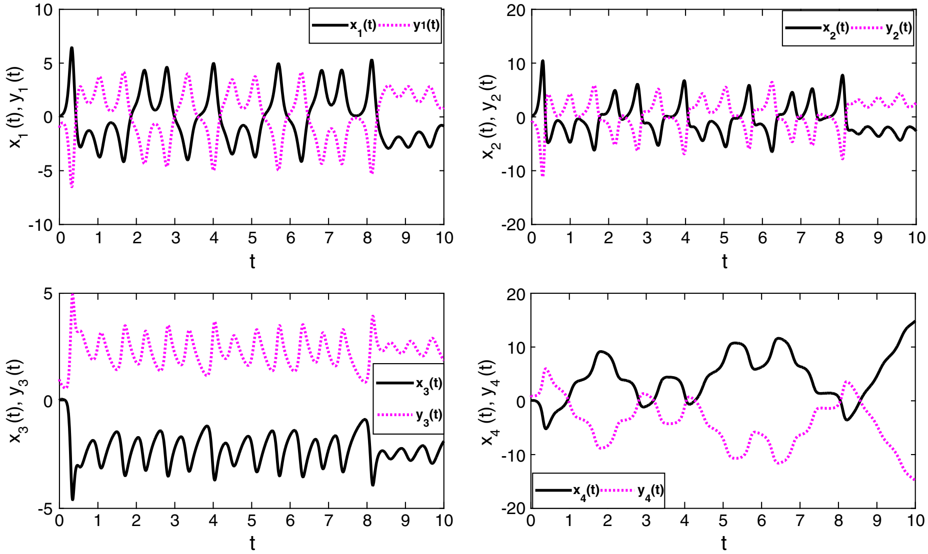

Fig. 2 State trajectories between the master system (6) and the slave system (7) when $l = 0.5$

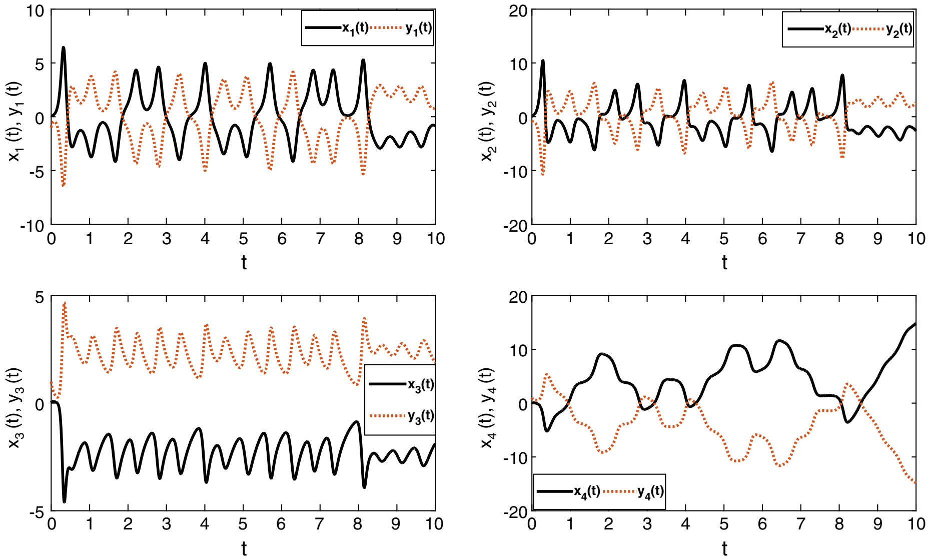

Fig. 3 State trajectories between the master system (6) and the slave system (7) when $l = 5$

Further, assume that I is the original image and D is the dummy image of size $M \times N$. The images (A_1, A_2, A_3) and (B_1, B_2) are the encrypted images computed by Alice and Bob respectively. R is the decrypted image, which is computed by Bob. Alice and Bob agree on a positive integer ρ such that $\rho < 256$ and $\gcd(\rho, 256) = 1$. Note that, $|X|$ is the absolute value of X and $floor(X)$ is the largest integer less than or equal to X.

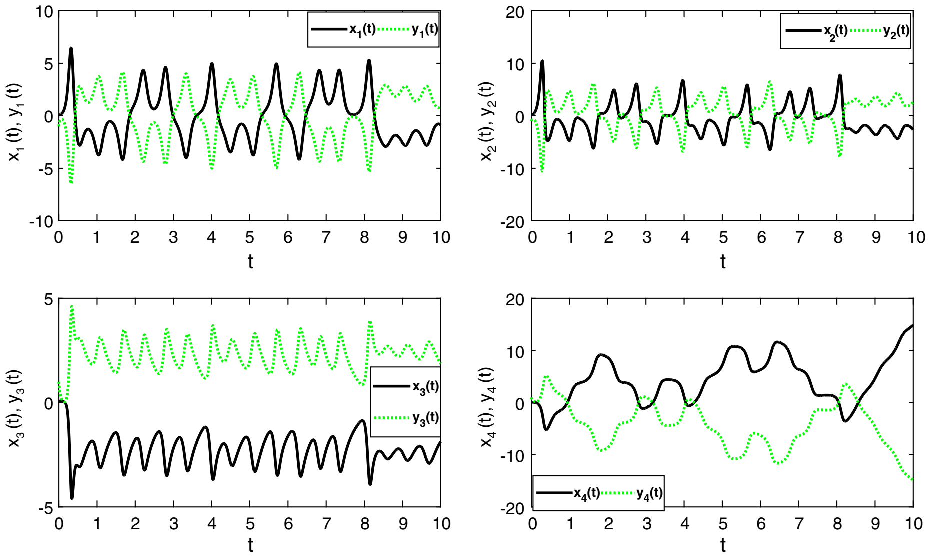

Fig. 4 State trajectories between the master system (6) and the slave system (7) when $l = 15$

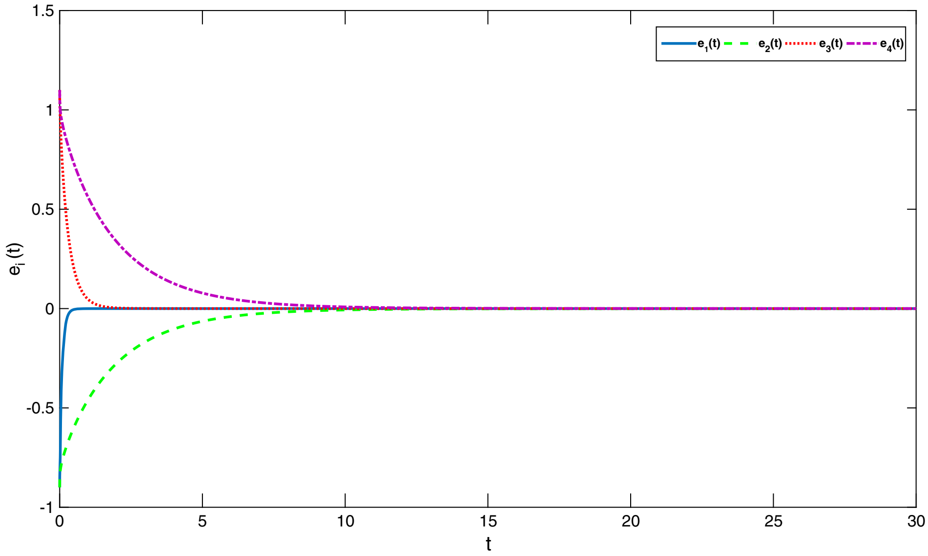

Fig. 5 Time response of the anti-synchronization error states when $l = 0.5$

Step 1. Alice wants to send a digital image I.
Step 2. Alice chooses a real number $t_1 > t_0$ and finds the solution of the system (6) at t_1.
Step 3. She computes the first encrypted image A_1 of I.

$$A_1 \equiv I\rho^r \pmod{256},$$

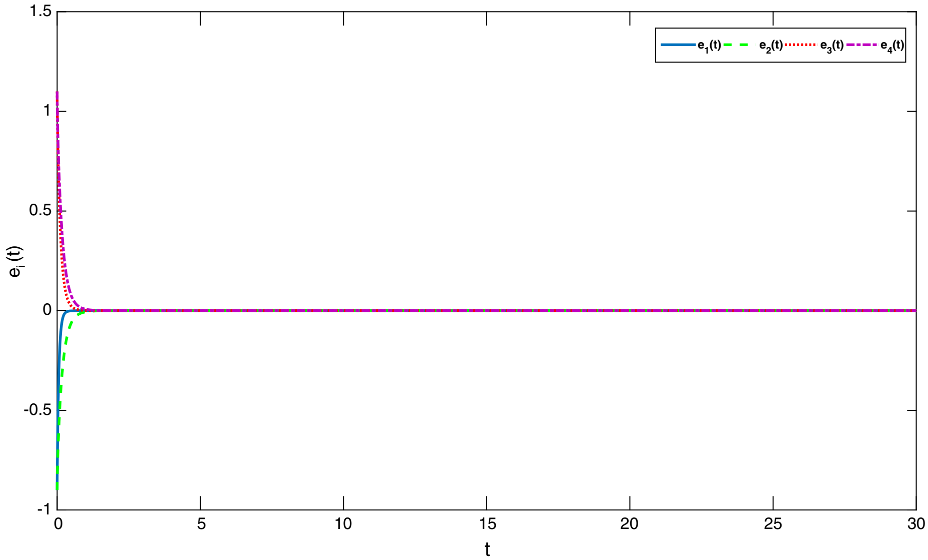

Fig. 6 Time response of the anti-synchronization error states when $l = 5$

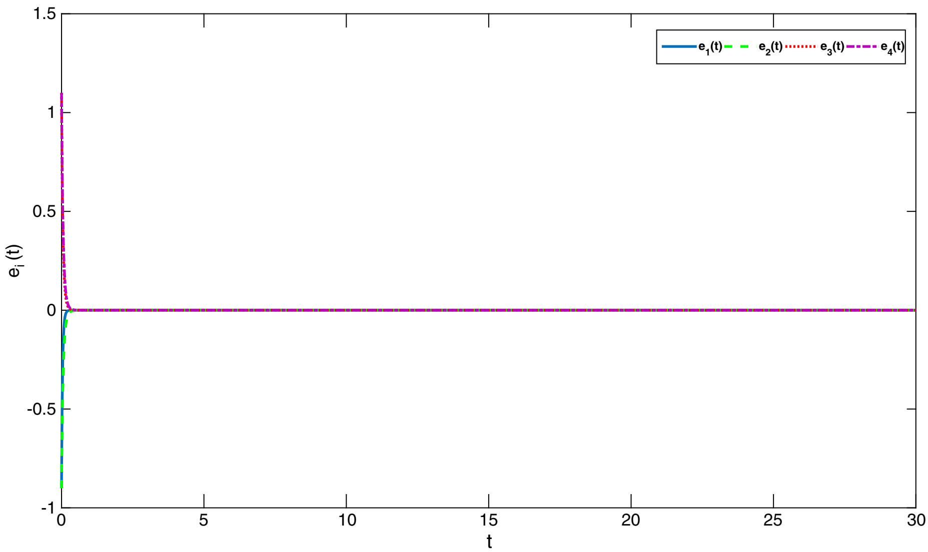

Fig. 7 Time response of the anti-synchronization error states when $l = 15$

where $r \equiv |floor(t_1 \sum_{i=1}^{4} x_i(t_1))| \pmod{256}$.

Step 4. The element r is kept secret by Alice and she sends A_1 to Bob.

Step 5. Bob receives A_1, then he chooses a real number $t_2 > t_0$ and finds the solution of the system (7) at t_2. Then, he chooses a dummy image D with the size of A_1.

Step 6. He computes the second encrypted image B_1 of I by using the dummy image D and assign the dummy image D as B_2.

$$\begin{aligned} B_1 &\equiv (A_1\rho^s + D) \pmod{256}, \\ B_2 &\equiv D \pmod{256}, \end{aligned}$$

where $s \equiv |floor(t_2 \sum_{i=1}^{4} y_i(t_2))| \pmod{256}$.

Step 7. The element s is kept secret by Bob and he sends (B_1, B_2) to Alice.

Step 8. Alice receives B_1 and B_2, then she computes the resulting encrypted image A_2 of I and the encrypted dummy image A_3 of D.

$$\begin{aligned} A_2 &\equiv B_1\rho^{-r} \pmod{256}, \\ A_3 &\equiv B_2\rho^{-r} \pmod{256}. \end{aligned}$$

Step 9. She sends the encrypted images A_2 and A_3 to Bob.

Step 10. Finally, Bob recovers an original image I by computing

$$R \equiv (A_2 - A_3)\rho^{-s} \pmod{256}.$$

For,

$$\begin{aligned} (A_2 - A_3)\rho^{-s} &\equiv (B_1\rho^{-r} - B_2\rho^{-r})\rho^{-s} \pmod{256} \\ &\equiv (B_1 - B_2)\rho^{-r}\rho^{-s} \pmod{256} \\ &\equiv (A_1\rho^s + D - D)\rho^{-(r+s)} \pmod{256} \\ &\equiv (I\rho^r\rho^s)\rho^{-(r+s)} \pmod{256} \\ R &\equiv I \pmod{256}. \end{aligned}$$

Remark 1 The proposed encryption and decryption algorithm is fully based on the discrete logarithm problem with the backbone of fractional order systems. Obviously, it contains an encryption (decryption) of encryption (decryption) images more than one time. Therefore, this algorithm is called as cascade encryption and decryption or multiple encryption and decryption algorithm.

The purpose of introducing multiple encryption is, no one got fully encrypted image or encrypted trick in the middle of the two parties because the encrypted image is encrypted more than one time. Consequently, nobody decrypts an image from the knowledge of encrypted image between two parties. Hence, the proposed cascade encryption and decryption processes are more efficient than existing encryption algorithms established by chaotic systems.

6 Experimental analysis and results

In this section, the performance of the proposed cascade image encryption algorithm is analyzed and its high level security has been investigated experimentally through various security test measures. These measures are taken as follows: key space analysis, statistical analysis including correlation coefficients of adjacent pixels, information entropy analysis, histogram analysis and test security against differential attack.

The standard image processing color plain image of Lena and the Baboon image with a size of 256×256 are utilized for encryption and decryption processes. The parameters of the systems (6) and (7) for experimentation are: $a = 10, b = 40, c = 2.5, d = 2, h = 1$ and $k = 16$. The value of the fractional order α, the feedback gain l, a positive integer ρ, the real numbers t_1 and t_2 are taken as 0.98, 5, 5, 7 and 3.85 respectively. Assume that the Lena image is an original image I and the Baboon image is a dummy image D. We implement the proposed algorithm by using Matlab 7.1. The original color image, the dummy image and the encrypted images are displayed in Fig. 8.

6.1 Key space analysis

The size of key space is the total number of different keys that can be applied in the encryption process. A good encryption algorithm should be sensitive to the secret keys and the key space should be large enough to ensure the security of the encryption algorithm against brute-force attacks. In our cascade encryption algorithm, the initial conditions of the master system $x_i(0)$ and the slave system $y_i(0)$, $i = 1, 2, 3, 4$, the fractional order α, the parameters a, b, c, d, h, k, the time t_1 and the feedback control gain l are secret keys. If the precision is 10^{-14}, then the size of the initial conditions key space is $10^{14\times 8}$. Additionally the fractional order, the time and the feedback control gain keys can also produce large key spaces. Therefore, the total key space is more than $10^{14\times 8}$, which is greater than 2^{370} approximately. Hence, the proposed cascade encryption algorithm has a large enough key space to resist all varieties of brute-force attacks.

6.2 Correlation analysis

The correlation coefficient between images can be used to evaluate the quality of the encryption algorithm. In ordinary images having definite visual content, each adjacent pixels are highly correlated. This means that the correlation coefficients of plain image are closer to 1. For the good encryption algorithm, the correlation coefficients among the adjacent pixels of the encrypted image are close to 0. The correlation coefficient of two adjacent pixels in an image is calculated by using the following formula:

$$\gamma_{xy} = \frac{cov(x, y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{14}$$

where

$$cov(x, y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)),$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2,$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{n}(x_i),$$

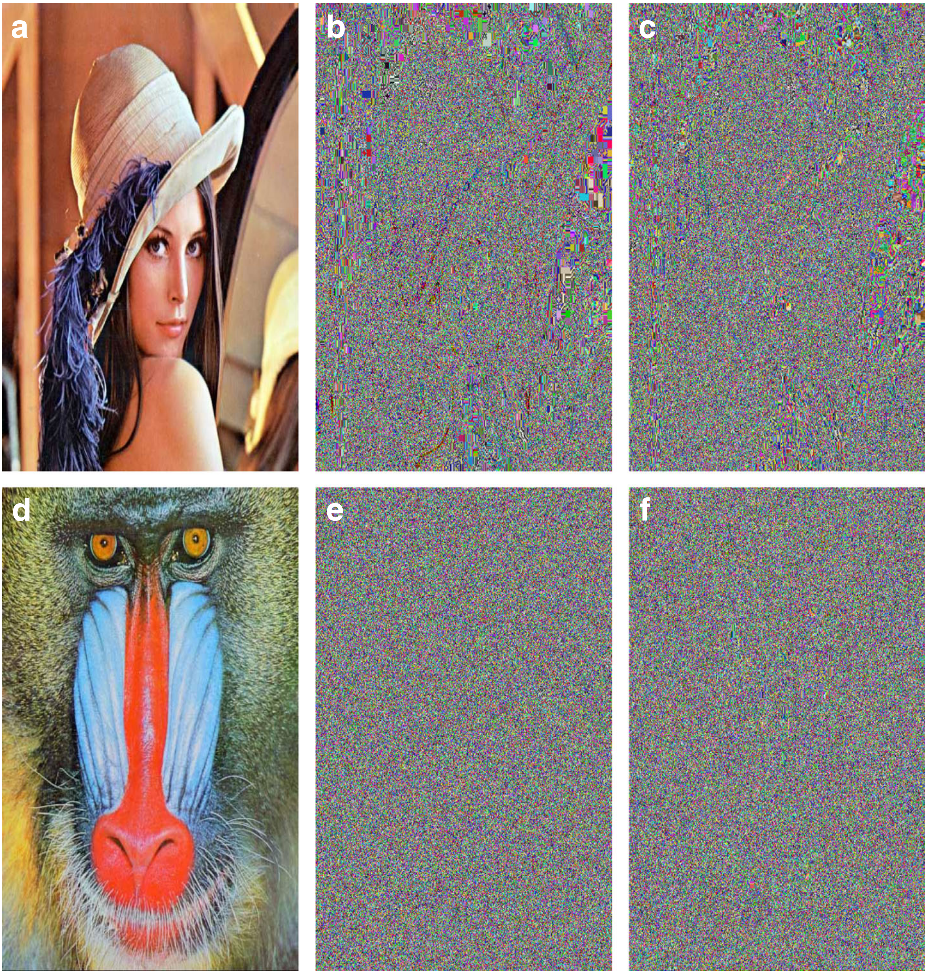

Fig. 8 **a** Original image I, **b** First encrypted image A_1, **c** Second encrypted image B_1, **d** Dummy image B_2, **e** Resulting encrypted image A_2 and **f** Encrypted dummy image A_3

where x, y are grey scale values of two adjacent pixels in the image, $cov(x, y)$ is the covariance between x and y, $D(x)$ and $D(y)$ are the variance of x and y respectively, and $E(x)$, $E(y)$ are the expectation of x and y.

For the proposed algorithm, the correlation coefficients of two adjacent pixels in the original image and encrypted images are tried out respectively in horizontal, vertical and diagonal directions. Table 1 shows the outcomes of the correlation coefficients in three directions. Figures 9 and 10 show the corresponding distribution of the original and the resulting encrypted image in horizontal, vertical and diagonal directions respectively. From Table 1, one can see that the estimated correlation coefficients of encrypted images in three directions are very close to 0, implying that the ciphered image has been well encrypted. Therefore, the proposed encryption algorithm is secure and robust against correlation attacks.

6.3 Information entropy analysis

Information entropy defines the randomness and the unpredictability of an information in the image. To measure the value of entropy $H(s)$ of a source s, we have

$$H(s) = -\sum_{i=0}^{2^N-1} P(s_i)\log_2 P(s_i), \tag{15}$$

where s_i is the i-th gray scale value for an 256 gray level image, $P(s_i)$ is the probability of s_i, $s_i \in s$. For truly random source emitting 2^N symbols, the entropy value of the source is $H(s) = N$. For a random image with 256 gray levels, the entropy should be $H(s) = 8$ theoretically. However, a good encryption algorithm should produce an encrypted image with the entropy very close to 8. For the proposed algorithm, the entropy values of encrypted images are calculated and listed in Table 2. The results show that the information entropies of encrypted images are close to 8 and the resulting encrypted image is very close to 8. Hence, the proposed encryption algorithm is secure against the entropy analysis.

6.4 Histogram analysis

For an image encryption algorithm, the histogram analysis is very important because it describes the distribution of the image pixels by plotting the number of pixels at each intensity level. If the histogram of an encrypted image is uniform, then the encryption scheme

Table 1 Correlation coefficients of two adjacent pixels in original image and encrypted images

Images	Directions		
	Horizontal	Vertical	Diagonal
The original image I	0.9897	0.9791	0.9687
First encrypted image A_1	0.1294	0.0597	0.0469
Second encrypted image B_1	0.1098	0.0706	0.0428
The dummy image B_2	0.8834	0.9404	0.8610
Resulting encrypted image A_2	0.0036	0.0032	0.0030
The encrypted dummy image A_3	0.0142	0.0093	0.0161
The decrypted image R	0.9897	0.9791	0.9687

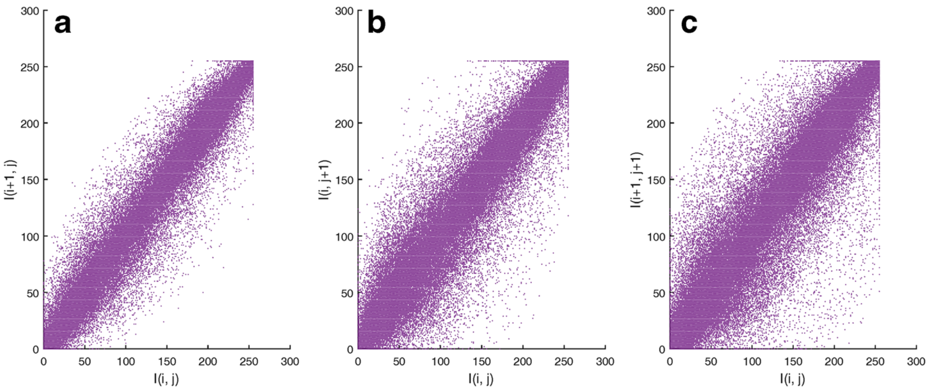

Fig. 9 The correlation of two adjacent pixels in different directions for original image I: (**a**) Horizontal, (**b**) Vertical and (**c**) Diagonal

is more robust against statistical attack and differential attack. Figure 11a and b represents the histograms of the original and resulting encrypted images in red, green and blue color components respectively. It shows that histograms of the resulting encrypted image are uniform and significantly different from the histograms of original image. Hence, it does not provide any clue to employ statistical attack and differential attack on the encrypted image.

6.5 Differential attack analysis

Differential attack means that attacker creates a slight change to the original image, and use the proposed image encryption algorithm to encrypt for the original image before and after changing, to find out the relationship between the original image and the cipher image through comparing two encrypted images. The number of pixel change rate (NPCR) and the unified average changing intensity (UACI) are two most common measures used to assess the strength of image encryption algorithms with respect to differential attacks. The NPCR

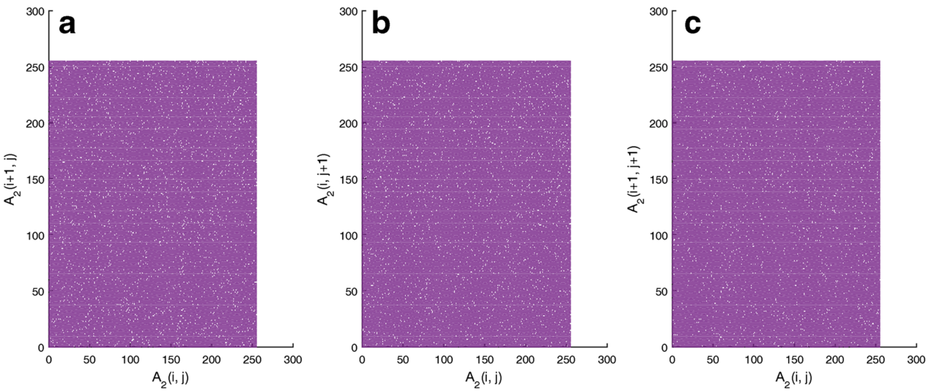

Fig. 10 The correlation of two adjacent pixels in different directions for resulting encrypted image A_2: (**a**) Horizontal, (**b**) Vertical and (**c**) Diagonal

Table 2 Information entropy of encrypted images

Images	Entropy
First encrypted image A_1	7.9562
Second encrypted image B_1	7.9998
Resulting encrypted image A_2	7.9998
The encrypted dummy image A_3	7.7555

is applied to measure the percentage of the number of pixels change rate of the ciphered image while one pixel of the original image has changed and it is calculated as:

$$NPCR = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} D(i, j) \times 100\%, \tag{16}$$

where

$$D(i, j) = \begin{cases} 0 \text{ if } I_1(i, j) = I_2(i, j) \\ 1 \text{ if } I_1(i, j) \neq I_2(i, j) \end{cases},$$

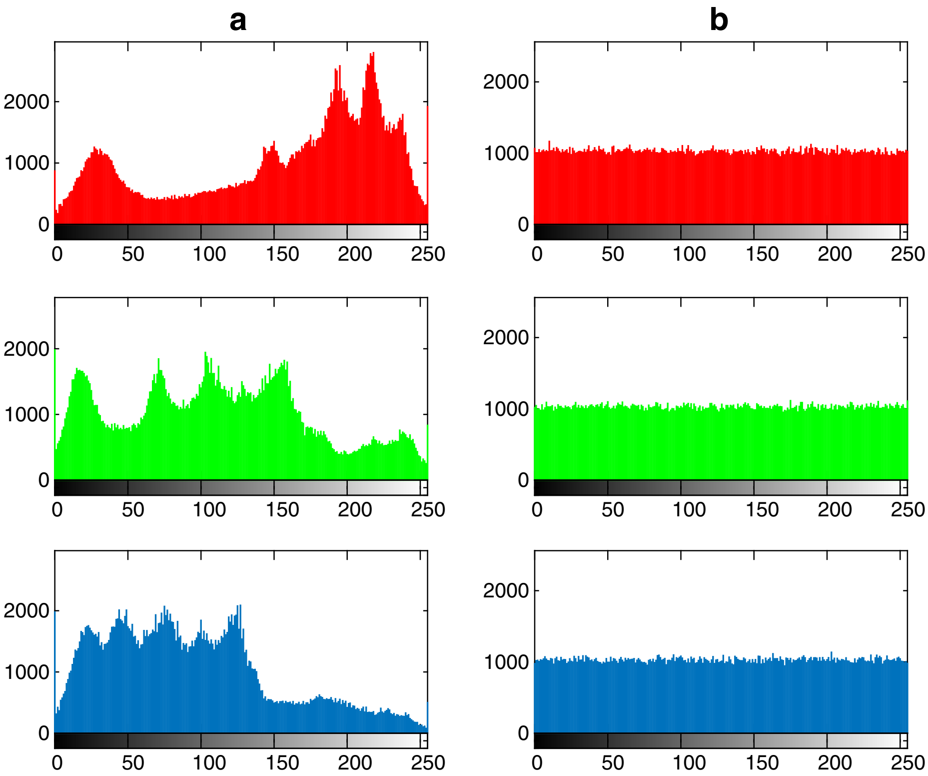

Fig. 11 Histograms of the color image in red, green and blue components: (**a**) Original image I and (**b**) Resulting encrypted image A_2

Table 3 NPCR and UACI percentage of encrypted images

Images	NPCR(%)	UACI(%)
First encrypted image A_1	98.2952	33.9635
Second encrypted image B_1	99.6151	34.0900
Resulting encrypted image A_2	99.6330	34.1319
The Encrypted dummy image A_3	99.6235	33.9419

where $I_1(i, j)$ and $I_2(i, j)$ are the pixel gray value of two cipher images in the same position. The closer the NPCR comes to 100 %, the more sensitive the encryption algorithm is to the original image and the more effective the encryption algorithm resists differential attack.

The UACI is applied to measure the percentage of the the average intensity difference of two ciphered images, whose corresponding original image has only one pixel difference and it is calculated as:

$$UACI = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{|I_1(i, j) - I_2(i, j)|}{2^N - 1} \times 100\ \%, \tag{17}$$

where $I_1(i, j)$ and $I_2(i, j)$ are the pixel gray value of two cipher images in the same position. The value of UACI is very close to 33%. The greater the UACI is, the better the encryption algorithm resists the differential attack.

For a image with 256 gray levels, the expected NPCR and UACI values are 99.6094 % and 33.4635 % respectively. For the proposed algorithm, the NPCR and UACI values are given in Table 3 for resulting encrypted images with one bit difference in original image. Note that the value of NPCR and UACI of resulting encrypted image is higher than their expected values.

7 Comparison with previous work

In this section, we compare the security performance of the proposed encryption algorithm with other existing chaos based image encryption algorithms suggested in Refs. [9, 10, 12, 14, 19, 20, 24, 36, 37, 40].

The total key space of the proposed algorithm is greater than 2^{370}, which is enough to prevent the exhaustive searching. Thus, brute-force attacks on the key are computationally infeasible and the proposed scheme has the large key space size than other encryption algorithms in Refs. [9, 10, 12, 19, 20]. This signifies more number of trials required to crack the proposed encryption algorithm by comparing the other chaos based encryption algorithms.

Table 4 Comparison of correlation coefficients of two adjacent pixels in different directions encrypted Lena image using the proposed algorithm with some other algorithms

	Directions		
Images	Horizontal	Vertical	Diagonal
The proposed algorithm	0.0036	0.0032	0.0030
Ref. [9]	0.0802	0.0706	0.0738
Ref. [12]	−0.0006	0.0051	0.0094
Ref. [14]	0.0141	0.0107	0.0097
Ref. [37]	−0.0037	0.0001	−0.0230

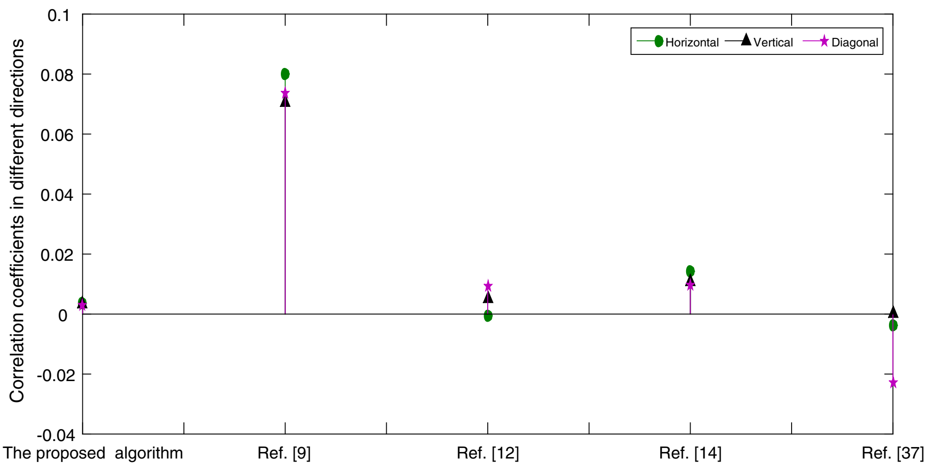

Fig. 12 Comparison graph of correlation coefficients of two adjacent pixels of encrypted Lena image in horizontal, vertical and diagonal directions with some other algorithms

The comparison performed of the correlation coefficient of the proposed algorithm in Table 4 shows that the proposed encryption algorithm is superior to other methods reported in Refs. [9, 12, 14, 37]. The comparison of correlation coefficients of two adjacent pixels of encrypted Lena image in different directions with some other algorithms is depicted in Fig. 12. It shows that the correlation coefficients of the proposed algorithm in horizontal, vertical and diagonal directions are close to 0. Therefore, The encrypted image using our proposed algorithm has the highest performance in the horizontal, vertical and diagonal directions. Table 5 compares information entropy using the proposed encryption algorithm with those using the existing algorithms mentioned in Refs. [9, 10, 14, 19, 20, 24, 36, 37, 40]. Hence, the entropy obtained using our proposed algorithm is indeed closer to the maximum entropy value of 8, which shows the strength of the proposed encryption algorithm. So, information leakage in the encryption process could be negligible and the proposed algorithm is secure against entropy analysis. Table 6 compares the NPCR and UACI for the proposed encryption algorithm and the existing algorithms in Refs. [9, 10, 12, 14, 19, 20,

Table 5 Comparison of information entropy of encrypted Lena images with different algorithm

Encrypted image	Entropy
The proposed algorithm	7.9998
Ref. [9]	7.9973
Ref. [10]	7.9979
Ref. [14]	7.9972
Ref. [19]	7.9899
Ref. [20]	7.9811
Ref. [24]	7.9973
Ref. [36]	7.9896
Ref. [37]	7.9895
Ref. [40]	7.9993

Table 6 The results of NPCR and UACI with different algorithm

Images	NPCR (%)	UACI (%)
The proposed algorithm	99.6330	34.1319
Ref. [9]	99.6058	33.5260
Ref. [10]	99.6196	33.2648
Ref. [12]	99.6013	33.4134
Ref. [14]	99.6124	33.4591
Ref. [19]	99.6180	33.6069
Ref. [20]	99.6216	33.4158
Ref. [24]	99.6100	33.3600
Ref. [40]	99.6080	33.4712

24, 40]. From the results, one can easily see that the proposed encryption algorithm achieves a higher performance by comparing the other methods. Therefore, the proposed algorithm is very sensitive with respect to the small changes in the original image and it has a strong power and secures to resist the differential attack.

Remark 2 The experimental and comparison results show that the proposed cascade encryption algorithm has large key space and more secure against the most common attacks such as correlation attack, entropy attack, differential attack, sensitivity to the secret key. Therefore, the proposed encryption algorithm can be applied to encrypt images for transmission over insecure channel.

8 Conclusions

In this paper, anti-synchronization scheme for fractional order reverse butterfly-shaped hyperchaotic system has been suggested by using active control technique . In order to verify the effectiveness of the anti-synchronization, enough numerical investigations have been done by different values of active controller gain. Finally, we conclude that the convergence rate of anti-synchronization errors are inversely proportional to an active controller gain. A novel secure cascade encryption-decryption algorithm for digital images has been presented analytically and numerically. The security and performance analysis of the proposed algorithm have been carried out by several tests. The obtained results prove that the proposed image encryption algorithm preserves good encryption performance than existing algorithms.

Acknowledgments This work was supported by the University of Malaya HIR Grant UM.C/625/1/HIR/MOHE/SC/13, Malaysia.

Compliance with Ethical Standards

Conflict of interests The authors declare that there is no conflict of interests regarding the publication of this manuscript.

References

1. Aghababa MP, Borjkhani M (2014) Chaotic fractional-order model for muscular blood vessel and its control via fractional control scheme. Complexity 20(2):37–46
2. Asheghan MM, Delshad SS, Beheshti MTH, Tavazoei MS (2013) Non-fragile control and synchronization of a new fractional order chaotic system. Appl Math Comput 222:712–721
3. Balasubramaniam P, Muthukumar P, Ratnavelu K (2015) Theoretical and practical applications of fuzzy fractional integral sliding mode control for fractional-order dynamical system. Nonlinear Dyn 80(1-2):249–267
4. Bhalekar S (2014) Synchronization of non-identical fractional order hyperchaotic systems using active control. World J Modell Simul 10:60–68
5. Caputo M (1967) Linear models of dissipation whose q is almost frequency independentii. Geophys J Int 13(5):529–539
6. Chen D, Zhao W, Sprott JC, Ma X (2013) Application of takagi–sugeno fuzzy model to a class of chaotic synchronization and anti-synchronization. Nonlinear Dyn 73(3):1495–1505
7. Delavari H, Lanusse P, Sabatier J (2013) Fractional order controller design for a flexible link manipulator robot. Asian J Control 15(3):783–795
8. Fridrich J (1998) Symmetric ciphers based on two-dimensional chaotic maps. Int J Bifurcation chaos 8(06):1259–1284
9. Guesmi R, Farah MAB, Kachouri A, Samet M (2016) Hash key-based image encryption using crossover operator and chaos. Multimed tools Appl 75(8):4753–4769
10. He J, Yu S, Cai J (2015) A method for image encryption based on fractional-order hyperchaotic systems. J Appl Anal Comput 5(2):197–209
11. Huang X, Ye G (2014) An image encryption algorithm based on hyper-chaos and dna sequence. Multimed Tools Appl 72(1):57–70
12. Huang X, Sun T, Li Y, Liang J (2014) A color image encryption algorithm based on a fractional-order hyperchaotic system. Entropy 17(1):28–38
13. Jian X (2011) Anti-synchronization of uncertain rikitake systems via active sliding mode control. Int J Phys Sci 6(10):2478–2482
14. Khan M, Shah T, Batool SI (2016) Construction of s-box based on chaotic boolean functions and its application in image encryption. Neural Comput Appl 27(3):677–685
15. Kwuimy CK, Litak G, Nataraj C (2015) Nonlinear analysis of energy harvesting systems with fractional order physical properties. Nonlinear Dyn 80(1-2):491–501
16. Li HL, Jiang YL, Wang ZL (2015) Anti-synchronization and intermittent anti-synchronization of two identical hyperchaotic chua systems via impulsive control. Nonlinear Dyn 79(2):919–925
17. Li R, Chen W (2014) Lyapunov-based fractional-order controller design to synchronize a class of fractional-order chaotic systems. Nonlinear Dyn 76(1):785–795
18. Liang Y, Liu G, Zhou N, Wu J (2015) Color image encryption combining a reality-preserving fractional dct with chaotic mapping in hsi space. Multimed Tools Appl:1–16
19. Liu H, Kadir A, Niu Y (2014) Chaos-based color image block encryption scheme using s-box. AEU-Int J Electron Commun 68(7):676–686
20. Liu H, Kadir A, Gong P (2015) A fast color image encryption scheme using one-time s-boxes based on complex chaotic system and random noise. Opt Commun 338:340–347
21. Lopes AM, Machado JT (2016) Integer and fractional-order entropy analysis of earthquake data series. Nonlinear Dynam 84(1):79–90
22. Matignon D (1996) Stability results for fractional differential equations with applications to control processing. In: Computational Engineering in Systems Applications, vol 2. Citeseer, pp 963–968
23. Matthews R (1989) On the derivation of a chaotic encryption algorithm. Cryptologia 13(1):29–42
24. Murillo-Escobar M, Cruz-Hernández C, Abundiz-Pérez F, López-Gutiérrez R, Del Campo OA (2015) A rgb image encryption algorithm based on total plain image characteristics and chaos. Signal Process 109:119–131
25. Muthukumar P, Balasubramaniam P (2013) Feedback synchronization of the fractional order reverse butterfly-shaped chaotic system and its application to digital cryptography. Nonlinear Dyn 74(4):1169–1181
26. Muthukumar P, Balasubramaniam P, Ratnavelu K (2014a) Synchronization and an application of a novel fractional order king cobra chaotic system. Chaos: An Interdisc J Nonlinear Sci 24(3):033,105
27. Muthukumar P, Balasubramaniam P, Ratnavelu K (2014b) Synchronization of a novel fractional order stretch-twist-fold (stf) flow chaotic system and its application to a new authenticated encryption scheme (aes). Nonlinear Dyn 77(4):1547–1559

28. Muthukumar P, Balasubramaniam P, Ratnavelu K (2015a) Fast projective synchronization of fractional order chaotic and reverse chaotic systems with its application to an affine cipher using date of birth (dob). Nonlinear Dyn 80(4):1883–1897
29. Muthukumar P, Balasubramaniam P, Ratnavelu K (2015b) Sliding mode control design for synchronization of fractional order chaotic systems and its application to a new cryptosystem. International Journal of Dynamics and Control:1–9
30. Norouzi B, Mirzakuchaki S (2015) Breaking a novel image encryption scheme based on an improper fractional order chaotic system. Multimedia Tools and Applications:1–10
31. Qin W, Jiao X, Sun T (2014) Synchronization and anti-synchronization of chaos for a multi-degree-of-freedom dynamical system by control of velocity. J Vib Control 20(1):146–152
32. Razminia A, Baleanu D (2013) Fractional hyperchaotic telecommunication systems: a new paradigm. J Comput Nonlinear Dyn 8(3):031, 012
33. Srivastava M, Ansari S, Agrawal S, Das S, Leung A (2014) Anti-synchronization between identical and non-identical fractional-order chaotic systems using active control method. Nonlinear Dyn 76(2):905–914
34. Tavazoei MS, Haeri M (2007) A necessary condition for double scroll attractor existence in fractional-order systems. Phys Lett A 367(1):102–113
35. Wu GC, Baleanu D, Lin ZX (2016) Image encryption technique based on fractional chaotic time series. J Vib Control 22(8):2092–2099
36. Wu X, Bai C, Kan H (2014) A new color image cryptosystem via hyperchaos synchronization. Commun Nonlinear Sci Numer Simul 19(6):1884–1897
37. Wu X, Li Y, Kurths J (2015) A new color image encryption scheme using cml and a fractional-order chaotic system. PloS one 10(3):e0119, 660
38. Xu J, Cai G, Zheng S (2009) A novel hyperchaotic system and its control. J Uncertain Syst 3(2):137–144
39. Xu Y, Wang H, Li Y, Pei B (2014) Image encryption based on synchronization of fractional chaotic systems. Commun Nonlinear Sci Numer Simul 19(10):3735–3744
40. Yao W, Zhang X, Zheng Z, Qiu W (2015) A colour image encryption algorithm using 4-pixel feistel structure and multiple chaotic systems. Nonlinear Dynx 81(1-2):151–168
41. Zhang R, Gong J (2014) Synchronization of the fractional-order chaotic system via adaptive observer. Syst Sci Control Eng: Open Access J 2(1):751–754
42. Zhong J, Li L (2015) Tuning fractional-order controllers for a solid-core magnetic bearing system. IEEE Trans Control Syst Technol 23(4):1648–1656

P. Muthukumar was born in Dindigul, Tamil Nadu, India. He obtained his the B.Sc. and M.Sc. degrees in Mathematics from Madurai Kamaraj University, India in 2004 and 2006 respectively. He received the M.Phil. degree in Mathematics from and Gandhigram Rural Institute-Deemed University, India in 2007. Subsequently, he served as a Lecturer in Mathematics for four years. He received his Ph.D. degree in Mathematics from Gandhigram Rural Institute-Deemed University, Gandhigram, India in 2015. At present, he is working as a Postdoctoral Fellow in the Institute of Mathematical Sciences, University of Malaya, Malaysia. He is a life member of Cryptology Research Society of India, Indian Statistical Institute, Kolkata, India. His research interest includes: Stability analysis, Dynamical systems, Fractional order dynamical systems, Chaos, Synchronization, Cryptography, Number theory and Algebra.

P. Balasubramaniam post graduated in the year 1989 and subsequently completed Master of Philosophy in the year 1990 and Doctor of Philosophy (Ph.D.) in 1994 in the field of Mathematics with specialized area of Control Theory from Bharathiar University, Coimbatore, Tamilnadu, India. Soon after his completion of Ph.D. degree, he served as Lecturer in Mathematics in Engineering Colleges for three years. Since February 1997 he served as Lecturer and Reader in Mathematics and now he is rendering his services as a Professor, Department of Mathematics, Gandhigram Rural University, Gandhigram, India, from November 2006 onwards. He has worked as a Visiting Research Professor during the years 2001 and 2005–2006 for promoting research in the field of control theory and neural networks at Pusan National University, Pusan, South Korea. Also he has worked as Visiting Professor in the Institute of Mathematical Sciences, University of Malaya, Malaysia, for the period of six months from September 2011 to March 2012. He is a member of several academic bodies including a life member of Cryptology Research Society of India, Indian Statistical Institute, Kolkata. He has 23 years of experience in teaching and research. He has published more than 211 research papers in various SCI journals holding impact factors with Scopus H-index 29 and web of knowledge HIndex 23. Also he has edited 7 proceedings including a book and 3 international conference proceedings in Springer publications. He is serving as a reviewer of many SCI journals and member of the editorial board of Journal of Computer Science, Advances in Fuzzy Sets and Systems and the Sceintific World Journal: Mathematical Analysis, Hindawi Publisling Corporation, USA. He is an Editor-in-Chief of the journal Modern Instrumentation, Scientific Research Publishing Inc. (SCIRP) and Associate Editor of Advances in Difference Equations, Springer, Germany. He has received the Tamilnadu Scientist Award (TANSA) for the discipline of Mathematical Sciences instituted by the Tamilnadu State Council for Science and Technology in the year 2005. His research interest includes the areas of Control theory, Stochastic differential equations, Soft Computing, Stability analysis, Cryptography, Neural Networks and image processing.

K. Ratnavelu obtained his BSc (First Class Hons) and his MSc by research from the Department of Mathematics, University Malaya and furthered his PhD study in Atomic Physics at Flinders University in 1985 with a Flinders Research Scholarship. He started as a Lecturer in 1989; was promoted to Associate Professor in 1994 and subsequently as Professor in 2001. Prof Ratnavelu's research and academic achievements has been recognized and he was awarded the Malaysian Toray Science Foundation Science & Technology Award in 2004 and also the Young Scientist Award (Strategic Sector) in 1996 by MOSTE. He was elected as a Fellow of the Academy of Sciences Malaysia in 2005. In 2006, he was awarded the Inaugural Distinguished Alumni Award by Flinders University. His main research interest is in Theoretical Atomic Collision Processes with specific interest in positron collisions with atoms. His outstanding contributions are in the recent development and the demonstration of an optical potential method to positron-hydrogen atom scattering process and its extension to other hydrogenic-type atoms. Another major contribution is his joint theoretical work with Jim Mitroy on anti-hydrogen formation in 1995. His scientific contribution's is evidenced by his international publications; as a reviewer for international journals and his collaboration with eminent international researchers. He has contributed to the scientific community in Malaysia as the Associate Editor of the Jurnal Fizik Malaysia (the leading physics journal in Malaysia) and the Associate Editor of Malaysia Journal of Science (one of the oldest journal in Malaysia). He has immensely helped in the professional development of Physics and Mathematics in Malaysia since the 1990's in his capacity as the Honorary Secretary of the Institut Fizik Malaysia (1996-now) and Malaysian Mathematical Society (PERSAMA) respectively. At University of Malaya, he has served as a Deputy Dean of Science (2003–2006) and acting Deputy Dean (1999–2000).