Hyper-chaos encryption using convolutional masking and model free unmasking*

Qi Guo-Yuan(齐国元)† and Sandra Bazebo Matondo

Department of Electrical Engineerin, Tshwane University of Technology Pretoria, South Africa, 0001

(Received 5 July 2013; revised manuscript received 4 November 2013; published online 25 March 2014)

In this paper, during the masking process the encrypted message is convolved and embedded into a Qi hyper-chaotic system characterizing a high disorder degree. The masking scheme was tested using both Qi hyper-chaos and Lorenz chaos and indicated that Qi hyper-chaos based masking can resist attacks of the filtering and power spectrum analysis, while the Lorenz based scheme fails for high amplitude data. To unmask the message at the receiving end, two methods are proposed. In the first method, a model-free synchronizer, i.e. a multivariable higher-order differential feedback controller between the transmitter and receiver is employed to de-convolve the message embedded in the receiving signal. In the second method, no synchronization is required since the message is de-convolved using the information of the estimated derivative.

Keywords: Qi hyper-chaos, masking, high-order differentiator, chaos-based encryption

PACS: 05.45.Vx, 05.45.Xt, 05.45.Pq, 05.45.–a **DOI:** 10.1088/1674-1056/23/5/050507

1. Introduction

The properties of chaos, wideband spectrum, non-periodic waveform, random-like behavior, and simple implementation, make chaos an attractive candidate for secure communication.[1,2] Chaotic masking is widely used in chaos communication techniques. The well-known masking technique is a chaos additive mixing scheme in which a message $m(t)$ is simply added to the chaotic mask $c(t)$ and then transmitted as $s(t)$. However, because of the simplicity of the technique, it is easily broken and extracted by methods such as the wavelet multi-scale decomposition algorithm, which can separate two signals using different wavelet scales.[3] In our work, a convolutional masking method is employed, where the message acts as an applied force driving the chaotic system. The chaos signal carrying the message convolved is transmitted out.

The security of chaos masking is not only dependent on the algorithm used, but is also dependent on the characteristic of chaos. Hyper-chaotic systems have a higher degree of complexity than simple chaotic systems, which makes hyper-chaos more suitable for secure communication.[4] In this paper, we utilize Qi hyper-chaos[4] which has a large number of parameters to ensure the cipher key space and two large positive Lyapunov exponents of more than 13 and 3 respectively to ensure the system randomness. The form of the hyper-chaos attractor is very irregular, neither butterfly nor scroll, which is visually more complex than the ordinary chaotic or other hyper-chaotic attractors proposed. The Qi hyper-chaos does not require a change in the frequency or time domain to exhibit a noise like system suitable for an efficient masking.[5]

To decrypt or recover the signal masked by chaos, many researchers designed controllers,[6] such as sliding mode control,[7] active control,[8] adaptive control, and an open and nonlinear closed loop method[9] to synchronize the master and slave chaotic systems.[10,11] However, most of these controllers have been designed for specific chaotic systems, and they are dependent on the models of the chaotic systems.

In this work, two methods are proposed to unmask the ciphered signal. A synchronizer is implemented between the driving system and the response system in the first method, in which a model-free controller called the multivariable higher-order differential feedback controller (MHODFC)[12] was applied. The MHODFC successfully implemented the synchronization for the Lorenz system, the Chen system, the Duffing–Holmes system, the Rössler system, and the four-dimensional (4D) chaotic system[12] and drove these systems' trajectories to the desired ones without changing the controller structure. In the second method, the synchronization is immune in the unmasking process. To decrypt or unmask the message, the derivatives of driving system signals using a higher-order differentiator (HOD) are estimated. The estimated derivative signals are applied in the deconvolution process to unmask the signal. Therefore, no hyper-chaotic or chaotic response system is required at the receiving end, which can be designed in the normal synchronization.

2. Masking

Two types of data are considered for masking: the binary sequence and the digital image. For security comparison, the Qi hyper-chaotic system and the Lorenz system are used in the

*Project supported by the Incentive Funding National Research Foundation of South Africa (Grant No. 70722) and the Eskom Tertiary Education Support Programme of South Africa.

†Corresponding author. E-mail: qig@tut.ac.za

© 2014 Chinese Physical Society and IOP Publishing Ltd

masking process.

2.1. Masking scheme using the Qi hyper-chaotic system

The data $m(t)$ is convolved with the 4D Qi hyper-chaotic system.[4] Through the convolution process, the data $m(t)$ is hidden in hyper-chaos and the resultant signal is transmitted out as $s(t)$. In our encryption process, the chaotic signal $x_i, i = 1, 2, 3, 4$ and the derivative $\dot{x}_1$ are transmitted out

$$\begin{cases} \dot{x}_1 = a(x_2 - x_1) + x_2x_3 + m(t), \\ \dot{x}_2 = b(x_1 + x_2) - x_1x_3, \\ \dot{x}_3 = -cx_3 - ex_4 + x_1x_2, \\ \dot{x}_4 = -dx_4 + fx_3 + x_1x_2, \end{cases} \tag{1}$$

where $a = 50$, $b = 24$, $c = 13$, $d = 8$, $e = 33$, and $f = 30$. It is obvious that x_i, $i = 1, 2, 3, 4$ is not the original chaos signal anymore but the chaos signal masked by message $m(t)$.

2.2. Masking scheme using the Lorenz chaotic system

The Lorenz system[13] is also used for masking, shown as

$$\begin{cases} \dot{x} = \sigma(y - x) + m(t), \\ \dot{y} = rx - y - xz, \\ \dot{z} = xy - bz, \end{cases} \tag{2}$$

where $\sigma = 10$, $b = 8/3$, and $r = 28$, and x, y, and z are the state variables.

3. Result

3.1. Binary sequence masking

Binary sequences are generated by a Bernoulli binary generator. Figures 1 and 2 illustrate the successful masking of the same binary sequence by the Lorenz chaotic system and the Qi hyper-chaos respectively. From the masked signals, no information of the binary sequence can be exposed, in other words, the binary sequence is fully hidden in the masked signals. Since the magnitude of the binary number sequence is much smaller than those of the two systems, it is easy to hide.

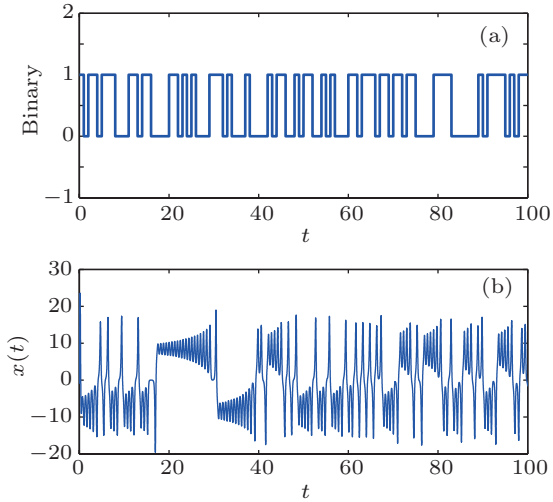


Fig. 1. (color online) Binary sequence masking using the Lorenz chaotic system: (a) binary sequence and (b) masked binary sequence.

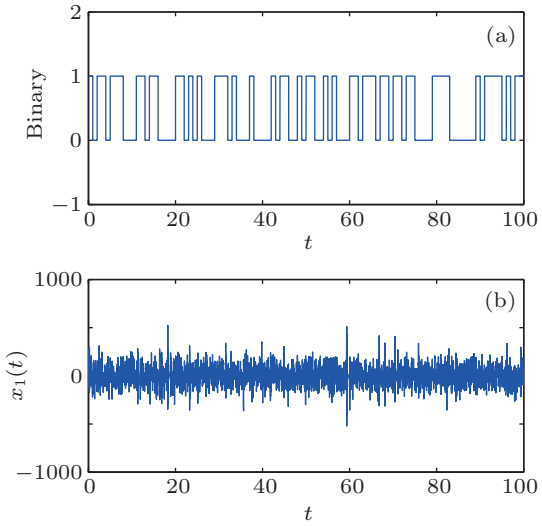


Fig. 2. (color online) Binary sequence masking using Qi hyper-chaos: (a) binary sequence and (b) masked binary sequence.

3.2. Image pixels masking

An image matrix of size $I \times J$ is converted into a vector of size L, here $L = I \times J$; all the pixel rows of the image are reshaped to create a single row matrix or vector. The rows are saved one after another in a single vector that has the same number of elements as the image matrix. After the conversion of the pixels matrix to a pixels vector, it convolves the Lorenz chaotic system and the Qi hyper-chaos respectively. Figures 3 and 4 illustrate the masking results of the image using the Lorenz chaotic system and the Qi hyper-chaos respectively.

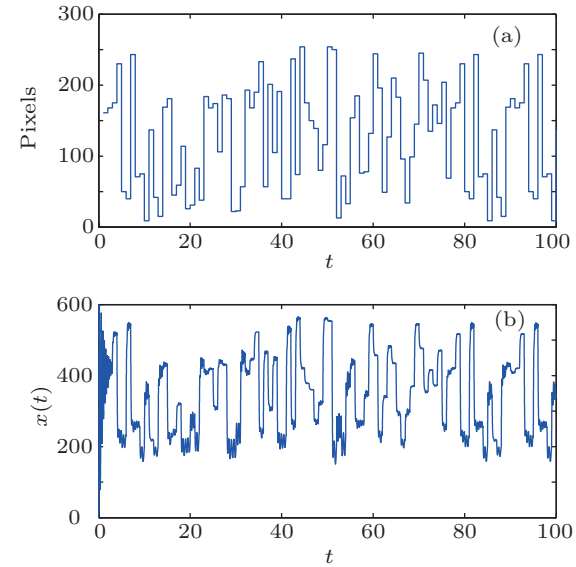


Fig. 3. (color online) Masked image pixels using Lorenz chaos $x(t)$: (a) image signal and (b) masked image signal.

The image pixels are not completely masked by the Lorenz chaotic system, as shown in Fig. 3. The masked signal clearly displays the amplitude and characteristics of the image vector, however, the masked image signal is completely

hidden in the Qi hyper-chaos. In Ref. [4], some dynamical properties of Qi hyperchaos and Lorenz chaos including the disorder rate, the value of the positive Lyapunov exponents, the bandwidth of the frequency spectrum, etc. Lorenz chaotic signal magnitudes are very small, so its energy level is low. The bandwidth of the signal frequency spectrum is narrow, and the disorder rate is low according to its value of positive Lyapunov exponent 0.9, therefore they cannot completely disguise the image signal. When the image signal $m(t)$ convolutes into the Lorenz system, the characteristics of the signal $m(t)$ are still visible after masking. However, Qi chaotic signals' magnitudes are very high, so its energy is high. The bandwidth of the signal frequency spectrum is 20 times more than that of the Lorenz chaos signal and the disorder degree is high according to the value of positive Lyapunov exponents. The image signal can be completely masked by Qi hyper-chaos. The masked signal does not show any characteristic of the image signal, as shown in Fig. 4.

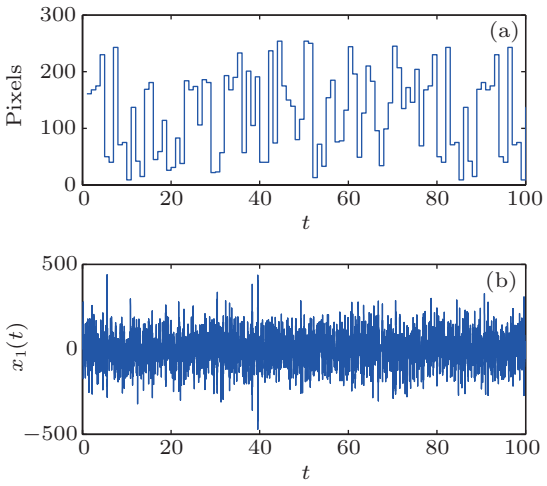


Fig. 4. (color online) Masked image using Qi hyper-chaos $x_1(t)$: (a) image signal and (b) masked image signal.

3.3. Power spectrum analysis and low pass filtering

To test the security level of the masking scheme, the power spectrum of the masked signal is analyzed; a low pass filtering attack is also performed on the masked scheme.

A fundamental requirement for the use of chaos in a masking scheme is that the spectrum of chaos should be flat, broader and denser than the signal to ensure that the message power spectrum will be effectively embedded in the chaos and hyper-chaos power spectrum. Figure 5 illustrates the power spectra of the Qi hyper-chaos and the image signal in time-series. The power spectrum of $m(t)$ is completely buried in the masked signal $s(t)$. The masked signal power spectrum is highly frequently changing, congested and dense; however, the image signal power spectrum is like a clear curve, much less congested and dense. The power spectrum of the Lorenz chaos is narrow and sparse, as shown Fig. 6.

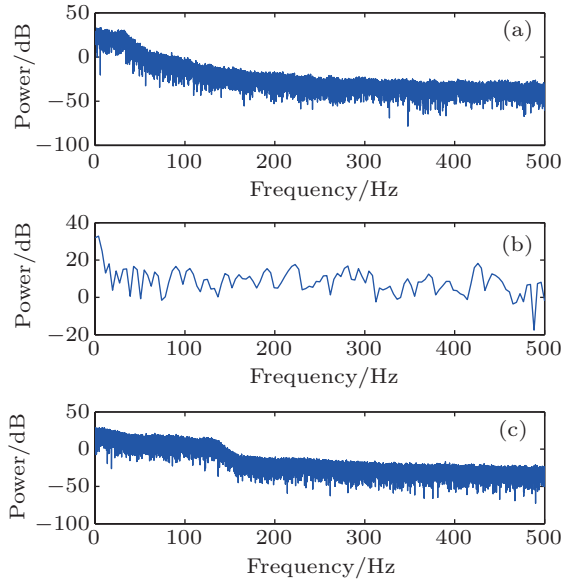


Fig. 5. (color online) Power spectra of Qi hyper-chaos x, image signal $m(t)$, and masked signal $s(t)$. (a) Periodogram power spectral density estimate x_1, (b) periodogram power spectral density estimate of the image signal, and (c) periodogram power spectral density estimate of the masked signal.

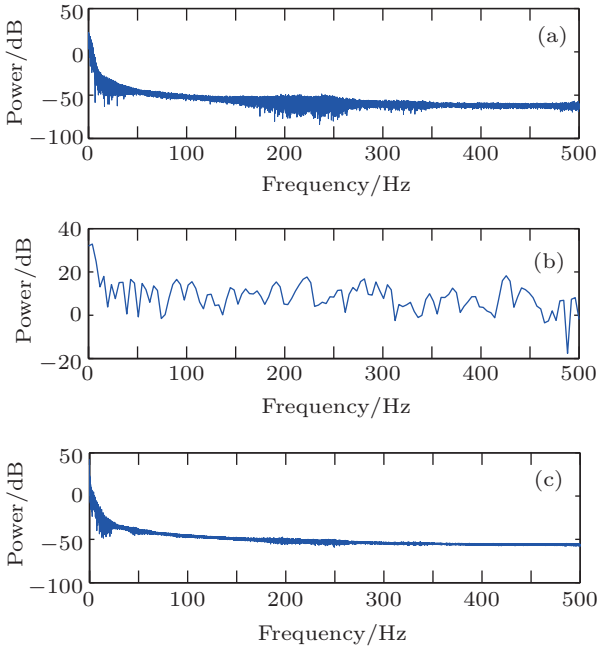


Fig. 6. (color online) Power spectra of Lorenz chaotic signal x, image signal $m(t)$, and masked signal $s(t)$. (a) Periodogram power spectral density estimate of x, (b) periodogram power spectral density estimate of the image signal, and (c) periodogram power spectral density estimate of the masked signal.

3.4. Low pass filtering on a masked image

The masked signals $s(t)$ based on Qi hyper-chaos and Lorenz chaos are fed into low pass filters respectively that attenuate (reduces the amplitude of) a signal masked with high frequencies higher than the cutoff frequency. After filtering $s(t)$, a low frequency signal is obtained. The unmasked signal using the filter for the Qi hyper-chaos based signal is totally

different from our original signal as shown in Fig. 7 where the blue line represents the original signal and the dotted red line represents the filtered signal. However, the image signal $m(t)$ masked by the Lorenz chaos is successfully extracted using the same low-pass filtering attack as shown in Fig. 8. Except for the difference in amplitude between the original image signal $m(t)$ and the filtered signal, the two signals have the same characteristics. Therefore, the Lorenz based image convolutional masking scheme cannot resist a low-pass filtering attack, as shown in Figs. 7 and 8.

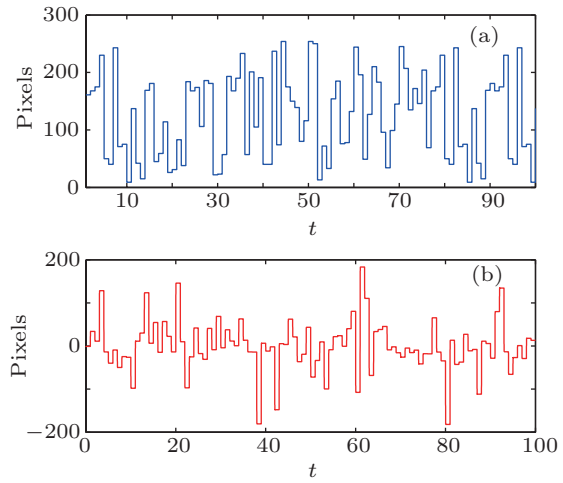


Fig. 7. (color online) Low-pass filtering attack of the Qi based image masking scheme: (a) original image signal and (b) unmasked image signal using a low pass filter.

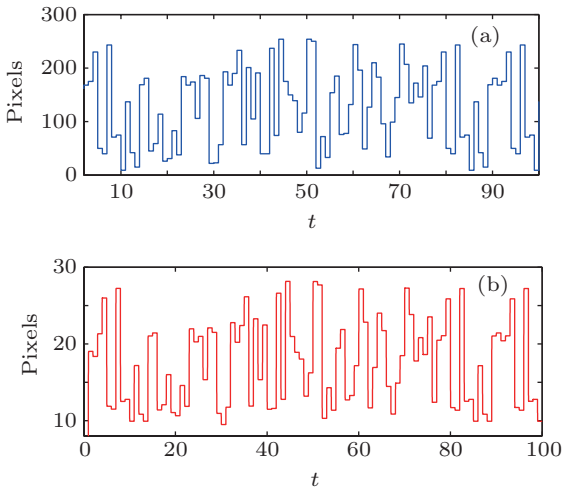


Fig. 8. (color online) Low-pass filter attack of the Lorenz based image masking scheme: (a) original image signal and (b) unmasked image signal using a low pass filter.

4. Synchronization based unmasking

Two unmasking methods are proposed in the paper: one method is based on synchronization, and the other does not employ synchronization but uses the information of the estimated derivative of the received signal. To make two systems keep synchronization, most controllers are designed by the use of specific chaotic systems. The controllers, such as pole assignment, are dependent on the models of the chaotic systems.

4.1. MHODFC and synchronization

A model free controller is applied in the synchronization in the paper. The model free controller is the multi higher-order differential feedback controller (MHOFDC)[12], which is simply described as below.

Consider a driving chaotic system as

$$\dot{x}_i = f_i(x,t), \quad i = 1,\ldots,n, \tag{3}$$

where $x = [x_1,\ldots x_n]^{\mathrm{T}}$ is the state variable vector, and a response chaotic system as

$$\dot{x}_{\mathrm{r}i} = f_i(x_{\mathrm{r}},\ t), \quad i = 1,\ldots,n, \tag{4}$$

where $x = [x_{\mathrm{r}1},\ldots,x_{\mathrm{r}n}]^{\mathrm{T}}$ is the state variable vector of the response system. Define error and error derivative as

$$e_i = x_i - x_{\mathrm{r}i}, \quad \dot{e}_i = \dot{x}_i - \dot{x}_{\mathrm{r}i}, \tag{5}$$

and the estimates of error and error derivative as

$$\hat{e}_i = \hat{x}_i - \hat{x}_{\mathrm{r}i}, \quad \hat{\dot{e}}_i = \hat{\dot{x}}_i - \hat{\dot{x}}_{\mathrm{r}i}, \tag{6}$$

$$\hat{E}_i = [\hat{e}_i\ \hat{\dot{e}}_i]^{\mathrm{T}}. \tag{7}$$

Using the HOD,[12,14] we estimate the first-order derivatives of both driving and response systems as

$$\begin{cases} \dot{z}_i = z_{i+1} + a_i(x - z_1), & 1 \le i \le n_0 - 1, \\ \dot{z}_{n_0} = a_{n_0}(x - z_1), \end{cases} \tag{8}$$

$$\begin{cases} \hat{x} = z_1, \\ \hat{x}^{(i)} = z_{i+1} + a_i(x - z_1), & i = 1,\ \ldots,\ n, \end{cases} \tag{9}$$

where n_0 is the order of the HOD, $n_0 \ge n+1, z_1, z_2, \ldots, z_{n_0}$ are the states of the HOD, a_i $(i = 1,\ldots,n_0)$ are the parameters and $\hat{x}^{(i)}$ denotes the estimate of $x^{(i)}$, and all parameters can be calculated using

$$\begin{cases} a_i = MC_{n_0}^{i-1}\alpha^{i-1}, \\ M = n_0^{n_0}\alpha/(n_0-1)^{n_0-1}, & i = 1,\ 2,\ldots,\ n_0, \end{cases} \tag{10}$$

where C_j^i is the combination expression, α is an adjustable parameter, and the precision of derivative estimation is increased by increasing the value of α and $n_0 = 5$ is taken in the specific design. Note that the HOD is independent of the model of the system rather than the signal x. In addition, it can extract the n-th order derivative of x, provided that: $n_0 \ge n+1$.[12,14]

In the synchronization process of a Qi hyper-chaotic system, we choose a 4D chaotic system[12,15]

$$\begin{cases} \dot{x}_{\mathrm{r}1} = a_1(x_{\mathrm{r}2} - x_{\mathrm{r}1}) + x_{\mathrm{r}2}x_{\mathrm{r}3}x_{\mathrm{r}4} + u_1, \\ \dot{x}_{\mathrm{r}2} = b_1(x_{\mathrm{r}1} + x_{\mathrm{r}2}) - x_{\mathrm{r}1}x_{\mathrm{r}3}x_{\mathrm{r}4} + u_2, \\ \dot{x}_{\mathrm{r}3} = -cx_{\mathrm{r}3} + x_{\mathrm{r}1}x_{\mathrm{r}2}x_{\mathrm{r}4} + u_3, \\ \dot{x}_{\mathrm{r}4} = -dx_{\mathrm{r}4} + x_{\mathrm{r}1}x_{\mathrm{r}2}x_{\mathrm{r}3} + u_4, \end{cases} \tag{11}$$

as a response system. Actually, we can choose any other 4D systems for the model-free controller, i.e., MHODFC designed as[12]

$$u_i = K_i \hat{E}_i + \hat{u}_i, \tag{12}$$

which is not dependent on the driving system. Here, $\hat{u}_i$ is the filtering value of u_i and can also be filtered by the HOD or other filters, K_i is a Hurwitz polynomial form to make a closed loop system stable. The controller is stable and ensures that the response tracks the reference asymptotically. The stability and convergence were proved in Ref. [12]. From Eq. (12), it does not contain the model information other than $\hat{E}_i = [\hat{e}_i\ \hat{e}_i]^{\mathrm{T}}$ which can be obtained using HOD and $\hat{u}_i$. In the case of the synchronization, $K_i = [20,\ 1]$, $i = 1,\ 2,\ 3,\ 4$ is taken for the controller, and $\alpha = 15$ is taken for the HOD parameter.

The synchronization of the response system to the driving system is shown in Fig. 9 where the x_1 tracks $x_{\mathrm{r}1}$ rapidly within $t \leq 0.01$.

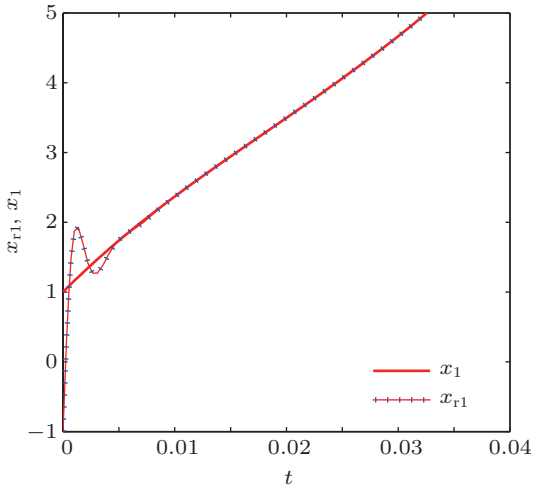


Fig. 9. (color online) synchronization of x_1 and $x_{\mathrm{r}1}$.

4.2. Unmasking

Since $\lim_{t\to\infty} x_i(t) = x_{\mathrm{r}}(t)$ and $\lim_{t\to\infty} \dot{x}_i(t) = \dot{x}_{\mathrm{r}}(t)$ under the control law (12) are ensured, from the first equation of Eq. (1), can be used to unmask the message $m(t)$ masked by the Qi hyper chaos

$$\tilde{m}(t) = \dot{x}_1 - [a(x_{\mathrm{r}2} - x_{\mathrm{r}1}) + x_{\mathrm{r}2}x_{\mathrm{r}3}]. \tag{13}$$

It requires that the first equation of the driving system must be communicated between the sender and the receiver. After unmasking, $\tilde{m}(t)$ is reshaped into an $I \times J$ ciphered image. The decryption process is performed using the same keys as the encryption process.

4.3. Results

The successful masking using Qi hyper-chaos and unmasking using the MHODFC is shown in Fig. 10; the signal $m(t)$ is successfully recovered from the masked signal $s(t)$.

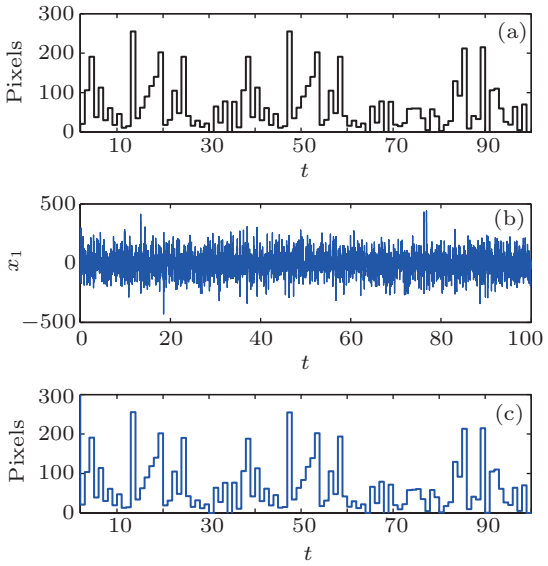


Fig. 10. (color online) Original image signal, the masked signal $s(t)$ and the unmasked ciphered image based on Qi hyper-chaos. (a) Original signal, (b) masked signal, and (c) unmasked signal.

5. Hod based unmasking

Suppose that at the receiving end, $s(t)$ only contains $x_i(t)$, $i = 1,2,3,4$, but $\dot{x}_1(t)$ is not sent by the sender; to extract the message $m(t)$, $\dot{x}_1$ should be estimated. The HOD can be used to estimate $(\dot{x}_1,\ \dot{x}_2,\ \dot{x}_3,\ \dot{x}_4)^{\mathrm{T}}$ which are the first order derivatives of the driving system using the algorithm in Eqs. (8)–(10). Therefore, the synchronization is exempted.

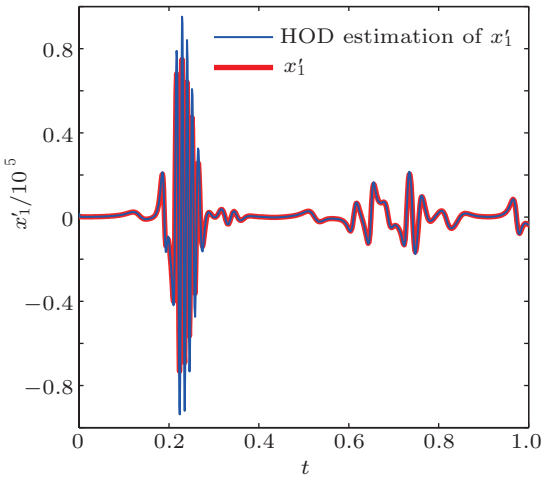


Fig. 11. (color online) HOD estimation of x_1', with $\alpha = 150$.

The estimation of the derivative information from the driving system using the HOD is shown in Figs. 11 and 12.

The states of the driving system $(x_1,\ x_2,\ x_3,\ x_4)^{\mathrm{T}}$ are the inputs of the HOD respectively, therefore the first-order states of $(\hat{x}_1,\ \hat{x}_2,\ \hat{x}_3,\ \hat{x}_4)^{\mathrm{T}}$ are the estimates of $(\dot{x}_1,\ \dot{x}_2,\ \dot{x}_3,\ \dot{x}_4)^{\mathrm{T}}$. The Qi hyper-chaos is not easy to estimate due to its very wide frequency spectrum of the derivatives of state. The results have been tested with parameter $\alpha = 1505000$. The results indicate that with the increase of α, the precision of the estimation becomes more accurate, as shown in Figs. 11 and 12.

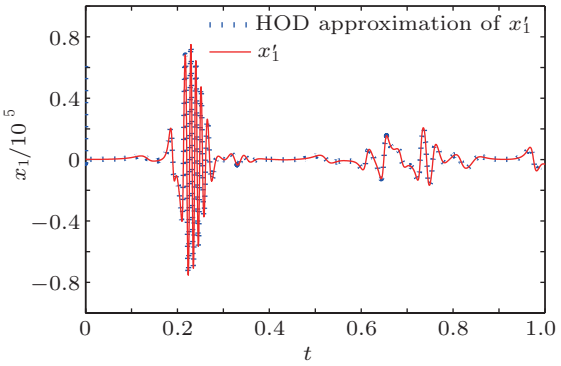


Fig. 12. (color online) HOD estimation of x_1', with $\alpha = 5000$.

The de-convolution process is depicted as

$$\tilde{m}(t) = \hat{x}_1 - [a(x_2 - x_1) + x_2 x_3]. \tag{14}$$

The successful unmasking using the HOD is shown in Figs. 13 and 14; as a result, the signal $m(t)$ is successfully recovered from the masked signal $s(t)$.

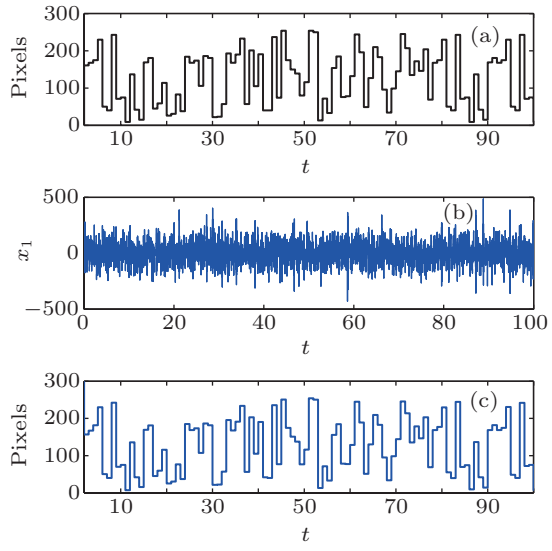


Fig. 13. (color online) Successful unmasking using HOD. (a) Original signal, (b) masked signal, and (c) unmasked signal using HOD.

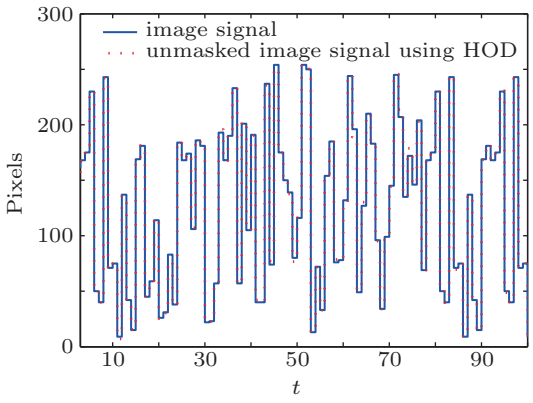


Fig. 14. (color online) Original signal and unmasked signal using HOD.

6. Conclusion

To secure data, a convolutional masking method has been used so that the image signal or its binary sequence could be hidden in the Qi hyper-chaotic system, which has a high disorder degree. The proposed algorithm resists against the known masking attacks via the filtering and power spectrum analysis. The masking scheme was tested using both Qi hyper-chaos and Lorenz chaos and indicated that Qi hyper-chaos based masking can resist attacks, while the Lorenz based scheme does not provide sufficient security to high amplitude data and is easily broken by the low-pass filtering method. Two unmasking methods were proposed in the paper: one method is based on synchronization, and the other does not employ synchronization but uses the information of the estimated derivative of the received signal. Simulations demonstrated the effectiveness of the two unmasking methods.

References

[1] Luo Y L and Du M H 2013 *Chin. Phys. B* **22** 080503
[2] Wang X Y and Xie Y X 2011 *Chin. Phys. B* **20** 080504
[3] You R Y and Huang X J 2011 *Chin. Phys. B* **20** 020505
[4] Qi G Y, van Wyk M A, van Wyk B J and Chen G R 2008 *Phys. Lett. A* **372** 124
[5] Pan J, Ding Q and Du B 2012 *Int. J. Bifurc. Chaos* **22** 1250125
[6] Grzybowski J M V, Rafikov M and Balthazar J M 2009 *Commun. Nonlinear Sci. Numer. Simul.* **14** 2793
[7] Lü L, Yu M, Wei L L, Wei L L and Li Y S 2012 *Chin. Phys. B* **21** 100507
[8] Ablay G and Aldemir T 2009 *IEEE Int. Conference in Electr. and Electro*. Eng., II-182
[9] Tang Q and Wang X Y 2010 *Chin. Phys. Lett.* **27** 030508
[10] Lu D and Wu R 2009 *Int. J. Nonlinear Sci.* **8** 67
[11] Wang S G and Zheng S 2013 *Chin. Phys. B* **22** 070503
[12] Qi G Y, Chen Z Q and Yuan Z Z 2005 *Phys. Lett. A* **344** 189
[13] Sparrow C 1982 *The Lorenz Equations: Bifurcations, Chaos and Strange Attractors* (New York: Springer-Verlag) p. 770
[14] Du S Z, van Wyk B J, Qi G and Tu C 2009 *Chaos Soliton. Fract.* **42** 1900
[15] Qi G Y, Du S Z, Chen G R and Chen Z 2005 *Chaos Soliton. Fract.* **23** 1671