A Novel Encryption/Decryption Framework for Ultrasonic 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 proven to be reliable for transmitting data, images, and video streams through solid channels to overcome certain physical barriers which prevent conventional wired or wireless communication networks. In this study, we propose a novel encryption framework for securing the video stream transmission while taking into consideration the characteristics and constraints associated with ultrasonic communication through solid channels. In this framework, a Chaotic encryption algorithm employing the 2-D Around Cat Map and 1-D Logistic Map is used to confuse and diffuse the video stream. A benchmark system was designed to examine the performance of the Chaotic encryption algorithm applied to ultrasonic video transmission. The horizontally adjacent pixels in a video frame and the same pixel in two consecutive frames are randomly selected to evaluate the frame-to-frame pixel correlation before and after encryption. The scatter plots and the correlation coefficient reveal that the Chaotic encryption fully scrambles and diffuses the original video stream.**

Keywords—Ultrasonic communication, Video transmission cryptosystem, Chaotic encryption

I. Introduction

Ultrasonic waves can be used as information carriers through solid channels for delivering data, images, and video streams [1-3]. Due to the attenuation, dispersion, or multipath effect of ultrasonic communication through the solid channel [4][5], the channel length is limited to a few meters. Consequently, for remote access to video data beyond a few meters the output of the ultrasonic channel must be interfaced to Ethernet or Wi-Fi. The transmission of video data through Ethernet or Wi-Fi demands cybersecurity protection. In this study, A benchmark system was designed to examine the performance of the encryption/decryption applied to ultrasonic communication through a steel pipe channel. A Chaotic encryption/decryption key updating algorithm is presented and tested for a video stream. 2-D Arnold Cat Map and 1-D Logistic Map are used to confuse and diffuse the video stream from the webcam [6-7]. This encryption technique adds no redundancy to the original video stream and is efficient and suitable for ultrasonic video communication. We assess the effectiveness and feasibility of encrypted images by comparing them to the original image using the correlation scatter plot between adjacent pixels and the same pixels in two consecutive frames [8-9].

This paper is organized as follows. Section II presents the ultrasonic video transmission system using a metal pipe channel. Section III presents the Chaotic cryptosystem including the structure and key updating algorithm for ultrasonic video transmission. Section IV presents the experimental data to validate the practicality of the proposed system. In this section, the performance of a Chaotic cryptosystem is analyzed and compared. Section V presents a summary of key issues related to video transmission, ultrasonic solid channel, and the efficiency of the Chaotic encryption algorithm.

II. Ultrasonic Video Transmission System

Fig. 1 is an example of applying an ultrasonic video transmission system in nuclear facilities where wired or wireless communication links are not feasible. The transmitter is placed in a sealed environment and is fully protected by the physical barrier for isolation and safety purposes. The video stream from the webcam surveillance in the sealed environment is modulated by the transmitter controller. The packetized video streams are transmitted through the steel pipe channel (see Fig. 2) using a 2.5 MHz piezoelectric transducer (PZT). The transmitted information is captured by the 2.5 MHz PZT receiver which is placed outside of the physical barrier (see Fig. 1). The receiver controller demodulates and recovers the video information. An Ethernet connection delivers the video stream to the remote client by a server. This condition demands securing video data. The next section presents a Chaotic cryptosystem to secure ultrasonic video transmission.

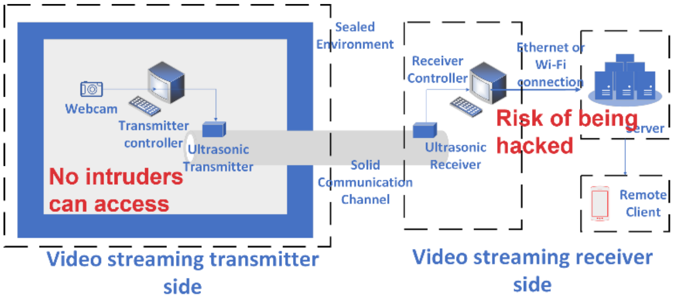

Fig. 1. Ultrasonic video transmission system architecture

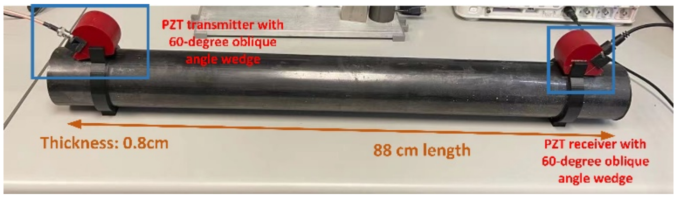
PZT transmitter with 60-degree oblique angle wedge
Thickness: 0.8cm
88 cm length
PZT receiver with 60-degree oblique angle wedge

Fig. 2. Steel pipe channel for ultrasonic video transmission

III. Chaotic Cryptosystem

Chaotic maps are studied in dynamic systems as they exhibit chaotic behavior [8]. Chaotic encryption for the video stream is robust, secure, and efficient for real-time implementation on the transmitter side of the ultrasonic video transmission [9]. Fig. 3 displays the Chaotic cryptosystem key updating algorithm for ultrasonic video transmission. The Arnold Cat Map (ACM) changes the positions of the pixels. It decreases the correlation of adjacent pixels and makes the video frame unreadable to eavesdroppers. Then the Logistic Map (LM) is used to substitute the value of each pixel. This process enhances randomness and breaks the statistical characteristics of the original video frame. An external key determines the initial conditions of ACM and LM.

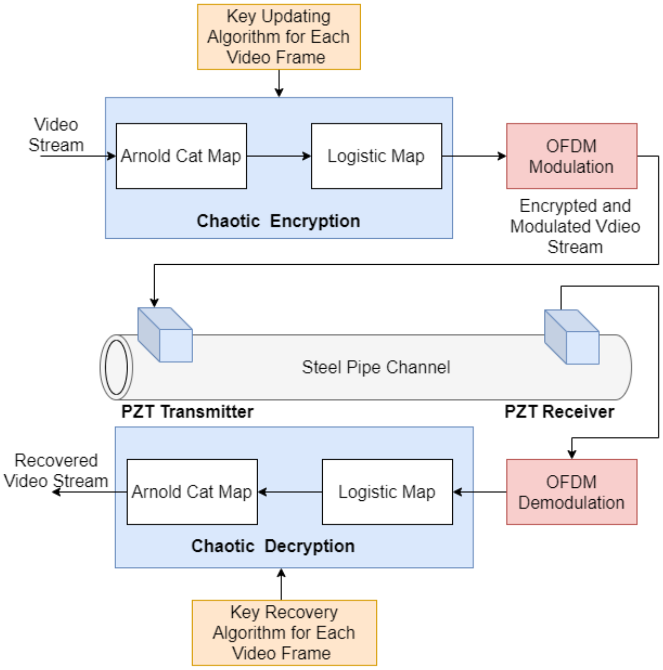

Fig. 3. Chaotic cryptosystem structure for ultrasonic video transmission

In video transmission, each frame is encrypted using Chaotic maps in three steps: **1.** The original video frame is scrambled by ACM, **2.** The obtained data is converted into a 1D sequence and substituted the pixel values by the LM, and **3.** Reshape the encrypted sequence back to the original image size. The encryption process adds no redundancy to the video stream and doesn't affect the encoding and modulation processes of the transmission procedures. However, we might have an artifact problem when running the Chaotic encryption process using the same key for consecutive frames. A key updating algorithm is designed to break the strong correlation of successive frames. The encryption/decryption algorithm is shown in Fig. 4. The original key_0 is used to encrypt video frame 0, then the new key is derived from the encrypted data after each encryption round and used for the encryption process for successive frames. The new key value is determined by key_0 and ciphered video frame. During the decryption process, the new key is derived before each decryption round. Even a tiny change in the key_0 can lead to the failure of the decryption process.

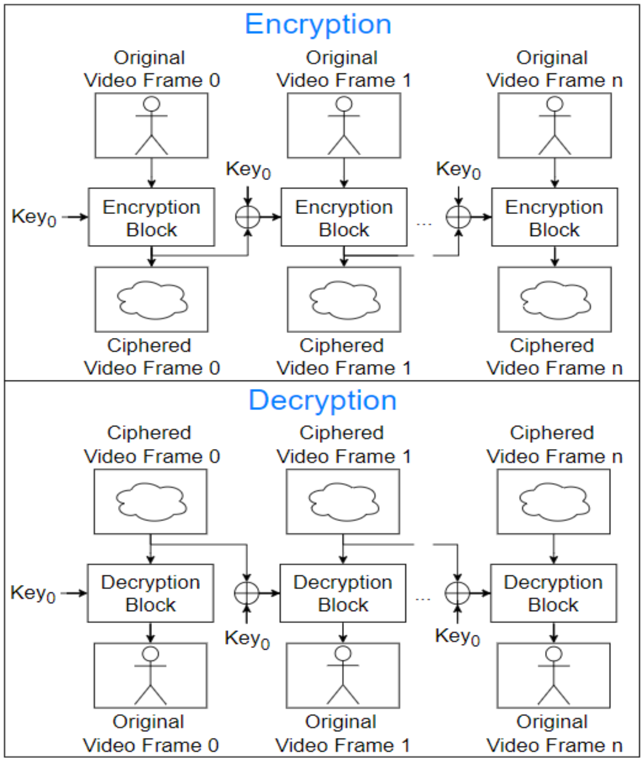

Fig. 4. Encryption/decryption key updating algorithm for ultrasonic video transmission

IV. Video Transmission Test Results

This section examines the feasibility and efficiency of the proposed Chaotic cryptosystem by using successive frames of a sample video stream. In Fig. 5, two consecutive video frames are selected as an example. They are almost identical by the sense of sight. Figs. 5c and 5d exhibit the ciphered video frames. The original video frames are encrypted into different noise-like images. No specific similar pattern can be observed. In the remote client, the decryption algorithm can fully recover the video stream lossless, as shown in Figs. 5e and 5f.

The horizontally adjacent pixels in a video frame and the same pixel in two consecutive frames are randomly selected to evaluate the frame-to-frame pixel correlation before and after encryption. The scatter plots are shown in Fig. 6. Figs. 6a and 6b reveal a high correlation of adjacent pixels. Particularly, pixels in the consecutive video frames display an even stronger correlation. Figs. 6c and 6d demonstrate the correlation of using the proposed novel encryption/decryption framework. As shown in Fig. 6 the encryption algorithm strongly decorrelates frame to frame pixel correlation and the scatter plots display random patterns. The correlation coefficient of encrypted video frames is 0.0065, which implies the Chaotic encryption fully scrambles and diffuses the original video stream.

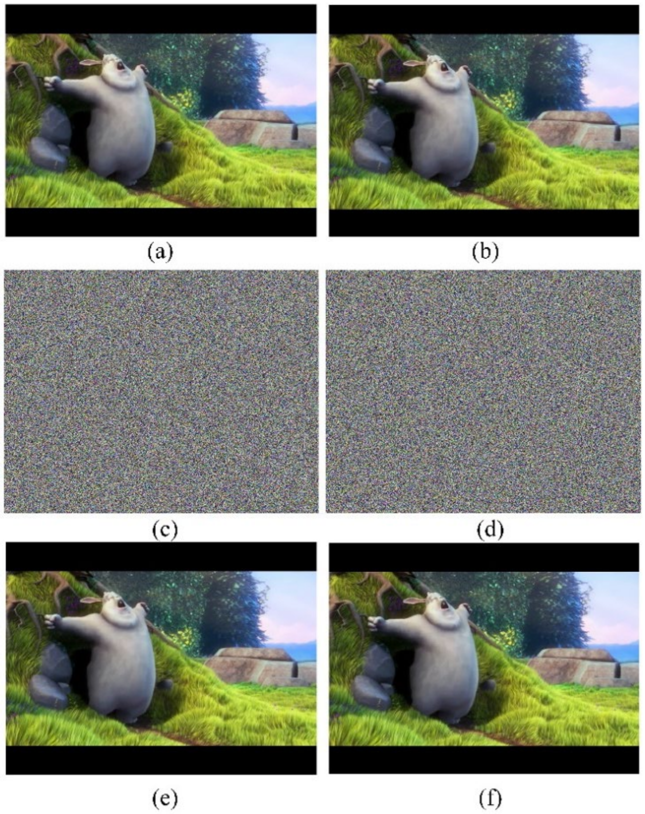

Fig. 5. Experimental test results: (a) original video frame 1, (b) original video frame 2, (c) video frame 1 after encryption, (d) video frame 2 after encryption, (e) recovered video frame 1, and (f) recovered video frame 2.

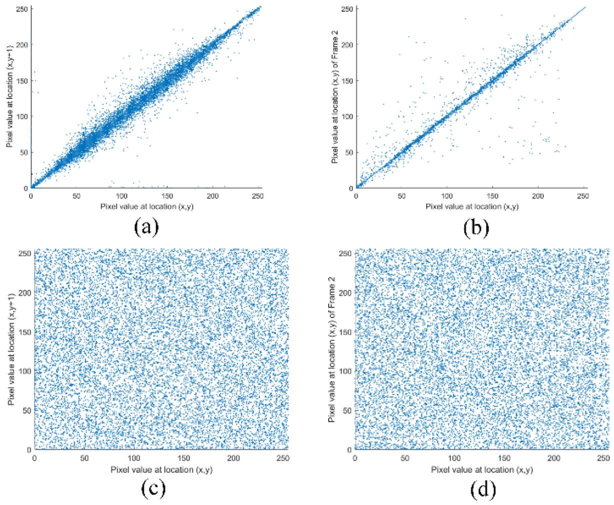

Fig. 6. Correlation results: (a) horizontally adjacent pixels in original video frame 1, (b) pixels in the original consecutive video frames, (c) adjacent pixels in encrypted video frame 1, and (d) pixels in the encrypted consecutive video frames.

V. Conclusion

In this paper, we proposed a novel encryption/decryption frame for the ultrasonic secure video transmission system. The proposed cryptosystem (ACM and LM algorithms) shows robust confusion and diffusion properties. The encryption/decryption algorithm updates the key to initialize the Chaotic maps, which maintains strong encryption quality and is resilient to a cybersecurity attack. By using the Chaotic cryptosystem, the correlation coefficient of the encrypted frame is 0.0065, a very small number practically zero. Furthermore, the correlation scatter plots also confirm the robustness of the algorithms. The Chaotic cryptosystem is a lossless decryption process that ensures the video can be fully recovered on the remote client site.

References

[1] X. Huang, J. Saniie, S. Bakhtiari and A. Heifetz, "Applying EMAT for Ultrasonic Communication Through Steel Plates and Pipes," 2018 IEEE International Conference on Electro/Information Technology (EIT), 2018, pp. 0379-0383, doi: 10.1109/EIT.2018.8500148.

[2] X. Huang, J. Saniie, S. Bakhtiari and A. Heifetz, "Ultrasonic Communication System Design Using Electromagnetic Acoustic Transducer," 2018 IEEE International Ultrasonics Symposium (IUS), 2018, pp. 1-4, doi: 10.1109/ULTSYM.2018.8580149.

[3] A. Heifetz, D. Shribak, X. Huang, B. Wang, J. Saniie, R. Ponciroli, E. R. Koehl, S. Bakhtiari & R. B. Vilim (2021) Transmission of Images on High-Temperature Nuclear-Grade Metallic Pipe with Ultrasonic Elastic Waves, *Nuclear Technology*, 207:4, 604-616, DOI: 10.1080/00295450.2020.1782626.

[4] X. Huang, J. Saniie, S. Bakhtiari and A. Heifetz, "Time Reversal Signal Processing for Ultrasonic Communication through Metal Channels," *2019 IEEE International Ultrasonics Symposium (IUS),* 2019, pp. 623-626, doi: 10.1109/ULTSYM.2019.8926138.

[5] 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.

[6] X. Huang, D. Arnold, T. Fang and J. Saniie, "A Chaotic-based Encryption/Decryption System for Secure Video Transmission," 2021 IEEE International Conference on Electro Information Technology (EIT), 2021, pp. 369-373, doi: 10.1109/EIT51626.2021.9491868.

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

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

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