Journal of Network Intelligence ©2018 ISSN 2414-8105 (Online)
Taiwan Ubiquitous Information Volume **3**, Number **1**, February **2018**

ARM-embedded Implementation of H.264 Selective Encryption Based on Chaotic Stream Cipher

Chunlei Fan, Qun Ding

Electronic Engineering College of Heilongjiang University
Harbin, China
Qunding@aliyun.com

Received November 2017; revised January 2018

Abstract. *Nowadays, embedded webcams have been widely used in the security fields. However, when these webcams are used, the transmission of H.264 video stream couldn't be guaranteed with a higher security. To address this issue, this paper designed an H.264 selective encryption based on chaotic stream cipher. Besides, aiming at machine with finite precision would make digital chaotic binary sequences into similar short period sequences so that it lowers the security of video stream for the problem. An novel chaotic stream cipher is proposed with the purpose of enhancing data securitywhich combines Logistic chaotic sequences with Arnold transformation to improve period of sequences. Consequences, ARM-based hardware device with S3C6410 processor is adopted to realize the H.264 remote secure communication with chaotic stream cipher. Results of related experiments indicate that the new algorithm of Logistic chaotic sequences has a good performance on safety.*

Keywords: H.264; Arnold; video security; chaotic mapping

1. **Introduction.** Nowadays, with the rapid development of science and network technology, embedded webcams have been widely used in the security fields. Consequence, there are some unassured factors that multimedia information may be eavesdropped and tampered in public Internet network. Nevertheless, the encryption of H.264 video stream is an effective strategy to guarantee video data security. It is not realistic to use traditional cryptogram standards to encrypt complete video streams. Because complex algorithm and big data operation can greatly reduce video code rate and quality. Therefore, some researchers propose the selective encryption scheme with the purpose of low-complexity operation and no changing video codec structure Besides, chaotic theory has good pseudo randomness, initial value sensitivity and resembles noise features so that chaotic systems were widely used in secret communication and cryptography field [1, 2].

At present, researchers have carried out a number of investigations and have already gained some achievements in this respect. References [3, 4] proposes a nonlinear nominal matrix-based discrete time chaotic system to encrypt completely compressed video data with chaos after H.264 encoding. Reference [5] analyzes a fuzzy-model-based chaotic synchronization for video secure communication with H.264 software encoding. Reference [6–11] researches a selective encryption scheme for protecting H.264 video. In the scheme, the part of syntax elements are encrypted for data security, including the sign of trailing, the sign of motion vector difference and intra-macroblock non-zero DCT coefficients. However, these research achievements use software H.264 codec or encrypt completely compressed video data, which leads to slower operation speed.

Considering the above situation and problems, this paper puts forward ARM-embedded implementation of H.264 selective encryption based on chaotic stream cipher to overcome the shortcomings. In the scheme, I-frame of compressed video data are encrypted based on a novel chaos stream cipher. In addition, a mobile client is implemented to access the remote video stream based on RTMP protocol and SRS server. Further, through the security analysis and performance simulation test, the algorithm obtained good encryption speed and security. The flow encryption algorithm does not cause the data to expand, which has a certain reference value in video encryption field.

2. Topology Structure of Video Transmission.

The design concept of H.264 encryption embedded system uses S3C6410 as the core processor of system. It connects with 1G Nand Flash and 256M SDRAM so that Linux embedded operating system can run normally. The S3C6410 processor is responsible for H.264 hardware encoding and video data encryption processing. Both USB camera interface and DM9000 Ethernet interface are significant in the bottom board. On the one hand, a UVC camera connects to the USB camera interface and provides YUV raw video data. On the other hand, the router connects to the DM9000 Ethernet interface for RTMP communication. The physical map of hardware circuit is shown in figure 1.

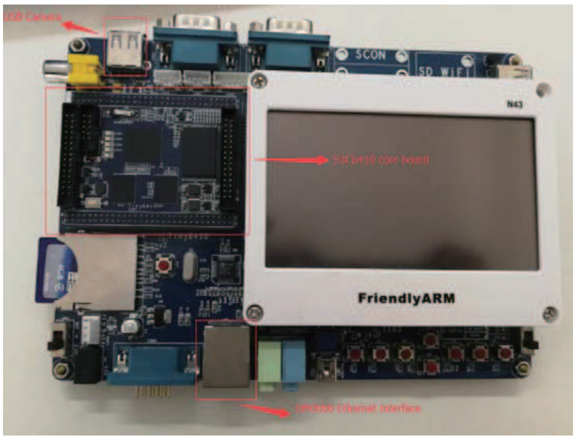


Figure 1. Hardware board with S3C6410 processor

Further, the flow diagram of video transmission is shown in figure 2. A UVC camera is responsible to provide the YUV raw video data. V4L2 is a collection of device drivers and an API for supporting realtime video capture on Linux systems. It supports many USB webcams, TV tuners, and related devices, standardizing their output, so programmers can easily add video support to their applications. In the paper, V4L2 captures real-time video data with the purpose of encoding video stream by H.264 hardware codec. Next, I-frame will be encrypted based on a novel chaos stream cipher after S3C6410 codec generates compressed video stream. RTMP is a TCP-based protocol which maintains persistent connections and allows low-latency communication. To deliver streams smoothly and transmit as much information as possible, it splits streams into fragments, and their size is negotiated dynamically between the client and server. In the scheme, RTMP is used to package the encrypted video stream by DM9000 Ethernet interface. The SRS server is responsible for forwarding the video stream to the client. The client designed an Android application program with chaotic decryption algorithm with the purpose of displaying YUV raw video data.

3. Design of a Novel Chaotic Stream Cipher.

3.1. Logistic chaotic mapping and quantification.

Logistic chaotic mapping is a classical model of non-linear dynamics system, and its simple equations as well as good performance are widely for chaotic secure communication system. The mapping is defined as:

$$x_{n+1} = \mu x_n \left(1 - x_n\right), \mu \in (0, 4], x_n \in (0, 1) \tag{1}$$

x_n is initial value of the Logistic iterative equation. Among μ is called as branch parameter, when the value area of μ is [3.5699456, 4], logistic mapping work on chaotic state and show a complex dynamic characteristics [12,13]. Substituting initial value x_1 into the chaotic equation, the chaotic binary sequences were generated based on repeated iterative operation. These sequences are periodic sequences, which possess sensitive dependence on initial value and strange attractor. These features correspond with character of cryptographic key. Therefore, chaotic mapping is widely used in the secure communication system.

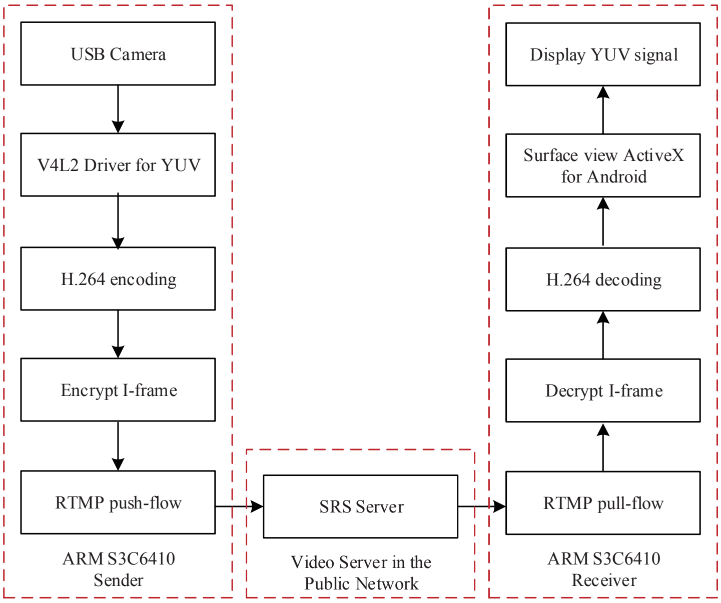


FIGURE 2. The flow diagram of video transmission

The original chaotic sequences $\{x_n\}$ are quantified into binary sequences $\{s_n\}$ as key sequences. It has a variety of ways to quantize chaotic sequences, this paper chooses relatively simple quantitative method to avoid complex computations. It's defined as follows:

$$x_n = \begin{cases} 0, s_n < c \\ 1, s_n \geq c \end{cases} \tag{2}$$

Where $c = 0.5$. When logistic mapping show chaotic state, iterative computation value x_n will traverse on (0, 1) interval. Therefore, it can get good chaotic binary sequences by the quantitative method.

3.2. **Arnold mapping and improved algorithm of chaotic sequences.** Classical Arnold transform is a two-dimensional reversible mapping. The definition can be expressed as

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = A \begin{bmatrix} x \\ y \end{bmatrix} (\text{mod} 1), A = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \tag{3}$$

The domain of definition $x/y \in [0, 1]$, $x'/y' \in [0, 1]$ is real number. An improved algorithm of chaotic sequence based on logistic mapping and Arnold transform is proposed in this paper, the algorithm block diagram as shown in figure 3.

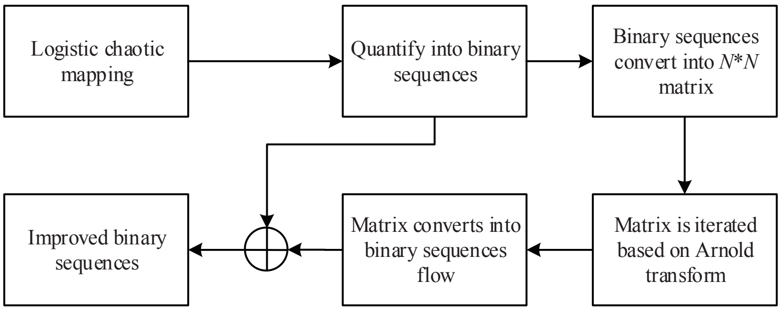

Logistic chaotic mapping
Quantify into binary sequences
Binary sequences convert into N*N matrix
Improved binary sequences
Matrix converts into binary sequences flow
Matrix is iterated based on Arnold transform

FIGURE 3. Block diagram of improved algorithm

Firstly, as can be seen clearly from the block diagram that 0/1 sequences flow are built into N order matrix. Secondly, this matrix is iterated based on Arnold transform. Due to the matrix of order N, namely the domain of definition $x/y \in [0, N-1]$, $x'/y' \in [0, N-1]$ is integer value [14–16]. In this paper, the formula (3) can be converted into formula (4) with the purpose of convenient operation. Finally, according to the row order, iterative matrix element convert into a binary sequences flow. It has a simple xor operation with original chaotic binary sequences to generate the final improved sequences.

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = A \begin{bmatrix} x \\ y \end{bmatrix} (\bmod N)\, , A = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \tag{4}$$

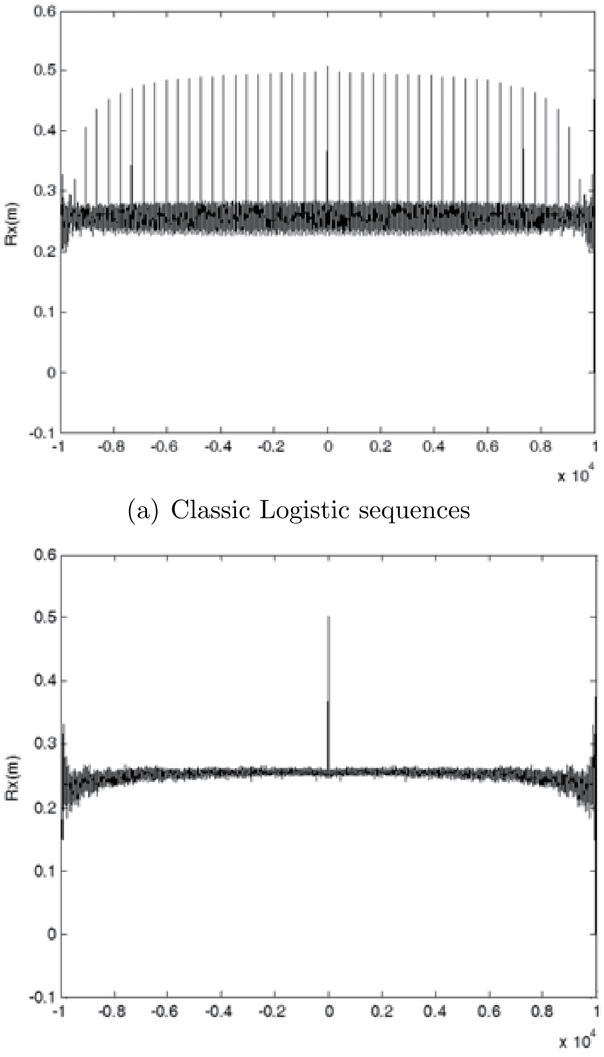
In contrast with the traditional algorithm, the improved algorithm easy to implement, and it will reduce the resource consumption of hardware circuit. Besides, there are problems that the short period of chaotic sequences in the restricted computer precision will be effectively solved.

3.3. **Security and Performance Analysis.**

Autocorrelation Test. Autocorrelation is an important property of pseudo random binary sequences, and the perfect pseudo random sequences are δ function. Suppose $x(n)$ is a chaotic binary sequences, $R_x(m)$ is the autocorrelation function of the sequences, the definition of autocorrelation function as following:

$$R_x(m) = \sum_{n=-\infty}^{\infty} x(n) x(n+m) \tag{5}$$

In this experiment, the sequences length are 10^6, the Matlab simulation diagram is shown in Figure 4. It can be seen from the diagram that the sequences in the case of the calculation accuracy of float type is close to the δ function, which shows good pseudo random property.



(a) Classic Logistic sequences

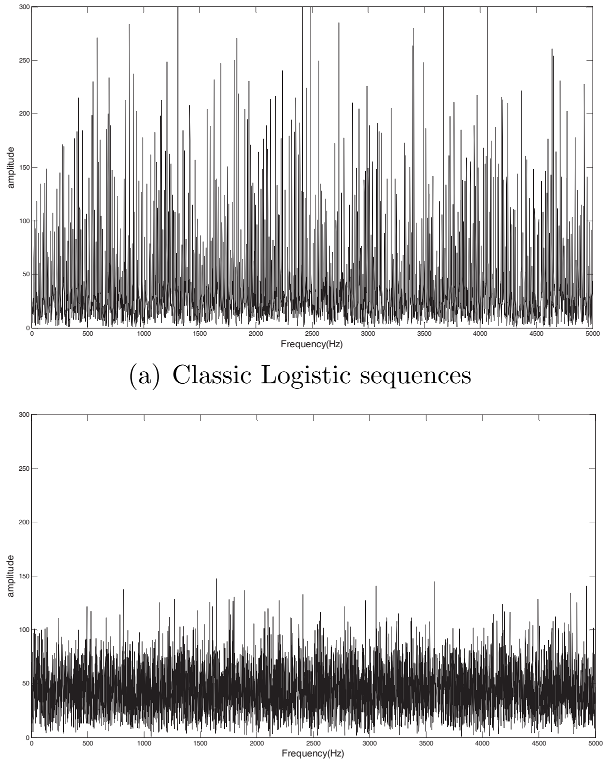
(b) Improved Logistic sequences

FIGURE 4. Simulation diagram of autocorrelation test

Sequence Spectrum Analysis. Due to the time domain waveform of chaotic sequence signal is more complex and difficult. Therefore, this paper analyzes the spectrum of chaotic sequences by Fourier transform processing. Suppose $x\,(n)$ is chaotic binary sequence. $F\,(k)$ is spectrum value. The discrete Fourier transform formula of this signal can be described as follows:

$$F\,(k) = \sum_{n=0}^{N-1} x\,(n) e^{\frac{-2j\pi nk}{N}}, k = 0, 1, \ldots, N-1 \tag{6}$$

By using this formula, Matlab simulation program can be used to test the pseudo-random sequences that generated by two algorithms respectively. Its spectrum of simulation diagram as shown in figure 5.



(a) Classic Logistic sequences

(b) Improved Logistic sequences

Figure 5. Spectrum simulation diagram of chaotic sequences

It can be seen from two simulation diagrams that the spectrum of the classical Logistic sequence has multiple peaks and shows the quasi-periodicity of the signal. The chaotic sequence generated by the new algorithm is more similar to the spectrum of Gaussian white noise, which shows that the better randomness can satisfy the requirement of network data encryption.

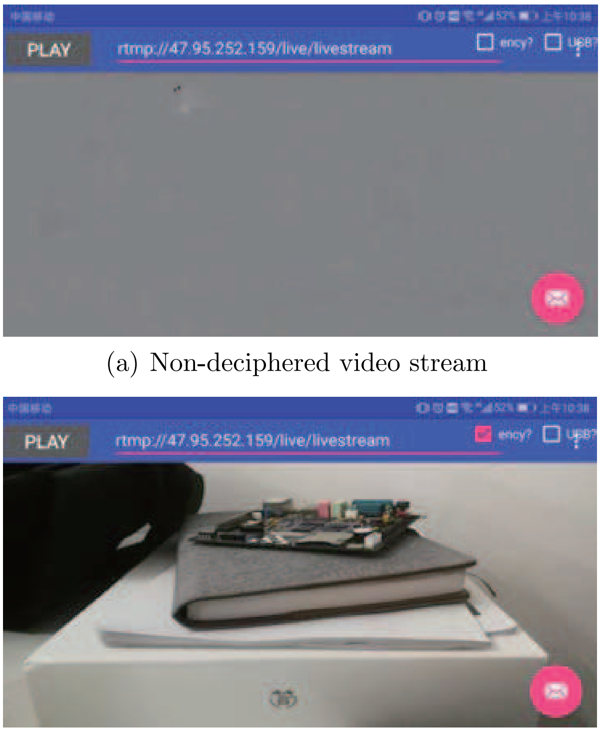
NIST Suite test. The NIST test suite is designed to test the sequence performance of the random number generator [17]. By comparing the performance of these two sequences with test results, the test results are shown in table 1. It can be seen that there are six unapproved items to classical Logistic sequences from table 1 while improved chaotic sequence has higher pass rate and shows better randomness.

4. **Overall Test of Video Encryption System.** Firstly, the cross development environment needs to be established for embedded application compilation. Application program is designed by C++ programming language with LibRtmp and Ffmpeg library. Ubuntu12.04 Linux operating system and cross-compilation tool chain of cross-3.4.2-eabi are used to compile video encryption program. Next, V4L2 driver and DM9000 network driver are compiled into Linux Kernel by relative Linux command. Finally, Linux operating system is burned into target ARM board with the purpose of executing encryption application program. The RTMP video sender command is used for video pull-flow. Besides, SRS server needs to be set up to forward video data in the public network. Client can access SRS server for video stream after these steps are finished. Decryption and non-decryption client programs are executed respectively for comparing shows. The experiment result is shown in figure 6. It can be seen from the

Table 1. NIST suite test results

Test items	Classical chaotic sequences	Improved chaotic sequences
Frequency	T	T
Block Frequency	T	T
Runs	T	T
Long Runs	F	T
Rank	T	T
Discrete Fourier Transform	T	T
Overlapping Template	F	T
Approximate Entropy	F	T
Cumulative Sums	T	T
Linear Complexity	T	T
Serial	F	T
Universal	T	T
Non-Overlapping Template	T	T
Random Excursions	F	F
Random Excursions Variant	F	F

figure that the undecipherable video stream shows the phenomenon of gray screen. This experiment is carried out in the real Internet environment. Therefore, the video stream is interferenced by some noise during transmission. From the results, the noise interference is not obvious. Besides, owing to the fact that stream cipher has a faster encryption speed. The main frequency of ARM processor is 667MHz. According to the experimental results, I-frame encryption time increased by 0.03 percent.



rtmp://47.95.252.159/live/livestream

(a) Non-deciphered video stream

rtmp://47.95.252.159/live/livestream

(b) Deciphered video stream

Figure 6. Video display of smartphone side in the real network environment

5. **Conclusion.** In recent years, the security of multimedia video cameras has been widely concerned in society. Aiming at the problems, this paper designs a H.264 video stream encryption system based on the improved chaotic stream cipher and embedded technology. Chaotic stream cipher combines Logistic chaotic sequences with Arnold transformation. Further some comparative experiments are done about

autocorrelation and randomness of new binary sequences, including NIST suite test, autocorrelation test and sequence spectrum analysis. The results indicate that the new algorithm of Logistic chaotic sequences has a good performance on safety.

Acknowledgments. This work is partially supported by Natural Science Foundation of China (No. 61471158).

REFERENCES

[1] H. B. Rogelio, R. R. Roxana, Cycle Detection for Secure Chaos-based Encryption, *Communications in Nonlinear Science and Numerical Simulation*, vol.16, no.8, pp. 3203-3211, 2011.

[2] D. Arroyo, F. Hernandez, Cryptanalysis of a Classical Chaos-Based Cryptosystem with Some Quantum Cryptography Features, *International Journal of Bifurcation* & *Chaos*, vol.27, no.1, pp. 1750004∼1-12, 2017.

[3] P. Chen, S. M. Yu, X. Y. Zhang, et al, ARM-embedded Implementation of a Video Chaotic Secure Communication via WAN Remote Transmission with Desirable Security and Frame Rate, *Nonlinear Dynamics*, vol.86, no.2, pp. 725-740, 2016.

[4] L. L. Tong, F. Dai, Y. D. Zhang, et al, Restricted H.264/AVC Video Coding for Privacy Region Scrambling, *Proceedings of 2010 IEEE 17th International Conference on Image Processing*, IEEE, Hong Kong, China, 2010.

[5] P. G. Chou, C. F. Chuang, W. J. Wang, et al, A Fuzzy-Model-Based Chaotic Synchronization and Its Implementation on a Secure Communication System, *IEEE Transactions on Information Forensics* & *Security*, vol.8, no.12, pp. 2177-2185, 2013.

[6] J. Jiang, Y. Liu, Z. Su, et al, An Improved Selective Encryption for H.264 Video based on Intra Prediction Mode Scrambling, *Journal of Multimedia*, vol.5, no.5, pp. 464-472, 2010.

[7] F. Peng, X. Q. Gong, M. Long, et al, A selective encryption scheme for protecting H.264/AVC video in multimedia social network, *Multimedia Tools* & *Applica-tions*, vol.76, pp. 3235-3253, 2017.

[8] R. H. Deng, X. Ding, Y. Wu, et al, Efficient block-based transparent encryption for H.264/SVC bitstreams, *Multimedia Systems*, vol.20, no.2, pp. 165-178, 2014.

[9] Z. Shahid, W. Puech, Visual Protection of HEVC Video by Selective Encryption of CABAC Binstrings, *IEEE Transactions on Multimedia*, vol.16, no.1, pp. 24-36, 2013.

[10] X. Wang, N. Zheng, L. Tian, Hash key-based video encryption scheme for H.264/AVC, *Signal Processing: image Communication*, vol.25, no.6, pp. 427-437, 2010.

[11] F. Dufaux, T. Ebrahimi, Scrambling for Privacy Protection in Video Surveillance Systems, *IEEE Transactions on Circuits* & *Systems for Video Technology*, vol.18, no.8, pp. 1168-1174, 2008.

[12] H. Xu, X. J. Tong, X. W. Meng, An Efficient Chaos Pseudo-random Number Generator Applied to Video Encryption, *OPTIK*, vol.127, no.20, pp. 9305-9319, 2016.

[13] B. X. Du, Q. Ding, X. L. Geng, Generation and Realization of Digital Chaotic Key Sequence Based on K-L Transform, *Chaos-Fractals Theories and Application*, IEEE, Hangzhou, China, 2011.

[14] Y. Hu, X. Xie, X. Liu, et al, Quantum Multi-Image Encryption Based on Iteration Arnold Transform with Parameters and Image Correlation Decomposition, *International Journal of Theoretical Physics*, vol.56, no.7, pp. 2192-2205, 2017.

[15] Y. J. Li, R. Z. Zhang, J. H. Ge, et al, Periods of the 3-Arnold Transformation and Its Application in Image Encryption, *Journal of University of Electronic Science and Technology of China*, vol.44, no.2, pp. 289-294, 2015.

[16] V. Gelfreich, D. Turaev, Arnold Diffusion in a Priori Chaotic Symplectic Maps, *Communications in Mathematical Physics*, vol.353, no.2, pp. 507-547, 2017.

[17] A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications [EB/OL], *https://csrc.nist.gov/publications/detail/sp/800-22/rev-1a/final.*