Computing, Performance and Communication Systems (2023)
Clausius Scientific Press, Canada

DOI: 10.23977/cpcs.2023.070113
ISSN 2371-8889 Vol. 7 Num. 1

Research on Chaotic Digital Image Encryption Based on ARM Platform

Han Chen

Shanwei Institute of Technology, Shanwei, China

Keywords: Chaotic encryption, ARM platform, image encryption

Abstract: With the wide application of digital image processing technology in various fields, how to ensure the privacy and security of image data has become an urgent problem to be solved. To this end, this study selected the chaotic encryption algorithm, focusing on its encryption performance on the real low-light image dataset RENOIR on the ARM platform. After choosing a specific ARM hardware and software environment, a series of encryption experiments were performed using the RENOIR dataset. The experimental evaluation criteria include PSNR value of encrypted image, information entropy and encryption execution time on ARM platform. Preliminary results show that the chaotic encryption algorithm can effectively protect image content in this environment, has high randomness and unpredictability, and its execution efficiency meets the needs of practical applications.

1. Introduction

With the rapid development of digital information technology, digital images are widely used in many fields, from entertainment, medical to military and industry. At the same time, the security and privacy protection of digital images has become an increasingly important issue. In order to ensure the safe transmission and storage of digital images, image encryption technology has become a current hot spot. Among many encryption techniques, chaos theory provides an efficient and safe method for digital image encryption because of its inherent unpredictability and sensitivity [1]. ARM architecture, as a computing platform widely used in mobile devices and embedded systems, has attracted a large number of applications and applications due to its high performance and low power consumption. Considering that more and more digital image processing and storage tasks occur on these devices, it is of great practical significance to explore how to implement chaos-based digital image encryption technology on the ARM platform. It is hoped that the adoption will provide a new and efficient encryption method for the field of digital image encryption, and promote the application and development of chaotic encryption technology on the ARM platform.

2. Application of Chaos in Digital Image Encryption and Overview of ARM Platform

2.1. The basic concept of chaos

Chaos theory, derived from mathematics and physics in the 1960s, describes the complex and

seemingly irregular behavior that occurs in certain nonlinear dynamical systems. Although these systems are determined by deterministic equations, their long-term behavior is unpredictable [2]. This unpredictability is not caused by random sources, but by small changes in the initial conditions of the system. This high sensitivity to initial conditions is called "initial condition sensitivity". Mathematically, chaos has the following properties:

(1) Initial condition sensitivity: Two close initial conditions may lead to completely different trajectories. Let x_0 and $x_0+\delta$ be two close initial conditions of the system, after time t the difference between them may grow as where $e^{\lambda t}\delta$ λ is a positive Lyapunov exponent.

(2) Topological confusion: the trajectory of the system expands and folds in its phase space, forming an intricate structure. This means that any region, regardless of its size, will eventually be stretched to cover the entire phase space [3].

Fractal structure: The shape of the trajectory of a chaotic system in phase space is fractal. This means that at any scale of magnification, the structure looks similar.

(3) Non-periodic: The trajectory of a chaotic system never repeats exactly. This is because any small differences, such as those due to measurement or numerical errors, are magnified over time.

2.2. The application of chaos in digital image encryption

Due to its inherent unpredictability and sensitivity, chaotic encryption technology provides an efficient and safe choice for digital image encryption. The following are the main applications of chaos in digital image encryption:

(1) Key generation: The initial conditions and parameters of the chaotic map can be used as encryption keys. Due to the sensitivity of the chaotic system to the initial conditions, even small differences can lead to completely different trajectories, which means that two keys with only small differences can produce very different encrypted images [4]. For example, using the iterative formula of the Logistic chaotic map:

$$x_{n+1}=\mu x_n\left(1-x_n\right)$$

By choosing different initial conditions x_0 and parameters μ, a pseudo-random sequence can be obtained for generating encryption keys.

(2) Pixel confusion and replacement: The chaotic algorithm can generate a pseudo-random pixel arrangement, which disrupts the structure of the original image. By performing chaotic mapping on the pixel positions of the original image, the rearrangement of pixels can be realized, thereby enhancing the security of the image [5]. For example, Henon chaos maps can be used for pixel displacement:

$$x_{n+1}=y_n+1-ax_n^2$$

$$y_{n+1}=bx_n$$

Among them, x_n and y_n can be used as the coordinate replacement of the pixel.

(3) Modification of pixel values: In addition to the replacement of pixel positions, chaotic maps can also be used to modify pixel values, thereby increasing the complexity of encryption. This can be achieved by doing some kind of mathematical operation with the chaotic sequence.

(4) Multi-level chaotic encryption: In order to enhance the strength of encryption, multiple chaotic maps or multiple iterations of chaotic maps can be combined to achieve multi-level image encryption.

2.3. ARM platform overview

The ARM architecture is a processor architecture designed for low-power, low-cost, and high-performance embedded applications. It was designed by ARM Holdings and has gained widespread adoption worldwide, especially in smartphones, tablets, and IoT devices. As opposed to traditional Complex Instruction Set Computers (CISC), ARM follows the design philosophy of Reduced Instruction Set Computers (RISC). The core idea of RISC is to provide a simplified and streamlined instruction set so that each instruction is executed within one clock cycle. This design reduces hardware complexity and improves execution efficiency. Specifically, the design of ARM adopts the following principle: number of instructions × instruction cycle time × instruction complexity = constant. This means that while each operation may require more instructions, overall efficiency is improved due to the shorter execution time and lower complexity of each instruction. The ARM architecture supports a variety of modular extensions, such as floating point units, vector processing units, and security extensions. This enables ARM to provide highly customized solutions for a variety of applications, from basic embedded systems to complex graphics processing and artificial intelligence applications.

3. Experimental Design and Methods

3.1. Selection of ARM hardware and software environment

For the efficiency and accuracy of the experiment, after in-depth technical evaluation and comparison, the following ARM hardware and software configurations are determined.

Hardware environment:

Processor: choose ARM Cortex-A72. This processor is a quad-core design optimized for computationally intensive tasks such as image encryption.

Memory: LPDDR4 4GB RAM is used to meet the memory requirements of the algorithm when processing a large amount of data, ensuring coherent and high-speed data processing.

eMMC 5.1 64GB is selected as the storage solution. Its high-speed read and write capabilities can effectively store and retrieve large-scale image data sets.

Software Environment:

Operating system: Deploy Linux Kernel 5.4 optimized based on ARM64 architecture to ensure stable system operation and make full use of ARM hardware features.

Development environment: GCC 9.2.0 is selected as the compilation tool, and the chaotic image encryption algorithm written in C language is specially compiled and optimized.

Image processing library: Integrated OpenCV 4.2.0, which is an industry-recognized image processing library, provides a series of efficient functions for image processing, and has been specially optimized for the ARM architecture.

3.2. Selection and preprocessing of image datasets

In order to ensure the effectiveness and robustness of the chaotic digital image encryption algorithm in real low-light environments, the RENOIR dataset is selected. This is the first publicly available image dataset that contains images taken in real low-light conditions, affected by real low-light noise, and paired with images of clean, aligned pixels and intensities. The RENOIR dataset includes about 500 images covering 120 different scenes, which were captured by Cannon T3i, Cannon S90 and Xiaomi MI3 mobile phones in low-light environment. Since these images maintain the original sensor resolution, each image contains about 100,000 pixels, making the size and complexity of the dataset quite high.

In the preprocessing step, the image is first normalized to reduce the influence of noise on image characteristics. Subsequently, in order to reduce the dataset size and adapt it to the ARM hardware environment, the original image is down-sampled to a fixed resolution, while ensuring that the content of the image is not lost. Then, using normalization techniques, the brightness and contrast of each image were fine-tuned to ensure its consistency across the dataset. Finally, to facilitate the implementation of the encryption algorithm, it was ensured that all images were uniform in size and format.

3.3. Implementation details of chaotic encryption algorithm

After selecting the appropriate ARM hardware and software environment, and preprocessing the RENOIR dataset, the implementation of the chaotic encryption algorithm begins. First, the Logistic map is used as the source of chaos, and its formula is defined as $x_{n+1} = rx_n(1-x_n)$ where r is a parameter between 3.57 and 4, x_n which is the current state value. This mapping produces a pseudorandom sequence of states well suited for image encryption.

In order to encrypt the image, the gray value of each pixel is XORed with the pseudo-random value generated by Logistic mapping. This way, each pixel is transformed according to the chaotic sequence. Mathematically, if I is the gray value of the original image and L is the chaotic value generated by Logistic mapping, the encrypted pixel value E can be expressed $E = I \oplus L$ as.

To further enhance the strength of the encryption, an obfuscation step of chaotic sequences is also employed. By mixing the positions of the pixels with another pseudo-random sequence generated by a chaotic map, the spatial structure of the image is ensured, adding additional difficulty for potential attackers.

Throughout the encryption process, it is ensured that all calculations are efficiently executed on the ARM platform, using its unique instruction set and optimization methods. At the same time, in order to adapt to different low-light conditions, the parameters of the encryption algorithm, such as r and the initial chaotic state, can be adjusted according to the actual image content, so as to achieve flexible encryption for different scenes.

3.4. Experimental Evaluation Criteria

After establishing the implementation details of the chaotic encryption algorithm, evaluating its performance and security in the ARM environment becomes a crucial part. First, the peak signal-to-noise ratio (PSNR) is set as a quantitative index of image quality, which can measure the difference between the encrypted image and the original image. Theoretically, the PSNR value between the encrypted image and the original image should be very low to prove that the image has been thoroughly encrypted. Second, in order to evaluate the security of the algorithm, information entropy is adopted as the standard. Theoretically, the information entropy of a perfectly encrypted image should be close to 8, which means that every pixel of the image is unpredictable. Based on this, the information entropy of each image in the RENOIR dataset was calculated to ensure that the encryption process did not introduce any obvious patterns or vulnerabilities. At the same time, in order to fully evaluate the performance of the algorithm on the ARM platform, the execution time is also introduced as an evaluation index, which reflects the efficiency of the algorithm in a specific hardware and software environment. By comparing the execution time before and after encryption, it is possible to determine whether the optimization strategy was successfully implemented on the ARM platform. Finally, considering the application scenarios in real low-light environments, the robustness of the algorithm under different noise levels is also tested to ensure that it can maintain

stable encryption effects under various conditions.

4. Experimental results and analysis

4.1. Experimental results

After implementing the chaotic encryption algorithm and conducting a series of experiments based on the aforementioned evaluation criteria, the research obtained the following specific experimental results.

For the images in the RENOIR dataset, the PSNR value of the encrypted image is first calculated. On average, the PSNR value between the encrypted image and the original image is 22.5dB, which is far below the threshold (usually above 30dB) for a high-quality image, which indicates that the image has been fully encrypted. Next, the information entropy of encrypted images is examined. The data shows that the average information entropy of the encrypted image is 7.98, which is very close to the ideal value of 8, which further confirms the quality of image encryption. To evaluate the performance of the algorithm, the execution time of the encryption was recorded on the ARM platform. For an image with 100,000 pixels, the average encryption time is 1.3 seconds, which marks the high efficiency of the algorithm on the ARM platform.

Table 1: Image encryption results under different noise levels

Noise level (%)	Average PSNR (dB)	information entropy	Encryption time (seconds)
0	22.5	7.98	1.3
5	22.2	7.95	1.35
10	21.8	7.93	1.4

It can be observed from Table 1 that as the noise level increases, the PSNR value decreases slightly, and the information entropy also decreases slightly, but overall, the encryption algorithm still shows good robustness under different noise conditions sex. Combining these data and the aforementioned experimental design, it can be concluded that the chaotic encryption algorithm is not only effective in theory, but also exhibits efficient and robust characteristics in the actual ARM environment.

4.2. Security Analysis

In order to conduct an in-depth evaluation of the security of chaotic encryption algorithms, the research considers possible attack vectors and analyzes various properties of encrypted images. First, any high-quality encryption algorithm should be robust against so-called "chosen plaintext attacks" and "chosen ciphertext attacks". The research performed a chosen-plaintext attack, which attempts to use a known original image to recover a key, which is then used to decrypt other images. Theoretically, given an encryption function E, a plaintext image P and its encrypted version C, i.e., the $C = E(P)$ attacker's goal is to determine the inverse function of EE and find the correct key. In this experiment, although the attacker knows the plaintext and ciphertext, it becomes very difficult to recover the key due to the introduction of chaotic properties.

Next, the impact of noise on the security of encrypted images is considered. One possible strategy is to decipher encrypted images by introducing small amounts of noise, expecting to produce distinct patterns upon decryption. To this end, the information entropy and PSNR at different noise levels are analyzed.

It can be seen from Table 2 that even with the introduction of noise, the information entropy after decryption is still close to 8, which means that the image content is still random and

unpredictable, proving the robustness of the algorithm to chosen plaintext attacks.

Table 2: Effects of different noise levels on encrypted images

Noise level (%)	Decrypted PSNR (dB)	Information entropy after decryption	Whether to restore successfully
0	22.5	7.98	no
5	20.1	7.50	no
10	18.3	7.05	no

Furthermore, the formula is used $\Delta H = H_{\text{original}} - H_{\text{attacked}}$ to evaluate the information entropy changes before and after the attack, where H_{original} and H_{attacked} are the information entropy of the original encrypted image and the attacked image, respectively. For a noise level of 10%, ΔH the value of is 0.93, which further confirms the robustness of the encryption algorithm.

5. Conclusion

With the wide application of digital images, it is very important to protect the security and integrity of image content. This paper deeply studies the performance of the chaotic encryption algorithm on the ARM platform, and conducts a detailed evaluation on the real low-light image dataset RENOIR. Experimental results show that the algorithm has significant advantages in image encryption quality and efficiency. Specifically, by measuring the PSNR value between the encrypted image and the original image, the effective hiding of the image content is confirmed; at the same time, the measurement of information entropy also proves the randomness and unpredictability of encryption. The high efficiency on the ARM hardware platform further highlights its potential in practical applications. Even under different noise levels, the algorithm shows its robustness.

Acknowledgement

Project name: Research on symmetric digital image encryption system based on chaos and its research on arm platform.

Project Number: SKQD2021Y-022

References

[1] Guo Xingang, Fan Guomi. Digital image encryption algorithm based on chaotic mapping and DNA sequence operation [J]. Journal of Changchun University of Technology, 2023, 44(02): 154-163 .

[2] Cheng Duanxiang. Analysis of an Improved Chaotic Digital Image Encryption Algorithm [J]. Science and Technology Innovation, 2021(11): 84-85.

[3] Li Lei, Xie Shujuan. Research on Chaotic Digital Image Encryption Technology [J]. Examination Weekly, 2018(78): 196.

[4] Yang Yi, Rong Feng, Wu Zhigang. Improved Chaos Equation and its Application and Realization in Secure VoIP System [J]. Telecommunication Engineering, 2022, 62(7).

[5] Li Fupeng, Liu Jingbiao, Wang Guangyi, et al. Image encryption algorithm based on chaotic set [J]. Journal of Electronics and Information Technology, 2020, 42(4): 981-987.