Image Secret Key Generation Method Based on Bit Extraction

Shuai Chen[1,*], Xiaojun Xu[2], Youneng Zhang[3], Fang Han[2], Ying Li[1] and Xiaodong Zheng[1]
[1]School of electronic engineering, Huainan normal university, Anhui, China
[2] School of mechanical and electrical engineering, Huainan normal university, Anhui, China
[3] Electrical engineering department, Anhui vocational &technical college of industry and trade, China
[*]Corresponding author

***Abstract*—Bit extraction method from chaos sequence was proposed in the paper to realize image communication secretly. The cipher comes from nonlinear chaos iteration by seeds and processing of bits transformation matrix. First, the principle of image encryption keys was described, the cipher sequence features was calculated. Secondly, the security of cipher was analyzed. Finally, the experiments were completed successfully for image encryption and decryption. The result is that the cipher sequence is with chaotic characteristics and pseudo randomness, and the cipher pool is huge. The conclusion is the bit extraction method with matrix may be used to calculate cipher keys for image confidential communications with high security.**

Keywords-cipher; bit extraction; image encryption; method; transformation matrix

I. INTRODUCTION

The purpose of image security algorithm is essentially for scrambling and diffusion of pixel value, which can be considered from two aspects of algorithm and the key image communication security. It requires more computation despite the complex algorithm [1-3] can improve security. The simple algorithm can reduce the computational complexity through the keys to enhance security.

With the limited number of keys, it needs to design randomness and huge amount of key pool to realize image confidential communications. The feature of chaos sequence is similar to random process and white noise, is extremely sensitive to the initial value. The chaos sequence is with characteristics of the pseudo random key, generated from the initial key by chaotic key stream. It only needs to transmit a small amount of the initial key as a seed when the chaos key used for secure communications. The paper [4] proposes a pseudo-random generator based on chaos. The paper studied the chaos synchronization [6-9]. The paper [10][11]constructs the image encryption algorithm using chaos. The chaos is used to diffuse and scramble plain-text and cipher text in the paper [12-14]. But the whole algorithm generated small key space with lower security. This paper puts forward a kind of key generation method based on seed key and combined with bits and bytes arrangement for image encryption communication.

II. RELATED WORKS

In order to realize image security processing in a hardware chip, an architecture chip with image capture and image encryption was designed. The chip is composed of Capture_ Control, SCCB_ Control, RAM module, Encryption Module and Key_ Generator, seeing Figure I.

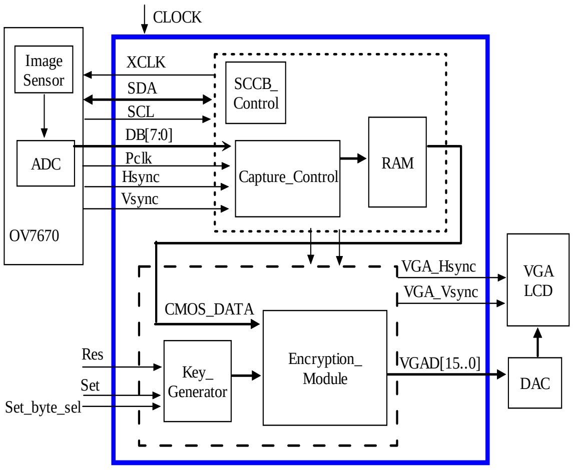


FIGURE I. CHIP STRUCTURE.

The module OV7670, digital to analogy convertor (DAC) and VGA LCD are outside of the design chip. The OV7670 includes analogy to digital convertor ADC, CMOS image sensor, controlled by chip through SCCB bus. The main clock frequency of the CLOCK is 50MHz, and divided to 25MHz for the working clock of the XCLK signal. The SCL is clock line of SCCB bus, the SDA is data line of SCCB bus. The Pclk signal is pixel clock of CMOS（25MHz）,the Hsync signal is line synchronization of CMOS, the Vsync signal is frame synchronization of CMOS, and the VGAD[15..0] are 16bit VGA signal. The Res signal is used to reset value to zero for the inner key register in the time the lowest byte of the key register was selected. The Set_ byte_ sel signal is used to select each byte of the 32bits key register increasingly in turn .The Set signal is used to adjust the selected register byte value.

The image capture is completed under the controlling of the SCCB Control module, Capture Control module and RAM module. The keys are generated through the Key_ Generator module, the image is encrypted in the Encryption Module.

The key generator module was introduced mainly in this paper.

III. Generator Module

A. Principle

Supposing the plain image is P, and then the encryption operation is

$$Q = E(P, K) \qquad (1)$$

where the Q is cipher image, the encryption operation is expressed using E, the K is cipher matrix as

$$K = \begin{bmatrix} k_{11} & k_{12} & \cdots & k_{1M} \\ k_{21} & k_{22} & \cdots & k_{2M} \\ \vdots & \cdots & \vdots & \vdots \\ k_{N1} & k_{N2} & \cdots & k_{NM} \end{bmatrix}, \qquad (2)$$

where the k_{ij} is the components of the matrix K with 16 bits, can be expressed as following vectors

$$\begin{cases} k_{ij} = (b_{15}b_{14}..b_1b_0) \\ b_t \in \{0,1\}, t = 0,1,...,15 \end{cases} \qquad (3)$$

And the k_{ij} is a arrangement of the variable $w_{i,j}$ with 32 bits, the relation is

$$k_{ij}^T = A(w_{i,j}^T \oplus u_{i,j}^T) \qquad (4)$$

The T is transpose of matrix, and the A is 16×32 Transformation matrix for bits, the $w_{i,j}$ may be expressed as

$$\begin{cases} w_{i,j} = (b_{31}b_{30}\cdots b_1b_0) \\ b_t \in \{0,1\}, t = 0,1,\cdots,30,31 \end{cases} \qquad (5)$$

The $w_{i,j}(i=1,2,\cdots,N; j=1,2,\cdots,M)$ is a integer in 32 bits. The $w_{i,j}$ can be calculated as

$$\begin{cases} w_{1,1} = S_1 \\ w_{i,j} = 4w_{i,j-1} - (w_{i,j-1} >> 30) - 1, \\ \quad i = 1,2,\cdots,N; j = 2,3,\cdots,M \\ w_{i,1} = 4w_{i-1,M} - (w_{i-1,M} >> 30) - 1 \\ \quad i = 2,3,\cdots,N \end{cases} \qquad (6)$$

where $S_1 \in [1, 2^{32} - 1]$.

And the $w_{i,j} \in [1, 2^{32} - 1] = [1, 4294967295]$.

The $u_{i,j}$ may be expressed as

$$\begin{cases} u_{i,j} = (b_{30}b_{29}...b_1b_0) \\ b_t \in \{0,1\}, t = 0,1,...,29,30 \end{cases}. \qquad (7)$$

The $u_{i,j}$ is a integer in 31 bits. The $u_{i,j}$ can be calculated as

$$\begin{cases} u_{1,1} = v_1 \\ u_{i,j} = (16807 \times u_{i,j-1}) \bmod (2^{31} - 1) \\ \quad i = 1,2,...,N; j = 2,3,...,M \\ u_{i,1} = (16807 \times u_{i-1,M}) \bmod (2^{31} - 1) \\ \quad i = 2,3,...,N \end{cases} \qquad (8)$$

where $v_1 \in [1, 2^{31} - 1]$ and the $u_{i,j} \in [1, 2^{31} - 1]$.

The transformation matrix A is 16×32 with 1s and 0s element as

$$A = \begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,32} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,32} \\ \vdots & \vdots & \vdots & \vdots \\ a_{16,1} & a_{16,2} & \cdots & a_{16,32} \end{bmatrix}, \qquad 9)$$

where $a_{i,j} \in \{0,1\}; i = 1,2,...,16; j = 1,2,...,32$, and only a 1 exits in each row of matrix A, and only a 1 exits in each line of matrix A.

B. Key Generator Module Realization

The realization are both in Field Programmable Gate Array—FPGA and MATLAB. Figure II. is the key generator structure in FPGA.

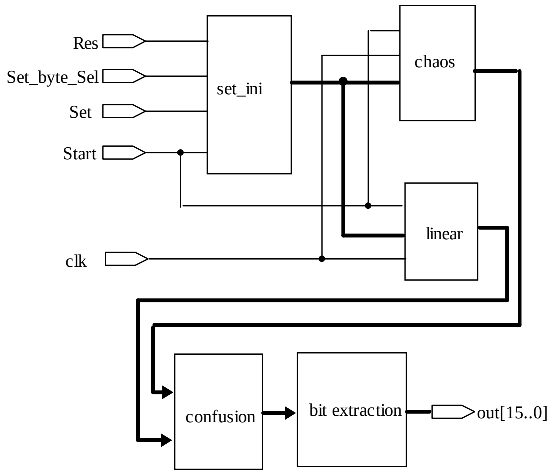


FIGURE II. KEY GENERATOR STRUCTURE.

The set ini module is used for set initial value. The chaos module is used to complete calculation as formula (6). The linear module is used to complete calculation as formula (7). The confusion module is used to complete exclusive 'OR' operation. The bit extraction module is used to complete extraction as matrix A.

In Matlab soft ,the key sequence is generated as Figure II. The 16-bit RGB image encryption and decryption is designed in Matlab soft.

IV. TEST

Figure III. is the simulation result by Modelsim soft. It is visible the sequence is generated rightly under the action of a clock clk signal.

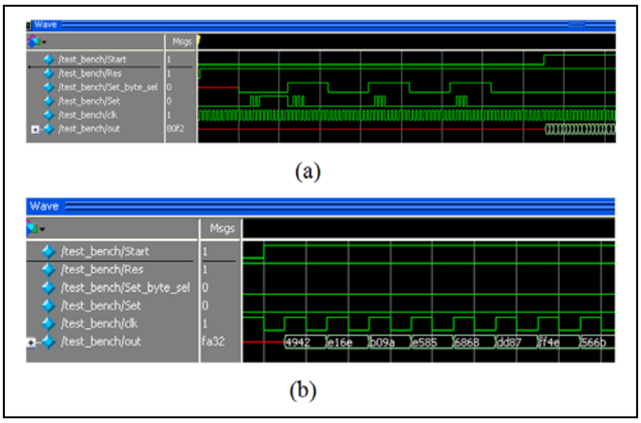
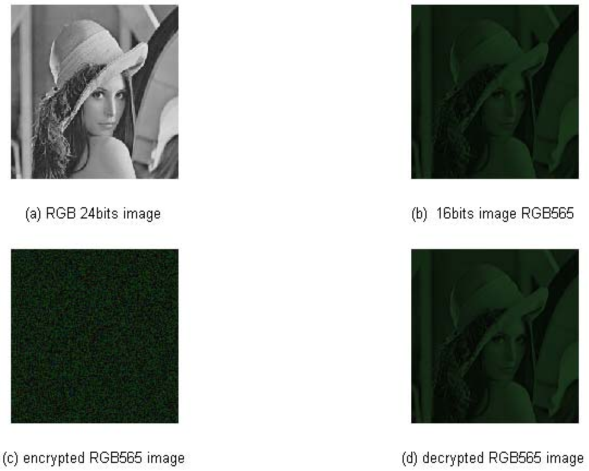


FIGURE III. SIMULATION RESULT BY MODELSIM.



(a) RGB 24bits image

(b) 16bits image RGB565

(c) encrypted RGB565 image

(d) decrypted RGB565 image

FIGURE IV. IMAGE ENCRYPTION AND DECRYPTION.

24-bit image in Figure IV(a) is converted to 16-bit image in 5:5:6 formatted. Using 16-bit RGB images as plain-text image for test inputting, it is shown in Figure IV(b). The random 32-bit seeds key is S1, for example 1235, the key sequence is generated as formula (4). The child keys was produced by the transform matrix A. It is assumed that A is

$$A=\begin{pmatrix}1 & 0 & \cdots & 0 & 0 & \cdots & 0\\ 0 & 1 & \cdots & 0 & 0 & \cdots & 0\\ \vdots & \vdots & \ddots & \vdots & \vdots & \cdots & 0\\ 0 & 0 & \cdots & 1 & 0 & \cdots & 0\\ 0 & 0 & \cdots & 0 & 1 & \cdots & 0\end{pmatrix} \tag{10}$$

According to formula (2), The cipher matrix K in 16-bits is produced from the formula (4). Using cipher matrix K to encrypt plain RGB565 image as formula (1), the encrypted RGB565 image is in Figure IV. (c). The right decrypted image is in Figure IV. (d).

V. ANALYSIS

A. Random Feature

Supposing initial value randomly, for example $S_1 = 1235$, generating cipher sequence with length 5×10^5, calculating its auto-correlation, the result is in Figure V. The auto-correlation in Figure V. has excellent binary feature, that is to say the sequence values is with independent features.

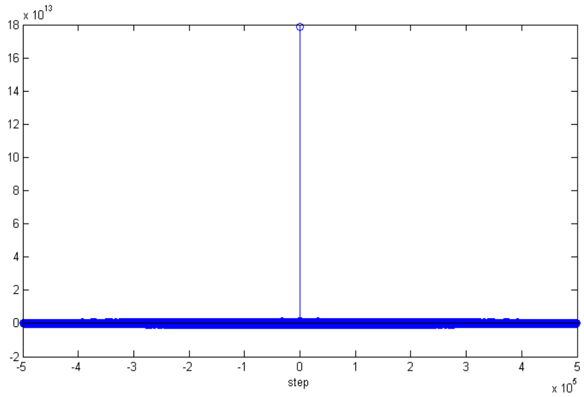


FIGURE V. AUTO-CORRELATION OF CIPHER SEQUENCE.

B. Hypothesis Testing

Total number statistics of bit 1 appears in a 16bit cipher sequence with length 5×10^5 is shown in table 1. The average is 250100 close to ideal of average 250000. The maximum is 2510833, the minimum is 249137. The Pearson χ^2 test is used to the statistical Hypothesis testing, the χ^2 statistics is

$$K_n^2=\frac{1}{n}\sum_{j=1}^{k}\frac{(n_j-np_j)^2}{p_j} \tag{11}$$

where the variable n_j is number of the sample $X_i, i=1,2,\cdots,n$ distributing in distribution interval S_j,the variable k is the number of distribution interval, the p_j is the probability of distribution interval(j is numerical order of distribution).the probability in uniform distribution is $p_j = 1/k$.

For giving level α , when $K_n^2 > \chi^2_{k-1,\alpha}$, the distribution is not uniform distributed in $x_1,\cdots,x_k$,otherwise, it is uniform distributed in $x_1,\cdots,x_k$.

TABLE I. STATISTICS OF THE BIT'1'EXISTING IN DIFFERENT 16BITS OF CIPHER SEQUENCE WITH LENGTH 5*10^5

Bits	**B0**	**B1**	**B2**	**B3**	**B4**
amount	250387	250300	249966	250214	251083
Bits	**B5**	**B6**	**B7**	**B8**	**B9**
amount	249137	250302	249708	249889	249952
Bits	**B10**	**B11**	**B12**	**B13**	**B14**
amount	250179	249942	250368	250052	250074
Bits	**B15**				
amount	250018				

Initial Value：1235.

From table 1, the statistics variable is $K_n^2 = 9.6784$ according to formula (11).if the confidence level $\alpha = 0.05$,then

$$\chi^2_{k-1,\alpha} = \chi^2_{15,0.05} = 25 \\ > K_n^2 = 9.6784 . \tag{12}$$

Hence, it is considered the 1s and 0s is in equality of opportunity in 16bits of the sequence.

C. Security Analysis

The initial cipher key S1 is 32bits, The possible total number of the initial cipher key is

$$W_1 = 2^{32} = 4.295 \times 10^9 \tag{13}$$

The initial cipher key v1 is 32bits, The possible total number of the initial cipher key is

$$W_2 = 2^{32} = 4.295 \times 10^9 \tag{14}$$

The total number of the transformation matrix is

$$W_3 = P_{32}^{16} = 4.1921 \times 10^{20} \tag{15}$$

So the total number of the cipher key is

$$P = W_1 \times W_2 \times W_3 \approx 7.734 \times 10^{39} \tag{16}$$

If the listed 1 trillion key per second by brute force attack, you may need to 2.45×10^{20} years to complete the list the whole key. It is Visible that the exhaustive method is difficult to attack the key solution.

VI. CONCLUSIONS

The key generator module was designed in this paper. Bit extraction method from chaos sequence was proposed in the paper to realize image communication secretly. The cipher comes from nonlinear chaos iteration by seeds and processing of bits transformation matrix. The result is that the cipher sequence is with chaotic characteristics and pseudo randomness, and the cipher pool is huge. The sequence was used for encryption image and decryption RGB565 image successfully.

ACKNOWLEDGMENT

The study was supported by the major fund of nature science for colleges and universities in Anhui province of China (KJ2014A239), and also was supported by the fund of nature science for colleges and universities in Anhui province of China (KJ2011Z342).

REFERENCES

[1] Zhong Z, Chang J, Shan M, et al. Fractionnal Forier-domain random encoding and pixel scrambling technique for double image encryption. Optics Communications,2012,285(1):18-23.

[2] Pande A, Zambreno J. The secure wavelet transform//Embedded Multimedia Security Systems. Springer London,2013:67-89.

[3] Bhatnagar G,Wu Q M J. Chaos-based security solution for fingerprint data during communication and transactions. Instrument and Measurement, IEEE transactions on,2012,61(4):876-887.

[4] Min L, Chen T, Zang H. Analysis of fips 140-2 test and chaos-based pseudorandom number generator . Chaotic Modeling and Simulation, 2013(2): 273-280.

[5] Xu X. Generalized function projective synchronization of chaotic systems for secure communication. EURASIP Journal on Advances in Signal Processing,2011,2011: No.14.

[6] Yang J, Zhu F. Synchronization for chaotic systems and chaosbased secure communications via both reduced-order and step-bystep sliding mode observers. Communication in Nonlinear Science and Numerical Simulation,2013,18(4):926-937.

[7] Hao L, Min L. Statistical tests and chaotic synchronization based pseudorandom number generator for string bit sequence with application to image encryption. The European Physical Journal Special Topics, 2014, 223(8):1679-1697.

[8] Yau H T, Wang M H, Wang T Y,et al. Signal clustering of power disturbance by using chaos synchronization. International Journal of Electrical Power and Energy Systems,2015,64:112-120.

[9] Al-hussaibi W. Effect of filtering on the synchronization and performance of chaos-based secure communication over Rayleigh fading channel. Communication in Nonlinear Science and Numerical Simulation,2015,26(1/2/3):87-97.

[10] Wang X,Wang Q.A novel image encryption algorithm based on dynamic S-boxes constructed by chaos. Nonlinear Dynamics,2014,75(3):567-576.

[11] Zhou Y., Bao L., Chen C. L..A new 1D chaotic system for image encryption. Signal Processing,2014,97:172-182.

[12] Zhu C.A novel image encryption scheme based on improved hyperchaotic sequences. Optics communications,2012,285(1):29-37.

[13] Wang X, Teng L. An image blocks encryption algorithm based on spatiotemporal chaos. Nonlinear Dynamics,2012,67(1):365-371.

[14] Wang X, Chen F, Wang T.A new compound mode of confusion and diffusion for block encryption of image based on chaos. Communications in Nonlinear Science and Numerical Simulation,2010,15(9):2479-2485.