Proceedings of the 2nd International Conference on Computing Innovation and Applied Physics
DOI: 10.54254/2753-8818/19/20230494

LFSR state sequence image encryption method based on VHDL language

Hongwei Niu

Electrical and Computer Engineering, McMaster University, Hamilton, ON, Canada, L8S 4L8

hongweiniukevin@gmail.com

Abstract. In the modern society of digitalization, integration, intelligence, and networking, while people enjoy the convenience of information technology to their production and lives, information security in the network, as the cornerstone of information communication, becomes more and more important. The research is to establish a new image encryption (IE) method based on LFSR state sequence (SS)s in VHDL language, and the stream cipher of LFSR is studied in detail to induce the idea of LFSR SSs based on VHDL language. The correlation coefficient (CC) of the original image (OI) and encrypted image (EI) pixel points (PP) are analyzed from horizontal direction, vertical direction and diagonal direction, and the results show that the CC of adjacent PP of the OI is large, which approaches 1. However, using the encryption algorithm proposed in this paper, the correlation coefficient of the PP of the EI is -0.0282 in the diagonal direction, and the highest correlation coefficient in the horizontal direction is only 0.0122, which indicates that the adjacent PP of the EI are almost uncorrelated with each other. Therefore, the encryption method can well resist statistical attacks, which illustrates the effectiveness, security, and reliability of this new IE method.

Keywords: VHDL Language, LFSR State Sequence, Digital Image, Image Encryption, Stream Cipher.

1. Introduction

As the range of network applications becomes wider and more users, the issue of how to secure data and prevent it from being stolen, tampered with or even destroyed has gained widespread attention. For example, applications such as mobile payment and cloud computing involve the security of national and personal information, which must be prevented from being stolen, leaked and maliciously used. The key technology to solve these problems is data encryption technology. The process of data encryption is actually a complex mapping process in which the plaintext is replaced and transformed by encryption algorithms to obtain the encrypted ciphertext, making it impossible for attackers to recover the plaintext from the encrypted ciphertext and thus improving the security of information. With the rapid development of multimedia technology, image has become one of the main carriers of information, and its security in communication and storage is becoming more and more important, and the research on IE has become more and more hot. This paper designs an LFSR state-sequence IE algorithm in VHDL language, which provides a reference scheme for IE algorithms. The theoretical knowledge of LFSR IE algorithm, including the structure of LFSR, the process of LFSR SS IE and the characteristics of VHDL

DOI: 10.54254/2753-8818/19/20230494

language, is studied; the encryption process of LFSR SS IE based on VHDL language is studied in detail, and the effectiveness, security and reliability of this new IE method are demonstrated and verified by the digital simulation method. Although the network brings convenience to people, it also poses some potential security problems. In terms of security, the openness of the Internet has become its fatal weakness. The LFSR state sequence image encryption method based on VHDL overcomes the problems of small key space and limited precision in the encryption system in the past. The 128b sequence of LFSR ensures the security of the encryption system: the encryption effect of one encryption at a time ensures the security of plaintext images.

2. Literature review

IE is an effective and important method for protecting confidential images. Due to the need for information security, people have been concerned and researching methods and means of securing data since ancient times, and cryptography has been of interest since the advent of traditional passwords. With the progress of technology and the development of cryptography, there has been a slow transition from the original traditional cipher to the modern cipher in today's society. For IE methods, many scholars at home and abroad have studied this.

Khan S proposed a new hybrid IE method to protect confidential and command images by using (LSS), 2D metacellular automata and FSM based DNA rule generator. A secure hashing algorithm is used to generate the key and compute the initial value of the LSS. The proposed encryption scheme is robust against well-known attacks such as statistical attacks, brute force attacks, differential attacks and pixel attacks [1]. Karimzadeh F proposed a hardware-aware pruning method using LFSRs (LFSR) to generate non-zero weighted positions in real time during inference. Two different architectures, LFSR-based row/column indexing and column indexing, are explored for hardware-friendly LGPS techniques [2]. Geng S scrambles the four frequency bands using chaotic sequences and zigzag scanning curves to construct scrambling matrix. Chaotic sequences, DNA coding and automata are combined, and the sequences are diffused by using key stream to further improve the security of cryptographic images [3].

Based on the stream cipher of LFSR, this paper analyzes the construction of LFSR in detail, and classifies and analyzes various stream ciphers based on LFSR. The characteristics of VHDL are discussed, and the idea of constructing stream cipher by block cipher unit and LFSR is introduced. The security and reliability of LFSR state sequence image encryption process based on VHDL are discussed.

3. VHDL Language and LFSR analysis

3.1. LFSR-based Stream Cipher

3.1.1. Nonlinear filter generator. The nonlinear filtering of the state of an LFSR is called the filter generator, as shown in Figure 1. The function f0 is called the filter function, and the generated sequence is called the filter sequence. The function f0 chosen in the generator must be nonlinear. Otherwise, the linear complexity of the filter sequence does not exceed the order of the LFSR, so that the generated sequence is easily attacked by the BM algorithm.

DOI: 10.54254/2753-8818/19/20230494

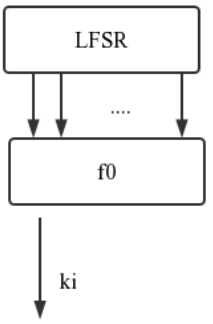

Figure 1. Filter generator [4].

3.1.2. Scaling down the generator. The basic components of the scaling generator are the binary linear shifters, noted as LFSR1 and LFSR2, as shown in Figure 2, and the function f0 is in fact the rule of scaling. So the generated sequence is a reduced sequence. The sequence is made by reducing the output sequence of LSFR1 under the control of LSFR2 as follows: if the current output of LSFR2 is 1, the output bits of LSFR1 are taken as the output; otherwise, the output of LSFR1 is discarded. The performance of the reduction generator is quite good, so many evolutions have appeared, such as self-reduction [5].

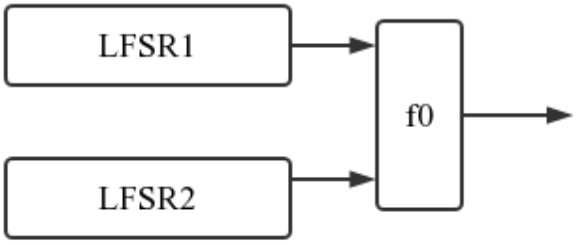

Figure 2. Reduction generator [6].

In addition to the above methods for constructing LFSR-based stream passwords, packet cipher techniques can also be used to construct LFSR-based stream passwords. This is because the design of grouped passwords is much more mature compared to stream passwords.

3.2. LFSR structure

Since the number of register levels r of the LFSR is uniquely related to the feedback coefficients ci (i $\in \{0, 1, 2, ..., r\}$) is unique, this relationship can be described using a polynomial in terms of the feedback coefficients, and the r-level LFSR polynomial F(x) can be expressed as shown in Equation (1).

$$F(x) = c_r x^r + c_{r-1} x^{r-1} + c_1 x^1 + c_0 x^0 = \sum_{i=0}^{r} c_r x^i \tag{1}$$

The LFSR has a length of 1 bit per register, and its linear feedback function is shown in Equation (2).

$$a_r = (c_r a_0 + c_{r-1} a_i + ... + c_1 a_{r-1}) \bmod 2 = (\sum_{i=1}^{r} ciar - i) \bmod 2 \tag{2}$$

Commonly used primitive polynomials corresponding to m-sequences of different lengths are shown in Table 1, giving the algebraic and 8-decimal representations of the primitive polynomials corresponding to different levels of r. Except for r = 2, there are multiple primitive polynomials for each m-sequence,

DOI: 10.54254/2753-8818/19/20230494

and Table 1 lists the commonly used primitive polynomials with simple structures.

Table 1. Common primitive polynomial [7].

Primitive polynomial		
r	Algebraic expression	Octal notation
2	x^2+x+1	7
3	X^3+x^2+1	13
4	X^4+x+1	23
5	X^5+x^2+1	45
6	X^6+x+1	103
7	X^7+x^3+1	211
8	$X^8+x^4+x^3+x^2+1$	435

3.3. VHDL Features

Hierarchical Segmentation Description Capability Designers can subdivide their design goals layer by layer until the final basic circuit module-level description by using the hierarchical segmentation description feature of the VHDL language. In hierarchical subdivision circuits, not only the most basic gate-level circuits can be described, but also the entire circuitry contained in the entire system can be written [8-9]. In terms of classification, it can be further divided into behavioral descriptions characterized by behavioral approach, structural descriptions with structured classification, or a mixture of both descriptions in a single constructive design.

The widely supported and easy to modify VHDL language is widely used and there are many designers who use it for programming and design. Since the VHDL hardware description language was added to the IEEE standard early and is an industry standardized description language, many EDA design software are written in this as the main language. Its ease of modification is also an important reason why the VHDL language is widely used. It is mainly compiled and simulated on the software in the pre-design stage, and if there are errors the software will issue error alerts or warnings, and only the program needs to be rechecked or changed before it is finally implemented in the physical hardware circuit, which is simple and easy to use [10].

Easy to call and efficient, the VHDL language can call many standardized modules already in the library (e.g., gate or register circuits), as well as use previously designed circuit modules of your own.

4. LFSR SS IE process based on VHDL Language

4.1. LFSR SS IE process

Let both the original reference image f(x,y) and the image to be encrypted g(u,v) be digital images of M × N pixels. The initial phase $\varphi(x,y)=\exp(i\theta(x,y))$ is a random phase function, where $\theta(x,y)$ denotes an independent white noise sequence uniformly distributed in $[0, 2\pi]$ of independent white noise sequences, and IE is implemented according to the following steps:

(1) Random coding of the OI f(x,y) yields:

$$F(x,y) = f(x,y)\cdot\varphi(x,y) \tag{3}$$

That is, the matrix f(x,y) is multiplied by the elements at the corresponding positions in $\varphi(x,y)$.

(2) A discrete dual-parametric vector transformation of the image F(x,y) yields the image G(u,v), i.e.

$$G(u,v) = \left|G(u,v)\right|\exp(i\phi(u,v)) \tag{4}$$

(3) A discrete dual-parameter vector inversion of the image g_1 (u,v) yields the image f_1 (x,y).

$$f_1(x,y) = \left|f'(x,y)\right|\exp(i\theta'(x,y)) \tag{5}$$

DOI: 10.54254/2753-8818/19/20230494

(4) Repeat the above steps to satisfy the condition $f(x,y)=f_1(x,y)$ at the end of the iteration. At this time, the corresponding obtained phase $\theta_1(x,y)$ is the EI C, which is the ciphertext image of the OI g(u,v). In the actual encryption simulation process, the double-parameter vector power-weighted you-transform GS algorithm end-of-iteration condition is modified as$\|f(x,y)-f_1(x,y)\| \leq \tau$, where$\tau > 0$ is a pre-given accuracy parameter.

In the LFSR SS IE process, the vector powers as well as the free parameters and the dimension M constitute the encryption key, so the dimension of the key space of this IE system will be a large value, which can significantly increase the security of the IE system.

4.2. LFSR SS IE based on VHDL Language

Suppose the pixel matrix of the PI is P, the pixel matrix of the middle ciphertext image is B and the pixel matrix of the final ciphertext image is C. The size of the PI is M × N.

Firstly, the digital image of M×N pixels is transformed into a parameter matrix of M×N; compare M and N, i.e., row and column sizes, if M=N, the image is directly disordered by Arnold transform, and the disordering effect is better after several times of disordering. If M≠N, the image is considered to be completed and then Arnold transformed, to balance complexity of algorithm and the effect of the Arnold transform, several typical pixel sizes are set, complete the image to the basic standard size and then carry out the disorder operation. The number of times of disorder is based on the image after the addition, and finally complete the Arnold disorder of the whole image.

A set of one-dimensional chaotic sequences $x=\{x_i, i=1,2,\cdots,L\}$ is generated by iterating with the keys x_0 and μ as the iterative initial values and parameters of the modified segmented logistic chaotic mapping, respectively. To ensure the chaotic properties of the sequences, the results of the first 100 iterations are discarded, when M=N, the length L of the x sequence coincides with the number of PP M×N of the PI, and if M≠N, the length L of the x the length L of the sequence is the same as the number of PP of the additive image.

The resulting chaotic sequence is mapped between [0, 255] to obtain the pixel diffusion key sequence k_i; the key sequence k_i is transformed into matrix K; the matrix K is anisotropic with each pixel point in the corresponding position of the matrix B after Arnold dislocation to complete the diffusion of the gray value of each pixel point of the image, so as to obtain the final matrix C by pixel value position dislocation and pixel gray value diffusion, and finally the EI is obtained. The whole encryption process is shown in Figure 3.

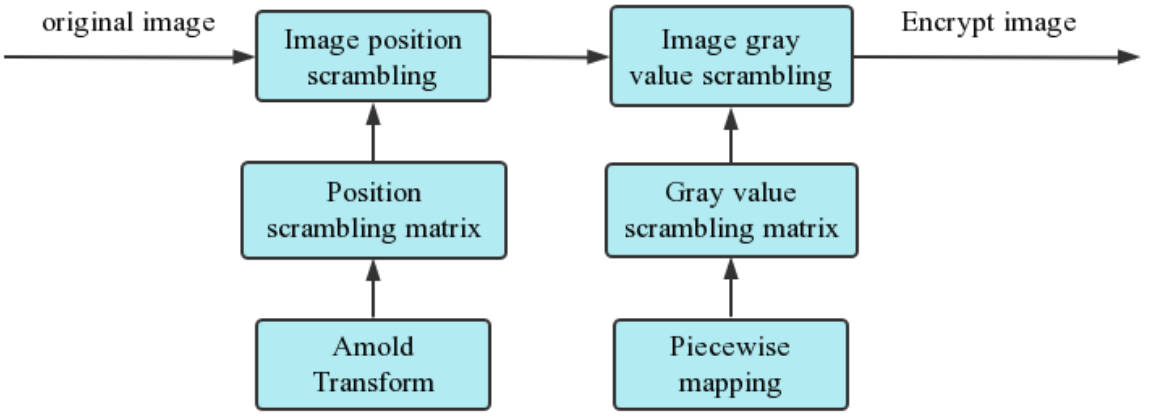

Figure 3. IE process [11].

5. Security and reliability analysis of LFSR SS IE algorithm based on VHDL Language

For most images, whether in their horizontal, vertical or diagonal direction, to analyze the correlation magnitude of adjacent pixels in the three directions of the image obtained by encrypting the barb image with the encryption method proposed in this paper, we randomly take out 5000 pairs of adjacent pixels in the horizontal, vertical and DD from the grayscale image of the barb and its cipher image, and

DOI: 10.54254/2753-8818/19/20230494

calculate them according to the following formula cc [12].

$$cc = \frac{\operatorname{cov}(x, y)}{\sqrt{D(x)D(y)}} \tag{6}$$

Among them:

$$\begin{aligned} \operatorname{cov}(x, y) &= \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \\ \mathrm{D}(x) &= \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \\ \mathrm{E}(x) &= \frac{1}{N}\sum_{i=1}^{N}x_i \end{aligned} \tag{7}$$

The results of correlation calculations for plaintext and ciphertext images are shown in Table 2 and Figure 4.

Table 2. Correlation analysis results [13].

direction	Pixel correlation coefficient of OI	Pixel correlation coefficient of dense map
horizontal direction	0.9292	0.0122
vertical direction	0.9591	-0.0187
Diagonal direction	0.9094	-0.0282

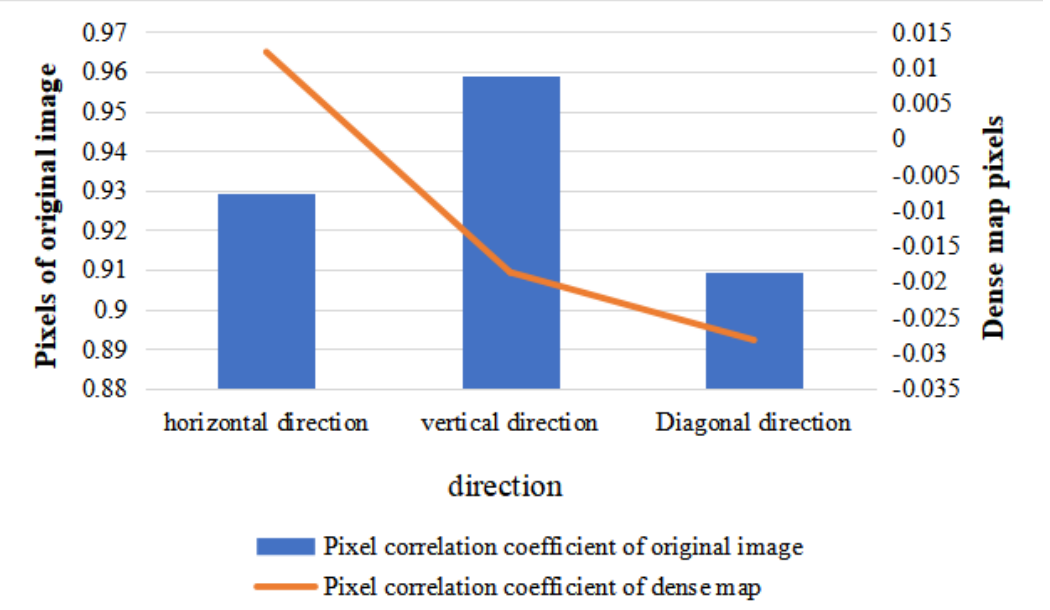

Figure 4. Analysis of pixel correlation between OI and EI [13].

However, the CC of the ciphertext images obtained after encrypting the barb images with the encryption algorithm proposed in this paper are very small, and some of them are even negative. The correlation coefficient of the ciphertext PP is -0.0282 in the diagonal direction and the highest correlation coefficient is only 0.0122 in the horizontal direction, which indicates that the CC of the EIs are almost irrelevant. This indicates that the adjacent PP of the EI are almost uncorrelated with each other. Therefore, the

DOI: 10.54254/2753-8818/19/20230494

encryption method can resist statistical attacks well. The LFSR technique based on VHDL language proposed in this paper is effective against the statistical method attack.

6. Conclusion

IE is an effective technique to protect the confidentiality of digital images. The author designed a VHDL-based LFSR state-sequence IE algorithm, and the correlation analysis between the OI and the EI PP has achieved the design performance index requirements. The IE algorithm designed in this paper can be considered to be applied to color IE and digital watermarking technology. But there are still some shortcomings in this paper due to the lack of the author's level and time: this paper has disordered the whole image too many times during the experimental process, which consumes a lot of resources. Because the process in this simulation system only abstracts the logic function of VHDL language in the translation stage, and does not deal with the delay characteristics of each element, the simulation cannot accurately reflect the delay characteristics of the actual elements.The next step needs to focus on the delay model to further improve the simulation system; Add the compiling and error checking function. You can consider embedding an open source VHDL compiler or a compiler module written by yourself for error checking; Expand support for VHDL syntax. Considering the complexity of VHDL, the system only extracts a part of VHDL syntax for support, so the next step is to expand VHDL syntax support to improve user friendliness.

References

[1] Khan S, Han L, Lu H, et al. 2019. A new hybrid IE algorithm based on 2D-CA, FSM-DNA rule generator, and FSBI [J]. IEEE Access, PP(99):1-1.

[2] Karimzadeh F, Cao N, Crafton B, et al. 2020. A Hardware-Friendly Approach Towards Sparse Neural Networks Based on LFSR-Generated Pseudo-Random Sequences [J]. Circuits and Systems I: Regular Papers, IEEE Transactions on, PP(99):1-14.

[3] Geng S, Wu T, Wang S, et al. 2020. IE Algorithm Based on Block Scrambling and Finite State Machine [J]. IEEE Access, PP(99):1-1.

[4] Man Z, Li J, Di X, et al. 2019. An Image Segmentation Encryption Algorithm Based on Hybrid Chaotic System [J]. IEEE Access, PP(99):1-1.

[5] Sun S, Guo Y, Wu R. 2019. A Novel Plaintext-Related IE Algorithm Based on Stochastic Signal Insertion and Block Swapping [J]. IEEE Access, 7(12):123049-123060.

[6] Paul, A., Kandar, S., & Dhara, B. C. 2022. Image encryption using permutation generated by modified Regula-Falsi method. Applied Intelligence, 1-20.

[7] Kapinesh, G., Sachin Kumaran, K., Gayatri, K., Mohan, T., Thanikaiselvan, V., Subashanthini, S., & Amirtharajan, R. 2022. New Image Encryption Method using Multiple Chaotic Map Computation and Irregular Diffusion Process. Journal of Uncertain Systems.

[8] Subhajit Adhikari, Sunil Karforma. 2022. A novel IE method for e-governance application using elliptic curve pseudo random number and chaotic random number sequence. Multim. Tools Appl. 81(1): 759-784

[9] Noor Munir, Majid Khan, Abd Al Karim Haj Ismail, Iqtadar Hussain. 2022. Cryptanalysis and Improvement of Novel IE Technique Using Hybrid Method of Discrete Dynamical Chaotic Maps and Brownian Motion. Multim. Tools Appl. 81(5): 6571-6584

[10] Kaimeng Chen, Chinchen Chang. 2021. High-capacity separable reversible data-Hiding method in EIs based on block-level encryption and Huffman compression coding. Connect. Sci. 33(4): 975-994

[11] Walaa M. Abd-Elhafiez, Mohamed Heshmat. 2020. Medical IE via lifting method. j. Intell. Fuzzy Syst. 38(3): 2823-2832

[12] Mahdieh Ghazvini, Mojdeh Mirzadi, Negin Parvar. 2020. A modified method for IE based on chaotic map and genetic algorithm. Multim. Tools Appl. 79(37-38): 26927-26950

[13] Farah Naz, Ijaz Ali Shoukat, Rehan Ashraf, Umer Iqbal, Abdul Rauf. 2020. An ASCII based effective and multi-operation IE method. Multim. Tools. Appl. 79(31-32): 22107-22129.