Video encryption based on chaotic array system: working with image directly

Hongyan Zang and Jing Yang

Department of Mathematics and Physics,
University of Science and Technology Beijing,
Beijing, China
Email: zhylixiang@126.com
Email: m18810963307@163.com

Guodong Li*

School of Mathematics and Computational Science,
Guilin University of Electronic Technology,
Guilin, China
Email: lgdzhy@126.com
*Corresponding author

Abstract: A new three-dimensional discrete chaotic system is proposed according to the Marotto theorem in this paper. On this basis, a coupled array chaotic system is given as the drive system. Moreover, with the help of the bidirectional generalised synchronisation theorem, the response system is constructed and proved to be chaotic. According to the chaotic matrix generated by the above systems, a special video encryption scheme was proposed. While the experiment shows that the encryption scheme occupies a large key space and enjoys an approximately uniform distribution of the ciphertext entropy already, the main contribution of the new constructed system is the higher speed than the vector system since once the encryption starts, the chaotic matrix generated by the array systems and the image with the same size to the matrix can be operated directly.

Keywords: generalised synchronisation; video encryption; coupled array chaotic system; computing simulation.

Reference to this paper should be made as follows: Zang, H., Yang, J. and Li, G. (2020) 'Video encryption based on chaotic array system: working with image directly', *Int. J. Information and Communication Technology*, Vol. 16, No. 1, pp.84–97.

Biographical notes: Hongyan Zang is working as an Associate Professor in the Department of Mathematics and Physics, University of Science and Technology Beijing. Her research field includes theory of chaos and chaos synchronisation, chaos cryptography and analysis.

Jing Yang received his BSc in Information and Computing Science from the University of Science and Technology Beijing, Beijing China, where he is currently working toward his MSc degree with the Department of Mathematics and Physics. His research interests include the chaos theory and computer simulations.

Guodong Li received his PhD degree in the School of Information Engineer, Being University of Science and Technology in 2008. He is currently a Professor in the School of Application Mathematics of the Xinjiang University of Finance and Economic. His research interests include image encryption, cellular neural network and image processing.

1 Introduction

Chaos is a specific phenomenon in non-linear dynamics. It is an unpredictable motion which seems like randomly generated by a deterministic dynamic system and is sensitive to the initial value. Taking the advantages of the chaotic system, chaotic ciphers are widely applied in the field of information security (Yu et al., 2016). On the other hand, with the popularity of the network, it becomes more and more important to take a safe and effective transmission of information in commercial and military fields. And the video is one of the most important information carriers. However, it is also well-known that the video has a great number of data which are almost impossible to be completely transmitted in channel. And the algorithm has satisfying encryption effect on the text information is not fully applicable to the video encryption (Chaudhari et al., 2015).

In the field of discrete chaotic system theory research, in 1975, Li and Yorke proposed the famous theory of "period three implies chaos" and gave the definition of Li-Yorke chaos. After that, Marotto extended the results of the theorem to the n-dimensional Euclidean space and proved that the snap-back repellers would lead to chaos in the sense of Li-Yorke (Marotto, 1978). In 2002, the Marotto theorem is extended to the Banach space further (Shi and Chen, 2002). Since then, the Marotto theorem becomes the main theoretical basis for constructing high dimensional discrete chaotic systems (Han et al., 2011).

On the other filed, the generalised synchronisation (GS) theory of chaotic system and its research in secure communication has been developed rapidly in recent years (Srinivasan et al., 2016). In 2014, a chaotic GS theorem was proposed in the form of discrete arrays by Zang et al. (2009), it solved the problem of the construction of general GS system. On their research, a GS system is constructed with the known chaotic systems based on their theorem. The result of experiment showed that it greatly improved the complexity and randomness of the chaotic sequence for encryption. Inspired by their great research, we developed our work in this paper by constructing a new system and applying the result to the video encryption.

On the research of video encryption, researchers improved the traditional encryption algorithm and proposed many algorithms to encrypt the original digital video data (Lian, 2009). In recent years, with the popularity of H.264 coding, researchers attempted to combine the encryption algorithm with video coding based on the traditional encryption algorithm and achieved a valid result (Hamidouche et al., 2017).

The video encryption algorithm in this paper encrypts image data with less operation. The result of experiments shows that it has a high security level. And it provides a new significant view to make a fast and safe video encryption.

2 GS chaotic systems with array form

2.1 A new three-dimensional discrete chaotic system

Consider the autonomous discrete system

$$X(k+1) = g(X(k)) \quad X(k) \in R^n,\ k = 0, 1, 2, \ldots$$

The following theorem was proposed:

Lemma 1 If the *n*-dimensional map *g* has a snap-back repeller, then g is chaotic in the sense of Li-Yorke (Marotto, 1978).

According to the *Marotto Theorem*, the following *Theorem 1* is given:

Theorem 1: Choosing the parameters as $a = 0.8$; $a_1 = 0.3$; $a_2 = 0.15$, $b = 1.1$; $b_1 = 0.2$; $b_3 = -0.4$, $c = 1.4$; $c_1 = 0.5$; $c_2 = 0.45$, then the system

$$X(k+1) = g\left(X(k)\right) = \begin{pmatrix} ax_1(k) + a_1 x_2^2(k) + a_2 x_2(k) x_3(k) \\ bx_2(k) + b_1 x_1(k) x_3(k) + b_2 x_3(k) \\ cx_3(k) + c_1 x_1^2(k) + c_2 x_1(k) x_2(k) x_3(k) \end{pmatrix} (\mathrm{mod}\, 1) \tag{1}$$

is chaotic in the sense of Li-Yorke.

Proof: It is clear that in equation (1), $g(0) = 0$,so $X^* = 0$ is a fixed point of *g*. Then we need to prove $X^* = 0$ is a snap-back repeller of *g*.

First, consider the equation:

$$h(X) = g(X) - A$$

where $A = (1, 1, 1)^T$. Under the effect of module 1 operation, $0 \le X(k) \le 1$, define .

1 while $X_0 = 0$,we have $h(X_0) = -1 < 0$.

2 while $X_1 = 1$, we have $h(X_1) = g(X_1) - 1 = (a_1 + a_2 + a_3 + {}_{\mathrm{a}},\ b_1 + b_2 + b_3 + b,\ c_1 + c_2 + c_3 + c)^T - 1 > 0$(Wang and Chen, 2000).

According to the intermediate value theorem, $\exists\ 0 < X_1(k) < 1$, s.t.

$$h\left(X^1(k)\right) = g\left(X^1(k)\right) - A = 0$$

so

$$g\left(X^1(k)\right) = A$$

and

$$X^1(k+1) = g\left(X^1(k)\right)(\mathrm{mod}\, 1) = 0$$

Taking the auxiliary functions into the consideration:

$$\overline{h}\left(X\right) = g(X) - X^1(k)$$

then

$$\overline{h}(0) = -X^1(k) < 0, \overline{h}\left(X^1(k)\right) = g\left(X^1(k)\right) - X^1(k) = A - X^1(k) > 0$$

According to the n-dimensional intermediate value theorem, $\exists\ 0 < X^0(k) < X^1(k)$, s.t.

$$\overline{h}\left(X^0(k)\right) = g\left(X^0(k)\right) - X^1(k) = 0$$

So

$$X^1(k) = g(\left(X^0(k)\right)(\text{mod}1)$$

and $X^1(k + 1) = g(X^1(k))(\text{mod}1)$. Then make the system (1) iterate from $X^0(k)$, under the effect of module 1 operation, after two iterations, $X^1(k + 1)$. Define $X^* = 0$, so that $g^m(X^0(k) = X^*)$, where $m = 2$. And the fixed point $X^* = 0$ satisfies the following two properties:

1 Choose $r = \| X^1(k)\|$, s.t., $X^0(k) \in (0, X^1(k))$ and $X^* = 0$ in the neighbourhood of $B_r(X^*)$, where the Jacobian matrix of arbitrary point X, $D_g(x_k)$ is

$$Dg(x_k) = \begin{pmatrix} 0.8 & 0.6x_2 + 0.15x_3 & 0.15x_2 \\ 0.2x_3 & 1.1 & 1.1x_1 - 0.4 \\ x_1 & 0.45x_1x_3 & 1.4 + 0.45x_1x_2 \end{pmatrix}$$

According to the Disc Theorem, $\forall\ X \in B_r(X^*)$, the all eigen values of $Dg(x_k)$ are greater than 1.

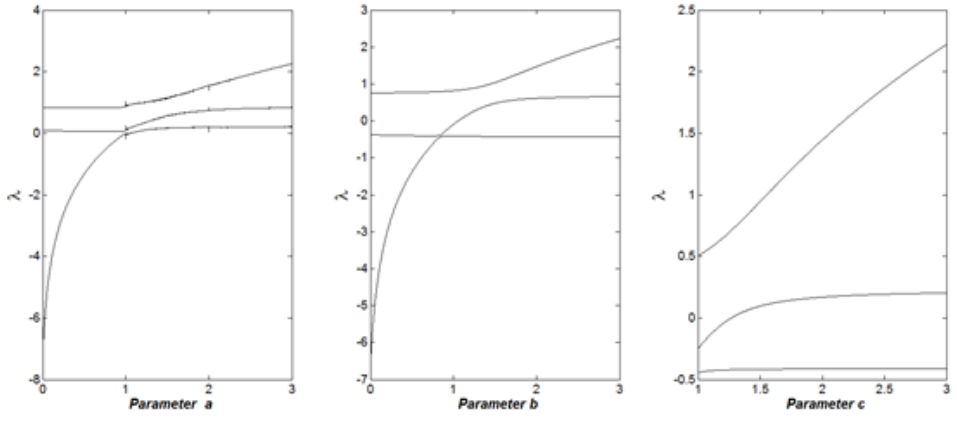
Notice that without considering the discontinuous points, the derivation of modular functions is consistent with the derivation results under normal conditions.

2 $\exists\ X^0(k)$ in $B_r(X^*)$ and $m = 2$,s.t. $g^m(X^0(k))$ and $X^0(k)$ is non-degenerate, i.e.,

$$\det\left\{Dg^m\left(X^0(k)\right)\right\} = \det\left\{Dg\left(X^0(k)\right)\right\} \cdot \det\left\{Dg\left(X^0(k+1)\right)\right\} \neq 0$$

According to the definition of snap-back repeller, $X^* = 0$ is a snap-back repeller of the mapping g. Therefore, on the basis of the Marotto Theorem, the system (1) is chaotic in the sense of Li-Yorke.

Figure 1 The Lyapunov exponents of system (1)



Lyapunov exponent is a numerical characteristic that represents the average exponential divergence rate of adjacent trajectories in phase space and it is one of the numerical characteristics used to identify chaotic motion. As shown in Figure 1, when the parameter is within a certain range, the three Lyapunov exponents of the system (1) are positive, so the system (1) exhibits chaotic characteristics.

2.2 GS theorem for coupled array chaotic system

A bidirectional discrete array of chaos systems consists of two parts:

$$X(k+1) = F(X(k), Y(k)) = \left(f_{1_{i,j}}(X(k), Y(k)\right), \ldots, f_{n_{i,j}}(X(k), Y(k)))^T \tag{2}$$

$$Y(k+1) = G(X(k), Y(k)) = \left(g_{1_{i,j}}(X(k), Y(k)\right), \ldots, g_{m_{i,j}}(X(k), Y(k)))^T \tag{3}$$

where

$$X(k) = \left(X^1(k), \ldots X^n(k)\right)^T = \left(\left(x_{l_{i,j}}(k)\right)_{M\times N}, \ldots, \left(x_{n_{i,j}}(k)\right)_{M\times N}\right)^T$$

$$Y(k) = \left(Y^1(k), \ldots Y^m(k)\right)^T = \left(\left(y_{l_{i,j}}(k)\right)_{M\times N}, \ldots, \left(y_{m_{i,j}}(k)\right)_{M\times N}\right)^T$$

$$i = 1, 2, \ldots, M; \quad j = 1, 2, \ldots, N; \quad m \le n$$

And then the following theorem was proposed:

Theorem 2: The systems defined by equations (2) and (3) are said to be in GS with respect to a transformation H: $R^{m\times M\times N} \to R^{m\times M\times N}$, then the $G(Y(k), X(k)$ in equations (3) has the following equation:

$$G(Y(k), X(k)) = H\left(F_m(X(k), Y(k))\right) - Q(Y(k), X(k))$$

where

$$F_m(X(k)), Y(k)) = \left(f_{1_{i,j}}(Y(k), X(k))\right)_{M\times N}, \ldots, f_{m_{i,j}}\left(Y(k), X(k)_{M\times N}\right)^T$$

define

$$Q(X(k), Y(k)) = \left(q_{1_{i,j}}(Y(k), X(k))\right)_{M\times N}, \ldots, q_{m_{i,j}}\left((Y(k), X(k))_{M\times T}\right)^T$$

which makes the zero solution of error equation $e(k + 1) = H(X_m(k + 1)) - Y(k + 1)$ be asymptotic stability (Zang et al., 2009).

This theorem gives a general mathematical expression for response systems with GS with known drive systems for bidirectional discrete array of chaos systems.

From the above theorem, we consider the array form of system (1):

$$X(k+1) = \begin{pmatrix} ax_{1_{i,j}}(k) + a_1 x_{2_{i,j}}^2(k) + a_2 x_{2_{i,j}}(k) x_{3_{i,j}}(k) \\ bx_{2_{i,j}}(k) + b_1 x_{1_{i,j}}(k) x_{3_{i,j}}(k) + b_2 x_{3_{i,j}}(k) \\ cx_{3_{i,j}}(k) + c_1 x_{1_{i,j}}^2(k) + c_2 x_{1_{i,k}}(k) x_{2_{i,j}}(k) x_{3_{i,j}}(k) \end{pmatrix} (\mathrm{mod}\, 1) \tag{4}$$

Add coupling term to equation (4)

$$X(k+1)=\begin{pmatrix} ax_{1_{i,j}}(k)+a_1x_{2_{i,j}}^2(k)+a_2x_{2_{i,j}}(k)+py_{1_{i,j}}(k) \\ bx_{2_{i,j}}(k)+b_1x_{1_{i,j}}(k)x_{3_{i,j}}(k)+b_2x_{3_{i,j}}(k) \\ cx_{3_{i,j}}(k)+c_1x_{1_{i,j}}^2(k)+c_2x_{1_{i,k}}(k)x_{2_{i,j}}(k)x_{3_{i,j}}(k) \end{pmatrix}(\mathrm{mod}1) \tag{5}$$

Considering non-linear reversible transformation H: $R^{2\times M\times N}\to R^{2\times M\times N}$

$$\left(y_{1_{i,j}}, y_{2_{i,j}}\right)^T=H\left(x_{1_{i,j}}, x_{2_{i,j}}\right)=\begin{pmatrix} \tanh\left(x_{1_{i,j}}\right)+\dfrac{u}{\sqrt{1+e^{-x_{2_{i,j}}}}}, v*\tanh\left(x_{1_{i,j}}\right) \\ +\dfrac{1}{\sqrt{1+e^{-x_{2_{i,j}}}}} \end{pmatrix}^T \tag{6}$$

Let $u = 1$; $v = 0.5$ here equation (5) can be written to the following form:

$$\begin{aligned} &X(k+1)= \\ &\left(f_{1_{i,j}}(X(k),Y(k))\right)_{M\times N}, f_{2_{i,j}}(X(k),Y(k))_{M\times N}, f_{3_{i,j}}\left(X(k),Y(k)_{M\times N}\right)^T \end{aligned} \tag{7}$$

$$Y(k+1)=G(Y(k),X(k)=\left(g_{1_{i,j}}(Y(k),X(k))\right)_{M\times N}, g_{2_{i,j}}\left(Y(k),X(k)_{M\times N}\right)^T \tag{8}$$

Then equations (7) and (8) are in GS with respect to H. Therefore, the response system has the form:

$$G(Y(k),X(k))=H\left(F_2(X(k),Y(k))\right)-(Q(Y(k),X(k)))_{2\times M\times N} \tag{9}$$

where

$$Q=\frac{1}{8}e(k)=\frac{1}{8}\left(H\left(F_2(X(k),Y(k))\right)-Y(k)\right).$$

2.3 Simulation

Select parts of variables of the drive-response systems, i.e., equations (5) and (9) to have a MATLAB numerical simulation for 1,000 iterations. The results are as Figures 2 to 4.

Figure 2 The chaotic trajectories of the state variables

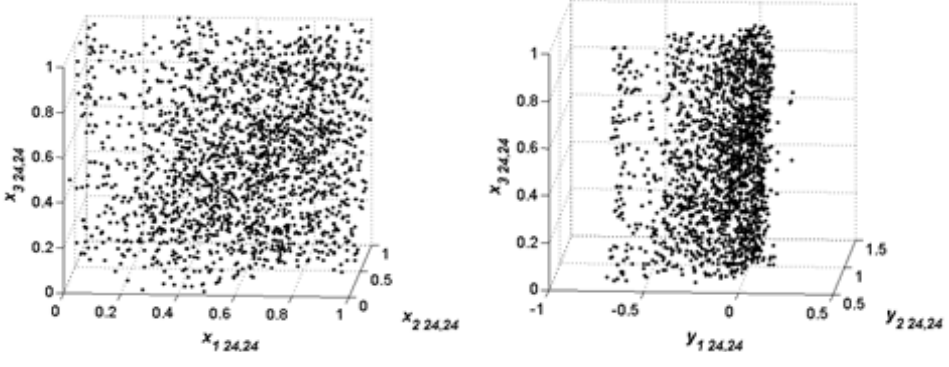
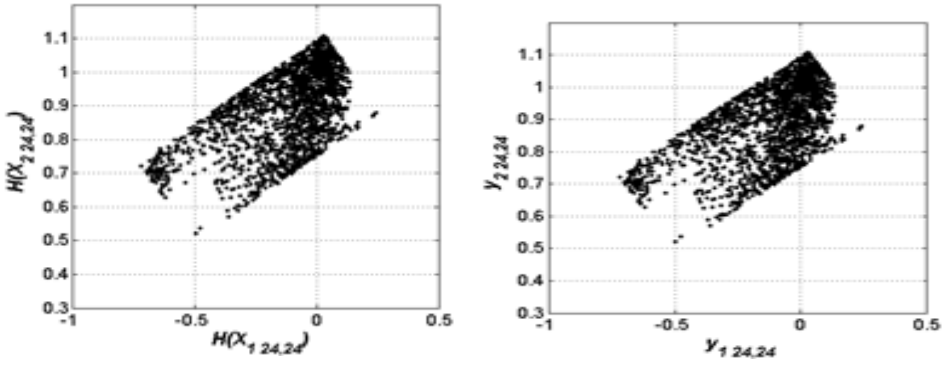


Figure 2 The chaotic trajectories of the state variables (continued)



From Figure 2(c) and 2(d) and Figure 3(a) and 3(b), it is clear that the state variables $x_{1_{i,j}}, x_{2_{i,j}}$ and $y_{1_{i,j}}, y_{2_{i,j}}$ have the synchronisation relationship with respect to H. And from the Figure 4, we can see that the selected two adjacent points of the same state variables sometimes are close to each other and sometimes are far away from each other.

Figure 3 The synchronisation diagrams

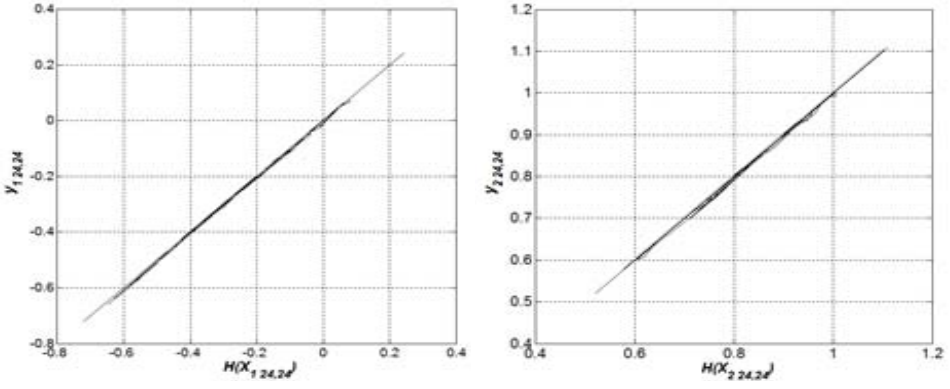


Figure 4 The iterative trajectories of adjacent position variables

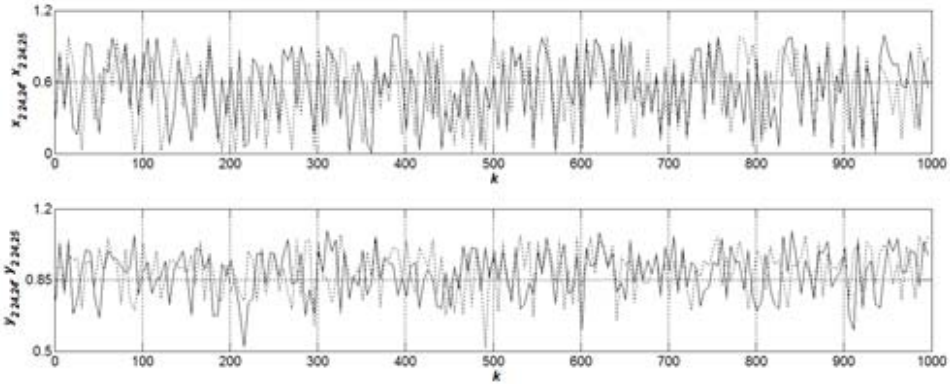
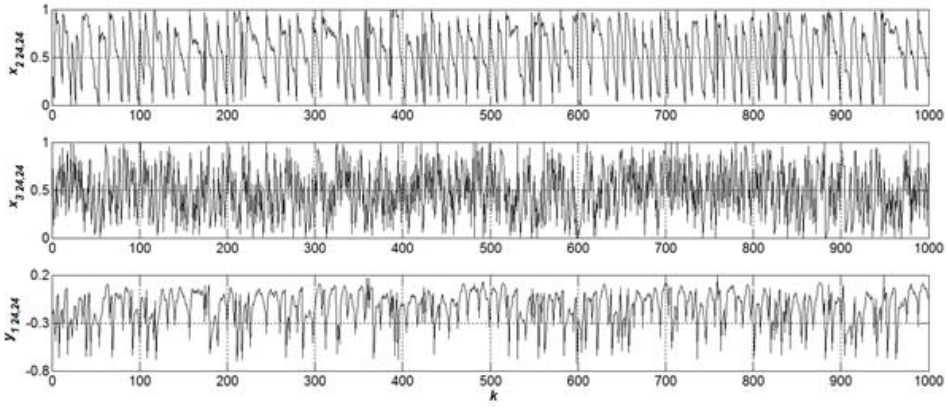


Figure 5 The iterative trajectories of some state variables



2.4 Randomness test

Select the sequences that come from the iteration result of the state variable $x_{2_{i,j}}$, $x_{3_{i,j}}$, $y_{1_{i,j}}$ at the cell position (i_0, j_0) and compute the sum of $R(k) = x_{2_{i0,j0}}(k) + x_{3_{i0,j0}}(k) + y_{1_{i0,j0}}(k)$, and then make the following transformation:

$$T(R(k)) = \mathrm{mod}\left(round\left(\frac{BIG\_NUM * (R(k) - \min(R(k)))}{\max(R(k)) - \min(R(k))} \right), 256 \right)$$

The $T(R(k))$ should be converted into 0–1 sequence and then the pseudo-random performance of the pseudo-random sequence generated by the proposed system can be tested by the FIPS 140-2 standard which is widely used in the world. The result is as follows:

Table 1 the result of FIPS140-2

Test term	*min*	*FIPS 140-2 permit interval*	*min*	*max*	*mean*	*Modified permit interval*
MT	0	9,725–10,275	9,756	10,237	10,000	9,725–10,275
	1	9,725–10,275	9,763	10,244	10,000	9,725–10,275
PT	–	2.16–46.17	4	39	15	2.16–46.17
LT	0	<26	10	24	14	<26
	1	<26	10	23	13	<26
1	0	2,315–2,685	2,353	2,637	2,499	2,362–2,638
	1	2,315–2,685	2,343	2,699	2,498	2,362–2,638
2	0	1,114–1,386	1,153	1,356	1,249	1,153–1,347
	1	1,114–1,386	1,149	1,352	1,249	1,153–1,347
3	0	527–723	552	700	624	556–694
	1	527–723	552	704	625	556–694

Table 1 the result of FIPS140-2 (continued)

Test term	*min*	*FIPS 140-2 permit interval*	*min*	*max*	*mean*	*Modified permit interval*
4	0	240–384	261	370	312	264–361
	1	240–384	265	368	313	264–361
5	0	103–209	118	199	157	122–191
	1	103–209	122	193	156	122–191
6+	0	103–209	125	199	156	122–191
	1	103–209	123	202	156	122–191

The sequence was tested 1,000 times in a particular experiment, all of the 1,000 times passed the test under the original standard and 24 times were not passed under the modified standard (Min et al., 2013). The passing rate reached 100% and 97.6% respectively. Since the initial values of X_0 in equation (5) have random terms, the completely same result as Table 1 cannot be repeated. However, from the average result of many times of experiments, we still come to the conclusion that the sequence produced by equations (5) and (9) have satisfying pseudo-random properties.

3 Video encryption scheme

3.1 Encryption procedure

Based on equations (5) and (9), we give the following video encryption scheme.

Supposing the frames of the original video is P, the resolution of each frame is $H*W*C$, where H represents the height, W represents the width and C represents the channels. Notice that our aim is to encrypt a series of images, instead of a video files, we can regard the video as P 3-dimentional matrixs, named as Plain $H*W*C$. Defining the key set of the chaotic systems (5) and (9) is keys = $\{a_1, a_2, a_3, b_1, b_2, b_3, c_1, c_2, c_3, a, b, c, p, u, v, X_0(l), m\}$, l = 1, 2, 3. Then we can encrypt the video as follows:

Step 1 Give the state variable and in equations (7) and (8) the same size as $H*W$ since Plain $H*W*C$ is known.

Step 2 Set the iteration times of equations (7) and (8), for example, 100 times. And choose C, for example, 3 of all the variables among $x_{l_i,j}$ and $y_{r_i,j}$, and their last P iterations of the 100 iterations. Thus we can obtain a 4-dimentional matrix with the size of $H*W*C*P$. Notice that the elements of the matrix is much smaller than that in $Plain_{H*W*C}$, so we multiplied it by a large number m which is in the keys and we name the new matrix as $Encry_{H*W*C*P}$.

Step 3 Encrypt the video as follows:

$$Ciper_{H*W*C}(k) = \mathrm{mod}\left(round\left(Plain_{H*W*C}(k) + Encry_{H*W*C*k}\right), 256\right); k = 1, 2, \ldots P$$

where $Plain_{H*W*C(k)}$ is the kth frame of the original video, $Encry_{H*W*C*k}$ is the kth submatrix of 4-dimentional encrypted matrix and $Ciper_{H*W*C(k)}$ is the kth frame of the

encrypted video. Taking a simple processing of all the P encrypted images, then the encrypted video can be obtained.

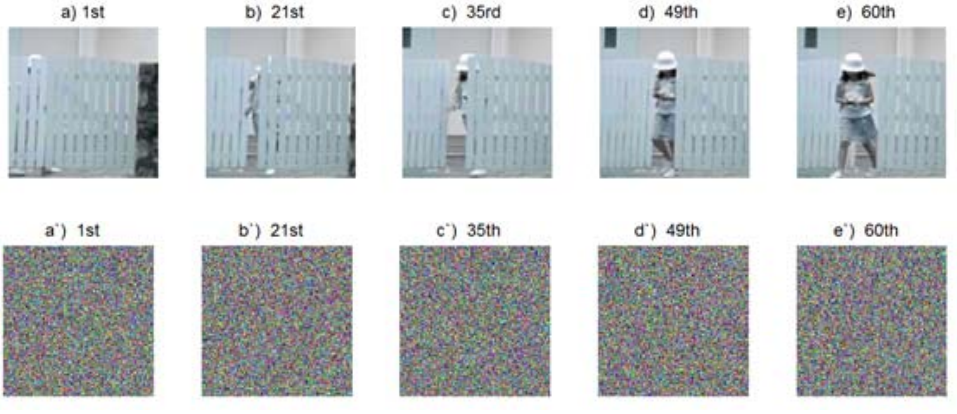
If anyone wants to decrypt the encrypted video, he should get the system (5) and (9) and receive the correct key set. Then he can decrypt the encrypted video as follows:

$$Decry_{H*W*C}(k) = \mathrm{mod}\left(round\left(Ciper_{H*W*C}(k) - Encry_{H*W*C*k}\right), 256\right); k = 1, 2, \ldots P$$

Similarly, after a simple processing, the decrypted images $Decry_{H*W*C}(1)$~$Decry_{H*W*C}(P)$ can be composed into the decrypted video.

Figures 6 and 7 shows some plaintext images and corresponding ciphertext images produced during the process of encryption and decryption.

Figure 6 Some frames in the original video and corresponding frames after encryption (see online version for colours)

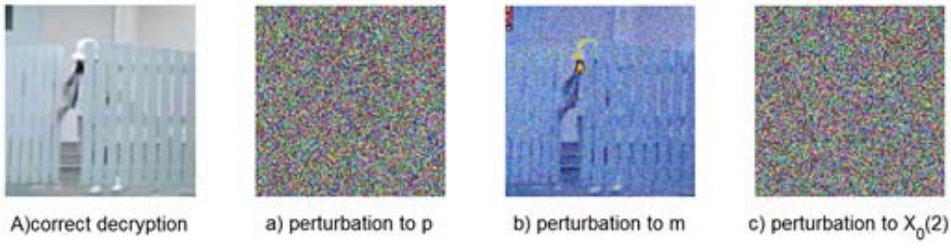


3.2 Key sensitivity

In order to resist the difference attack, the encrypted video must have a high sensitivity to the key of the chaotic systems, that is to say, making a small disturbance to the key may lead to the completely failure of the decryption, thus ensuring the security of the algorithm. The numerical simulation results show that the encryption algorithm in this paper is sensitive to the parameters in the key set keys. In the experiment, selecting parameters $p = 0.001$, $m = 314159265358$ and $X_0(2) = 0$ to have slight perturbation. The result is shown in Figure 8. It can be seen that the encryption scheme has a different sensitivity to the selected parameters. However, by testing all the parameters in the *keys*, we find our scheme main is sensitive to most parameters.

(A) is the a certain one frame decrypted with the correct key in *keys* and (a) (b) (c) is the corresponding frame decrypted after some parameter perturbation in the key set *keys*. (a) perturbation of parameter p with 10^{-15} (b) perturbation of parameter m with 10^{-15} and (c) perturbation of the parameters $X_0(2)$ with 10^{-15}.

Figure 7 Decryption with perturbation, (a) correct decryption (b) perturbation to p (see online version for colours)



3.3 Key space analysis

The ideal encryption scheme should make the key space as large as possible, so as to resist exhaustive attack. We conducted the sensitivity tests of each parameter in *keys*, we find that the parameters $\{a, a_1, a_2, b, b_1, b_2, c, c_1, c_2, X_0(l), p, u, m\}$, $l = 1, 2, 3$ are sensitive to the disturbance of 10^{-15} and the parameters m are sensitive to the disturbance of 10^{-9}. So the key space of *keys* achieves $10^{15\times15} \times 10^9 > 2^{777}$. The comparison of key space with the other schemes is shown in Table 2. It is clear that our encryption scheme has a much larger key space.

Table 2 Comparison of key space

	Ours	*Guan et al. (2005)*	*Chen et al. (2004)*	*Wang and Liu (2016)*	*Çavuşoğlu et al. (2016)*
Key space	2^{777}	2^{140}	2^{128}	2^{263}	2^{419}

3.4 Information entropy and statistical histogram

Information entropy is proposed by Shannon, which gives a metric of uncertainty of the data source. Suppose that $S = \{x_1, x_2, ..., x_n\}$ is an information source, P is the probability distribution on S and the probability of the occurrence of x_i is defined as p_i, then the information entropy of the source is defined as $H(S) = -\sum_{i=1}^{n} p_i \log p_i$. According to the maximum entropy principle, the maximum value of the entropy of each channel of the colour image is 8. If the information entropy of the encrypted picture is close to 8, the pixel values of the image almost obey the equal probability distribution. From Figure 8, the encrypted images always enjoy large information entropys extremely close to 8, concretely, all over 7.99 for each frame.

Selecting one of the video frames and drawing the histogram of the frequency distribution of pixel values before and after encryption, it can be seen that the distribution of the pixel value of the encrypted video image becomes uniform and close to the equal probability distribution, which is also greatly helpful to hide the plaintext information.

Figure 8 RGB information entropy of original frame (dotted line) and encrypted frame (solid line)

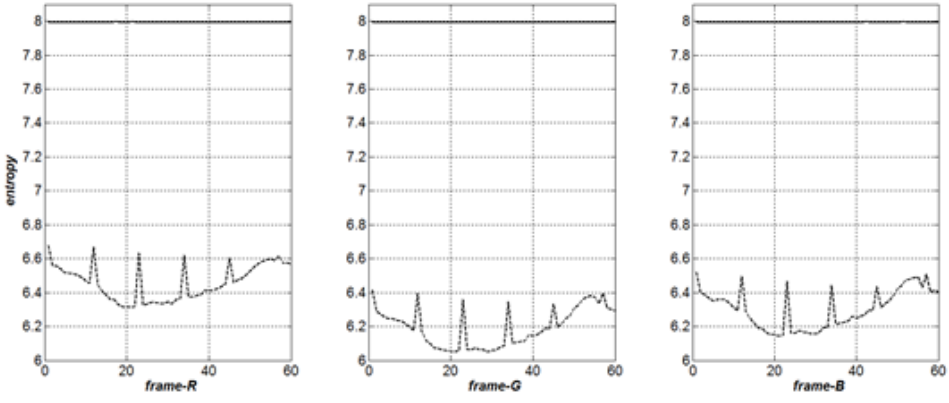


Figure 9 The frequency histogram of the 3rd frame RGB channels of the original video

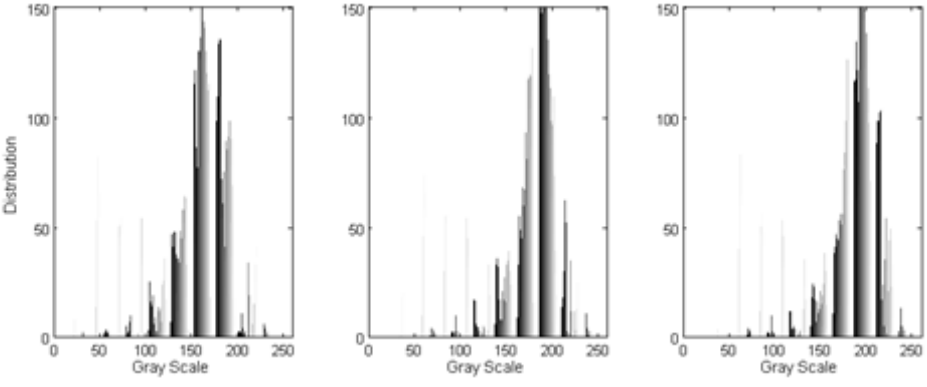
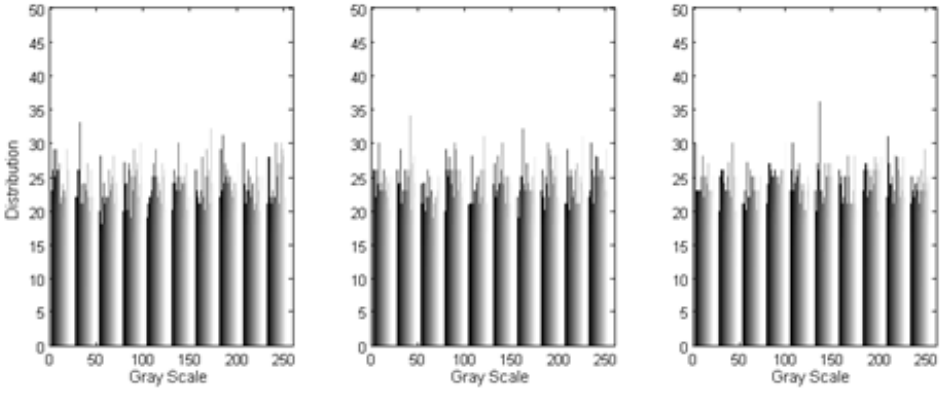


Figure 10 The frequency histogram of the 3rd frame RGB channels of the encrypted video



3.5 Time efficiency

We use the proposed array system to generate chaotic data and encrypt. Comparing to vector system, more data are generated within one iteration, but the time of iteration does not increase too much. And in the encryption stage, instead of reshaping a chaotic sequence to a matrix or flatting a matrix to a sequence before a series of arithmetic between chaotic data and plain text, as a chaotic sequence dose, the matrices generated by the proposed array system can work with the image matrices directly. Table 4 shows the comparison result of time efficiency between array system and vector system. The first column is the required average time (*ms*) to generate a set of encrypting data for one frame. The last two columns are average finish time for one encryption and decryption. Furthermore, the required average time for generating a 3-dimentional matrix for one frame plus the encrypting time makes about 0.4s, in other words, using the array system, we can encrypt about 25 images in a second ideally.

Table 3 Comparison of time efficiency

	Generate data	*Encryption*	*Decryption*
Array system	25.2	14.0	12.8
Vector system	193.5	15.4	15.4

4 Conclusions

In this paper, two discrete coupled array chaotic systems are constructed based on the Marotto theorem and the GS theorem. The 4-dimentional matrix for encryption is made up of the partial variables of two systems after a fixed times of iteration. The random test and the numerical simulation show that the sequence consists of the numbers at the same cell location in different iterations have positive characteristics of pseudorandom property. And the result of video encryption experiment shows that the encrypted video enjoys large information entropy and is extremely sensitive to the key and the key space of the system is over 2^{777}. Moreover, it can be seen that the proposed encryption algorithm in this paper can works efficiently with only 0.014 second for encrypting a frame of video and even have an opportunity to be applied to the real-time video encryption. As the major contribution, the chaotic coupled array system proposed may provide a new tool for video encryption algorithm.

Acknowledgements

The research was founded within the project No.06108236, entitled ‘The Fundamental Research Funds for the Central Universities’ and the project 2017D01A24, entitled ‘The Xinjiang Uygur Autonomous Region Natural Science Foundation’.

References

Çavuşoğlu, Ü., Akgül, A. and Kaçar, S. et al. (2016) 'A novel chaos‐based encryption algorithm over TCP data packet for secure communication', *Security and Communication Networks*, Vol. 9, No. 11, pp.1285–1296.

Chaudhari, S.A. and Bagde, M.D. (2015) 'Review on secret data hiding in encrypted compressed video bit streams', *International Journal of Computer Science Trends and Technology*, Vol. 3, No. 2, pp.94–96.

Chen, G., Mao, Y. and Chui, C.K. (2004) 'A symmetric image encryption scheme based on 3D chaotic cat maps', *Chaos Solitons and Fractals*, Vol. 21, No. 3, pp.749–761.

Guan, Z.H., Huang, F.J. and Guan, W.J. (2005) 'Chaos-based image encryption algorithm', *Physics Letters A*, Vol. 346, No. 1, pp.153–157.

Hamidouche, W., Farajallah, M. and Sidaty, N. (2017) 'Real-time selective video encryption based on the chaos system in scalable HEVC extension', *Signal Processing Image Communication*, Vol. 58, pp.73–86.

Han, S., Min, L. and Liu, T. (2011) 'Marotto's theorem-based chaotic pseudo-random number generator and performance analysis', *International Conference on Multimedia Technology*, pp.2500–2503.

Li, T.Y. and Yorke, J.A. (1975) 'Period three implies chaos', *Amer Math Monthly*, Vol. 82, No. 10, pp.985–992.

Lian, S. (2009) 'Efficient image or video encryption based on spatiotemporal chaos system', *Chaos Solitons and Fractals*, Vol. 40, No. 5, pp.2509–2519.

Marotto, F.R. (1978) 'Snap-back repellers imply chaos in Rn', *Math Anal Appl*. Vol. 63, No. 1, pp.199–223.

Min, L.Q., Chen, T.Y. and Zang, H.Y. (2013) 'Analysis of FIPS 140-2 test and chaos-based pseudorandom numbet generator', *Chaotic Modeling and Simulation*, No. 2, pp.273–280.

Shi, Y.M. and Chen, G.R. (2005) 'Discrete chaos in Banach spaces', *Science in China Series A: Mathematics*, Vol. 48, No. 2, pp.222–238.

Simin, Y.U., Jinhu, L. and Chengqing, L.I. (2016) 'Some progresses of chaotic cipher and its applications in multimedia secure communications', *Journal of Electronics and Information Technology*.

Srinivasan, K., Chandrasekar, V.K. and Pradeep, R.G. (2016) 'Different types of synchronization in coupled network based chaotic circuits', *Communications in Nonlinear Science and Numerical Simulation*, Vol. 39, pp.156–168.

Wang, X. and Liu, C. (2016) 'A novel and effective image encryption algorithm based on chaos and DNA encoding', *Multimedia Tools & Applications*, Vol. 76, No. 5, pp.1–17.

Wang, X.F. and Chen, G.R. (2000) 'Chaotifying a stable map via smooth small amplitude high-frequency feedback control', *International Journal of Circuit Theory and Applications*, Vol. 28, No. 3, pp.305–312.

Zang, H., Min, L. and Cao, L. (2009) 'An image encryption and digital signature scheme based on generalized synchronization theorem', *International Conference on Computational Intelligence and Security*, IEEE Computer Society, pp.504–510.