A Chaotic-based Encryption/Decryption System for Secure Video Transmission

Xin Huang, David Arnold, Tianyang Fang, and Jafar Saniie

Embedded Computing and Signal Processing (ECASP) Research Laboratory (http://ecasp.ece.iit.edu)
Department of Electrical and Computer Engineering
Illinois Institute of Technology, Chicago IL, U.S.A.

***Abstract*— Ultrasonic communication is an alternative communication method of transmitting information through solids. Sending video streams can deliver more information than a single sensor, and video monitoring shows great potential in ultrasonic communication applications. An efficient and secure cryptosystem is needed to protect the sensitive video stream. In this paper, we propose a novel Chaotic-based encryption scheme utilizing 1-D and 2-D iteration models for secure video streaming. This algorithm is based on the Arnold Cat Map and the Logistic Map and has good confusion and diffusion properties. The Arnold Cat Map transforms the dataset into a pseudo-random state over several iterations and is reversible, while the Logistic Map introduces a specific external key to replace and recover the pixels value during encryption and decryption. Both the encryption and decryption processes are presented and formulated in our cryptosystem scenario. The proposed method maintains a good encryption quality, provides key sensitivity, and has a low correlation between pixels. The results of a secured video frame using separate Chaotic Maps and the novel encryption scheme are compared and discussed. Experiments and analysis demonstrate that the Chaotic-based algorithm is best suited for the ultrasonic video communication system and is resilient to security attacks.**

I. Introduction

Ultrasonic communication through solid channels is a potential approach to overcoming physical barriers that prevent conventional wired or wireless communication [1] [2]. Sending video streams can deliver more information than a single sensor in scenarios such as the pharmaceutical or nuclear industries [3] [4]. Video monitoring has shown great potential in ultrasonic communication applications [5] [6] [7]. However, due to the limited transmission distance of ultrasonic waves [3] [8], the receiver will connect to traditional communication channels, such as ethernet or Wi-Fi, to send the video stream to a remote client. Thus, video encryption is needed to protect the confidentiality of the stream. Due to our video monitoring system structure, it is necessary to select a suitable cryptographic technique for the raw video stream. Figure 1 demonstrates the ultrasonic video communication architecture. The transmitter stays in a highly sealed environment and is full protected by the physical barrier. The video stream is transmitted through a solid channel. Therefore, no intruders can touch either the transmitter side or ultrasonic wave, while the receiver accesses the open channel and suffers from cybersecurity issues. Thus, it is fully secure to encrypt the video stream from a camera at the transmitter side. A Chaotic-based encryption method is robust for real-time implementation in secure communications. Chaotic Maps are studied in dynamic systems as they exhibit chaotic behavior [9] [10]. The techniques scramble and diffuse pixel information, which adds no redundancy to the original video stream. Thus, Chaotic-based encryption is efficient and suitable for ultrasonic video communication. These maps are categorized as discrete maps and continuous maps. Discrete maps usually utilize 1-D, 2-D, or 3-D iteration models, which possess important features such as ergodicity, quasi-randomness, sensitive dependence on initial conditions and system parameters [11] [12]. Additionally, Chaotic-based encryption utilizes variable keys to meet security requirements.

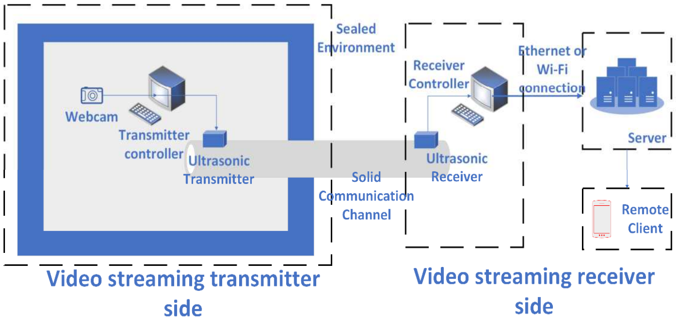

Figure 1. Ultrasonic Video Communication Architecture

A number of image encryption algorithms based on chaotic systems have been proposed. There are more than 100 types of Chaotic Maps. The main methods in Chaotic-based encryption algorithms are confusion and diffusion [12] [13] [14]. Confusion is achieved by changing the positions of the pixels. It can decrease the correlation between adjacent pixels and make the video frame unreadable and eavesdroppers. Diffusion is the process of substituting the value of each pixel with another value using a Chaotic-based map. Diffusion encryption can enhance the randomness and break the statistical characteristics of the original image. In this paper, we utilize two Chaotic Maps: the Arnold Cat Map (ACM) and the 1-D Logistic Map (LM) [9] [10] [15]. ACM is a discrete system that selects an area to be randomized by transformation and can be recovered to the original state after some iterations. The number of iterations can be used as a secret key. However, the changed positions alone cannot provide robust security due to the non-variance of the RGB distribution of a plain image. The 1-D LM is introduced to provide chaotic behavior to the encrypted image to enforce security [16]. The external key determines the initial conditions of ACM and LM. We demonstrate the encryption and decryption schemes using ACM and LM. The security analysis is done by using the histogram and correlation of the two horizontally adjacent pixels in a single video frame. The correlation coefficient results are compared and discussed to ensure the quality of the proposed Chaotic-based encryption for ultrasonic video communication.

The rest of the paper is organized as follows. In Section II, the encryption and decryption process of using ACM and LM is formulated and presented. In Section III, the security analysis of proposed Chaotic-based encryption is compared and discussed. Section V contains a summary and conclusion.

II. Proposed Chaotic Based Cryptosystem

A. Arnold Cat Map

The Arnold Cat Map can change the position of the pixel of an image without removing any information. The position of a pixel in the image can be expressed as (x,y) $\{x,y=0,1,2,3\ldots N\}$. The transformed pixel position based on ACM can be written as Equation (1)

$$\begin{bmatrix} \dot{x} \\ \dot{y} \end{bmatrix} = A \begin{bmatrix} x \\ y \end{bmatrix} (mod\ N) = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (mod\ N) \qquad (1)$$

Here, the determinant of A is 1, which makes it reversible. P and Q are integers. $(\dot{x}, \dot{y})$ is the mapped new position. The transformation randomizes and decreases the correlation between adjacent pixels. However, after a number of iterations, the image is back to the original state. The reverse mapping can be written as an Equation (2)

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} pq+1 & -p \\ -q & 1 \end{bmatrix} \begin{bmatrix} \dot{x} \\ \dot{y} \end{bmatrix} (mod\ N) \qquad (2)$$

The image rapidly degenerates to chaotic status after several iterations and returns to the original state on a certain iteration. We call the number of iterations Arnold periodicity. The periodicity is related to the size of the image (N) but is not fully proportional. Considering p=1, q=1, the periodicity varies with the image size is shown in the table below,

Table I. Arnold Periodicity

Size	Periodicity
32*32	24
124*124	15
512*512	378
764*764	265
1024*1024	768

B. Logistic Map

A Logistic Map is a simple nonlinear chaotic discrete system that exhibits chaotic behavior. The Logistic Map is written as,

$$x_{n+1} = rx_n(1 - x_n) \qquad (3)$$

Here, $x(n)$ is the initial state of the LM and its value is between 0 and 1. r is the initial parameters and its value is between 0 and 4. The LM chaotic system exhibits great sensitivity to the initial conditions. We design an external key based on the ACM and LM. As a result, the proposed approach is sensitive to minor changes of the key and against a brute force attack.

The external key is 48 bits long, which corresponds to 6 alphanumeric characters. The system parameter is selected to be a constant ($r > 3.9\ and\ r < 4$), which shows highly chaotic behavior. To get an encrypted initial condition x_0, three alphanumeric characters are chosen and converted into a binary string. The x_0 is determined by Equation (4)

$$x_0 = (l_0 \times 2^0 + l_1 \times 2^1 + \cdots + l_5 \times 2^5 + l_6 \times 2^6 + \ldots + l_{15} \times 2^{15} + l_{16}2^{16} + \cdots + l_{22} \times 2^{22} + l_{23} \times 2^{23})/2^{24} \qquad (4)$$

Here, $l_1, l_2, \ldots, l_{24}$ is the binary information of three alphanumeric characters. Then the image $I(i,j)$ is transferred into 1D matrices p. The key_1 is generated using the LM with the initial value x_0 and r.

$$\begin{gathered} key_1(i) = round(x_i * 255) \\ \forall\ i = 1,2,3,\ldots,262144 \end{gathered} \qquad (5)$$

Two alphanumeric characters are used to determine the value of p and q, which is calculated by Equation. (6)

$$\begin{gathered} p = round(EK_1/10) \\ q = round\ (EK_2/10) \end{gathered} \qquad (6)$$

Here, EK_1 and EK_2 are two external keys. One alphanumeric character is used as a seed of the pseudo-random number generator (PRNG) to generate a key_2 whose length is 262144 (512 × 512). The key is generated by Equation (7).

$$\begin{gathered} key_2 = key_{prng} \\ key = key_1 \oplus key_2 \end{gathered} \qquad (7)$$

Here, $\oplus$ denotes the exclusive OR (XOR) operation. The final key is obtained only from the external key and LM. The pixel value of the plain image is replaced by the key using the Equation (8).

$$p_{encrypted} = p_{plain} \oplus key \qquad (8)$$

C. Proposed Encryption and Decryption Algorithm

The proposed cryptosystem has good confusion and diffusion properties since both ACM and LM are applied in the algorithm. The structure of the encryption scheme is shown in Figure 2. Every frame of the video is encrypted in four steps: 1. The original video frame is scrambled by ACM. 2. The obtained frame is converted into 1D matrices, and the image is decomposed into Red (R), Green (G), and Blue (B) color channels. 3. The substitution process is to change the pixel value by using PRNG and LM. Then the 1D matrices and RGB channels are combined back to the original image size. The obtained encrypted video frame is not only unreadable but also has excellent confusion and diffusion properties. The six alphanumeric characters are used as the external key to determine the initial conditions of ACM and LM and make the encryption even secure.

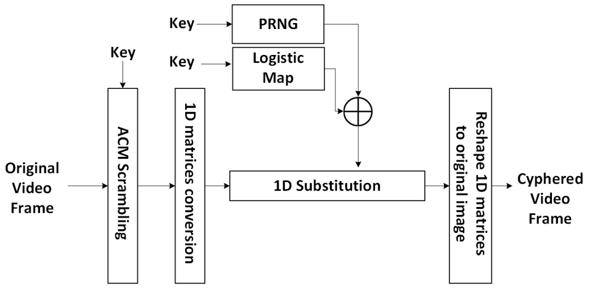

Figure 2. Illustration of Proposed Encryption Algorithm

In the decryption, only the correct key can completely recover the original video frame. Even a tiny change in the external key can lead to the failure of the decryption process. We follow the inverse steps of the encryption process shown in Figure 3 and the original video frame can be fully reconstructed.

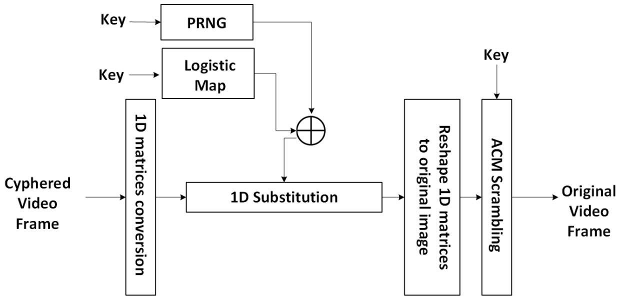

Figure 3. Illustration of the Proposed Decryption Algorithm

III. Experimental Tests Results and Analysis

This section examines the effectiveness and feasibility of the proposed method by using a sample image (size: 512x512) as the plain image. The statistical and correlation analysis are presented.

In Figure 4, we have shown the plain image as well as the three encrypted images and decrypted images. The proposed algorithm is lossless, and the recovered image is the same as the plain image. The initial conditions of ACM and LM are determined by the six-bit external key. The encrypted results show that the original image is randomly encrypted into different noise-like images, and it is not readable by the sense of sight using a Chaotic map.

Statistical analysis is done by calculating the histogram, which illustrates the pixel distribution at each color density level. The histogram of original image is shown in Figure 5 (a), and the histogram of encrypted images using ACM, LM, and proposed encryption scheme, including the RGB (red, green, blue) channels, are shown in Figure 5 (b), (c), (d). ACM transforms the position of pixels and does not change their value. Therefore, the histogram of the image after ACM is the same as the original image, which has the same statistical information. The image after LM and the proposed encryption scheme offer a uniform distribution and are different from the original image. This outcome prevents the leakage of any statistical information of the plain image and resilient to the statistical attack.

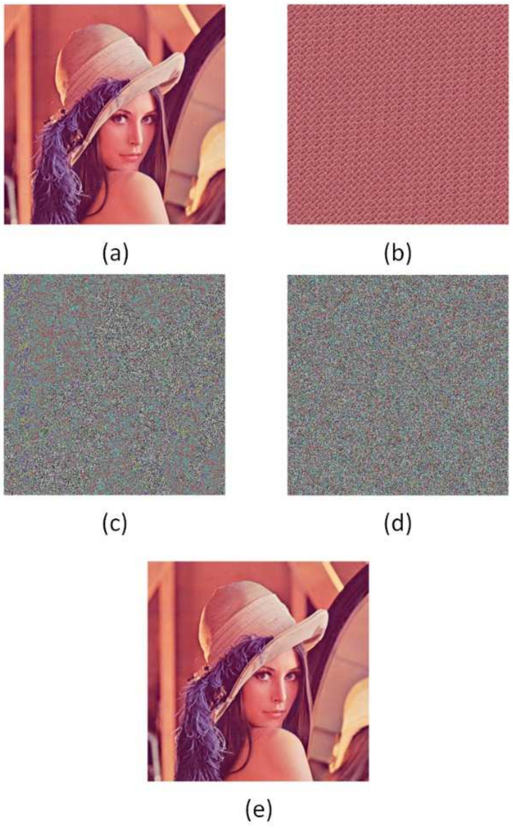

Figure 4. Encrypted Results; (a) Plain Image, (b) Image after ACM, (c) Image after LM. (d) Image after the Proposed Encryption Scheme, (e) Encrypted Image.

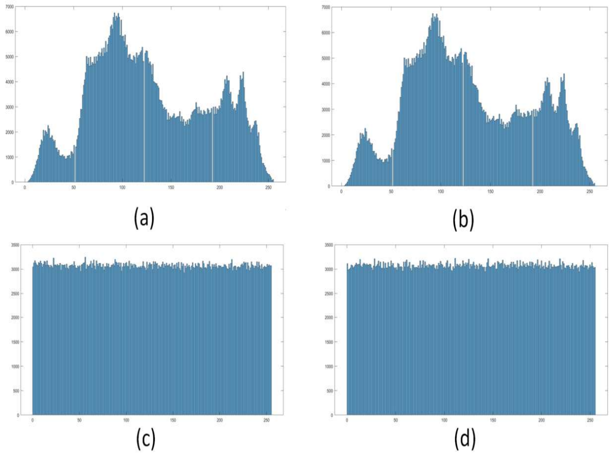

Figure 5. Histogram Analysis; (a) Plain Image, (b) Image after ACM, (c) Image after LM, (d) Image after the Proposed Encryption Scheme.

The correlation of two horizontally adjacent pixels in a regular image should be highly correlated. Figure 6 displays the scatter plot of the plain image, image after ACM, image after

LM, and image after proposed encryption scheme in red, green, and blue channels. The scatter plot reveals the correlation of two adjacent pixels in the horizontal distribution. The RGB channels of the plain image have a strong correlation between adjacent pixels, which show up as a clear linear pattern in Figure 6 (a), (b), and (c). The ACM display with a less observable pattern in Figure 6 (d), (e) and (f), and LM and proposed encryption scheme display a more random pattern which is shown in Figure 6 (g), (h), and (i) and Figure 6 (j), (k), and (l). In addition, LM and the proposed encryption scheme demonstrate a similar random pattern for all R, G, B channels.

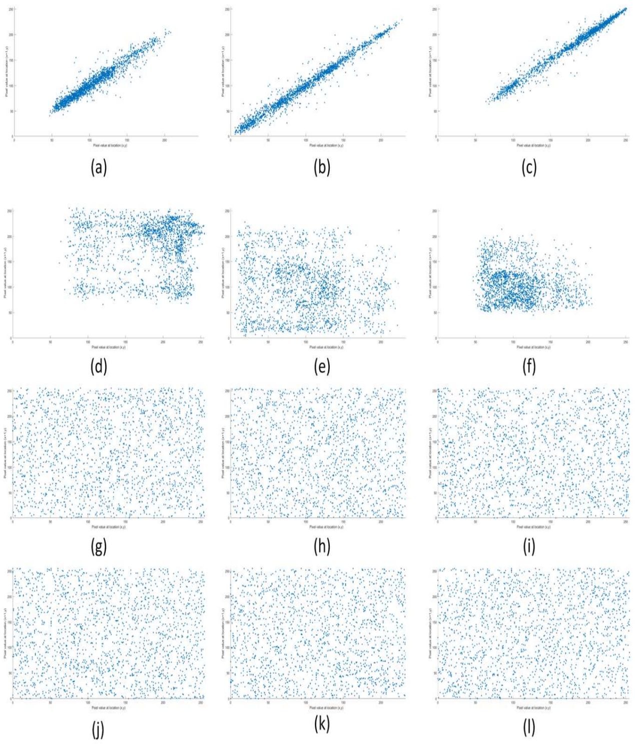

Figure 6. Correlation of Two Horizontally Adjacent Pixels; (a), (b), (c) respectively show the correlation of red, green, and blue channels of the plain image. (d), (e), (f) respectively show the correlation of red, green, and blue channels of the image after ACM. (g), (h), (i) respectively show the correlation of red, green, and blue channels of the image after LM. (j), (k), (l) respectively show the correlation of red, green, and blue channels of the image after the proposed encryption scheme.

Since the correlation scatter plot of the LM method and proposed encryption scheme is similar, we utilize the correlation coefficient $r_{x,y}$ to test the pixel correlation of four images. To measure the correlation coefficient, 15000 adjacent pixel pairs of a plain image, image after ACM, image after LM, and image after proposed encryption scheme are randomly selected. The correlation is calculated using the Equation (9),

$$r_{x,y} = \frac{\sum_i (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_i (x_i - \bar{x})^2 \sum_i (y_i - \bar{y})^2}} \tag{9}$$

Here, $y(i)$ is the horizontal adjacent pixel value of $x(i)$ and $\bar{x} = \frac{1}{15000}\sum_i x(i)$, $\bar{y} = \frac{1}{15000}\sum_i y(i)$. The correlation coefficient results of the four images are shown in Table II.

The measured correlation value of the plain image is close to 1 which indicates the high correlation between pixels. The chaotic-based encryption algorithm can reduce the correlation of images into little or none. Therefore, a good encryption algorithm should have a correlation coefficient close to zero. From Table II, we can see that the correlation coefficient can be greatly reduced by the proposed encryption scheme.

TABLE II. CORRELATION COEFFICIENT RESULTS

Input Image	Coefficient value
Plain image	0.9901
Image after ACM	0.0369
Image after LM	0.0127
Image after proposed encryption scheme	7.7e-4

IV. CONCLUSION

In this paper, we proposed a chaotic-based encryption/decryption scheme for ultrasonic video transmission systems. The proposed cryptosystem has good confusion and diffusion properties since both ACM and LM are applied in the algorithm. The algorithm is proved to be efficient and suitable for ultrasonic video communication. The encryption algorithm, including a 6-bit external key, maintains good encryption quality and is robust to the statistical attack and brute force attack. The experimental results show that the algorithm greatly reduces the correlation between pixels and offers a histogram with uniform distribution. The lossless decryption algorithm guarantees the video can be fully recovered on the remote client-side.

V. ACKNOWLEDGMENT

This material is based upon work supported under an Integrated University Program Graduate Fellowship. Any opinions, findings, conclusions, or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the Department of Energy Office of Nuclear Energy.

REFERENCES

[1] X. Huang, J. Saniie, S. Bakhtiari and A. Heifetz, "Applying EMAT for Ultrasonic Communication through Steel Plates and Pipes," in *IEEE International Conference on Electro/Information Technology*, Rochester, Michigan, USA, 2018.

[2] X. Huang, J. Saniie, S. Bakhtiari and A. Heifetz, "Ultrasonic Communication System Design Using Electromagnetic Acoustic Transducer," in *IEEE International Ultrasonics Symposium (IUS) proceedings*, Kobe, Japan, 2018.

[3] X. Huang, J. Saniie, S. Bakhtiari and A. Heifetz, "Time Reversal Signal Processing for Ultrasonic Communication through Metal Channels," in *IEEE International Ultrasonics Symposium (IUS) proceedings*, Glasgow, UK, 2019.

[4] A. Heifetz, X. Huang, D. Shribak, J. Saniie, S. Bakhtiari and R. Vilim, "Communication in a Nuclear Facility with Elastic Waves Excited with Ultrasonic LiNbO3 Transducers on Pipes," *Transactions of the American Nuclear Society,* vol. 121, pp. 508-510, 2020.

[5] A. Heifetz, D. Shribak, X. Huang, B. Wang, J. Saniie, J. Young and S. B. a. R. B. Vilim, "Transmission of Images with Ultrasonic Elastic Shear Waves on A Metallic Pipe using Amplitude," *IEEE Transactions on Ultrasonics, Ferroelectrics, and Frequency Control,* vol. 67, pp. 1192-1200, 2020.

[6] X. Huang, J. Saniie, S. Bakhtiari and A. Heifetz, "Performance Evaluation of High-Temperature Ultrasonic Communication System," in *2020 IEEE International Ultrasonics Symposium (IUS) proceedings*, Las Vagas, USA, 2020.

[7] X. Huang, J. Saniie, S. Bakhtiari and A. Heifetz, "Software-Defined Ultrasonic Communication System Based on Time-reversal Signal Processing," in *2020 IEEE International Ultrasonics Symposium (IUS) proceedings*, Las Vegas, USA, 2020.

[8] X. Huang, J. Saniie, S. Bakhtiari and A. Heifetz, "Contoured PPM-EMAT Design for Ultrasonic Communication On Metalic Pipe Channels," in *IEEE International Conference on Electro/Information Technology*, Naperville, IL, USA, 2020.

[9] M. W. Hirsch, S. Smale and R. L. Devaney, Differential Equations, Dynamical Systems & An Introduction to Chaos, Elsevier Academic Press, 2003.

[10] E. Ott, Chaos in Dynamical Systems, CAMBRIDGE university press, 1993.

[11] S. Behnia, A. Akhshani, S. Ahadpour, H. Mahmodi and A. Akhavan, "A fast chaotic encryption scheme based on piecewise nonlinear chaotic maps," *Physics Letters A,* p. 391–396, 2007.

[12] Y. Zhou, L. Bao and C. Philip, "A New 1D Chaotic System for Image Encryption," *Signal Processing,* p. 172–182, 2014.

[13] X. Wang, N. Guan, H. Zhao, S. Wang and Y. Zhang, "A new image encryption scheme based on coupling map lattices with mixed multi-chaos," *Scientific Reports,* vol. 10, pp. 2045-2322, 2020.

[14] S. Koppu and V. M. Viswanatham, "A Fast Enhanced Secure Image Chaotic Cryptosystem Based on Hybrid Chaotic Magic Transform," *Modelling and Simulation in Engineering,* pp. 1687-5591, 2017.

[15] S. Som and A. Kotal, "Confusion and Diffusion of Grayscale Images Using Multiple Chaotic Maps," in *National Conference on Computing and Communication Systems*, 2012.

[16] K. J. Aval, M. S. Kamarposhty and M. Damrudi, "A Simple Method for Image Encryption Using Chaotic Logistic Map," *Journal of Computer Science & Computational Mathematics,* vol. 3, no. 3, 2013.