Media and Communication Research (2024)
Clausius Scientific Press, Canada

DOI: 10.23977/mediacr.2024.050412
ISSN 2523-2584 Vol. 5 Num. 4

Application of Blockchain and 5G Virtual Reality Technology in Digital Media Art Design

Juan Wu[1,a,*], Nianhao Xu[1,b]

[1]*College of Digital Commerce and Live Broadcasting, Anhui Lvhai Vocational College of Business, Hefei, Anhui, China*
[a]*1660071620@qq.com*, [b]*nianhaoxu@163.com*
[*]*Corresponding author*

Keywords: Digital Media Art Design, Virtual Reality Technology, Digital Simulation, Chaos Theory, Triple Data Encryption Standard Algorithm, Blockchain Technology

Abstract: Blockchain technology originates from the underlying framework of bitcoin system. It is a distributed storage scheme featuring decentralization, distrust, collective maintenance, timing data, programmable and immutable, etc., which has great historical significance for many fields and even the whole macro social system. The emergence and innovation of communication technology makes digital media art (DMA) appear in the public eye. Its medium and form are constantly changing. Among them, digital images have become the mainstream of DMA design. The emergence of digital images not only brings new visual experience to the public, but also has been applied and innovative in various fields. However, it also brings security problems of image data. Image data involves the privacy and property of others, which needs to be protected and encrypted. Aiming at the above problems, this paper compared and analyzed the performance of Triple Data Encryption Standard (TDES) image encryption system, Advanced Encryption Standard (AES) image encryption system and chaos-based image encryption algorithm. The research results showed that the chaos-based image encryption algorithm had advantages in real-time performance. The encryption time and decryption time were 3.6s and 3.9s, respectively. In images of different sizes, the pixel change rate (NPCR) of both plaintext sensitivity and key sensitivity of the chaos-based image encryption algorithm was 99%. It has laid the foundation for the innovation and development of digital image encryption algorithms.

1. Introduction

Blockchain is a chain structure that combines data blocks in chronological order with cryptography, consensus mechanism, smart contract and other technologies to form a decentralized public account technology. As technology advances, digital images in DMA design have been widely used in many fields. However, it also brings an important problem, which is the security of image data. There is no effective encryption scheme for the most used image data currently. This is because traditional encryption algorithms have long been incapable of performing encryption operations on image data with large amounts of data and high redundancy. In order to further understand and analyze the development and practice of DMA design, this paper studies and analyzes the development and practice of DMA design based on the virtual reality technology (VRT) of digital simulation.

The development of DMA is more and more extensive. Many scholars have conducted research on DMA design. Scholar Moreno L reflected and summarized the new status of museums in the digital age [1]. Li H believed that digital technology had a profound impact on the changes in artistic expression and language forms [2]. Kong W believed that the development of digital media (DM) technology has broadened people's way of life. Thus a new visual formal language was constructed [3]. Lucas T studied how fictional and non-fictional characters were represented in various media [4]. Guo S proposed a method to directly extract I-frames in the compressed domain, which overcame the shortcomings of traditional video retrieval algorithms that decompress video files before processing [5].

In view of the above problems, this paper researched the development and practice of DMA design based on the VRT of digital simulation. VRT has many uses. Scholar Maples-Keller J L evaluated the literature on the effectiveness of virtual reality (VR) in the treatment of psychiatric disorders [6]. Liang Z conducted research on value identification and traditional village protection based on VRT [7]. Zhang H explored the idea and method of interactive real-time rendering to achieve realistic indoor scenes [8]. Liu Y proposed the primary and secondary combined digital simulation system of distribution network relay protection [9]. Verkuyl M evaluated the ease of use and practicality of a newly developed interactive digital analog meter [10]. The above studies demonstrate the application of digital simulation and VRT in the fields of medicine and cultural preservation. However, there was a lack of research and analysis on DMA design. Therefore, this paper studied the development and practice of DMA design based on the VRT of digital simulation, which could provide a theoretical direction for the subsequent development of digital images and lays a foundation for the design of encryption schemes.

In this paper, the research on digital images in DMA design was mainly based on the VRT of digital simulation. Encryption schemes for digital images were explored from novel perspectives, thereby achieving innovation. This paper compared TDES, AES and chaos-based image encryption algorithm. The result was that the image encryption algorithm based on chaos had more advantages in real-time. The plaintext sensitivity test data of the chaos-based algorithm was very close to the expected value. The innovations of this paper are: (1) VRT is used to study DMA design. (2) The performances of TDES, AES and chaos-based image encryption algorithm are compared and analyzed.

2. DMA Image Design and Encryption

2.1 DMA design

(1) DM

DMA design refers to the use of digital technology by designers to create or communicate through DM [11-12]. There are three main areas of DMA design, as shown in Figure 1.

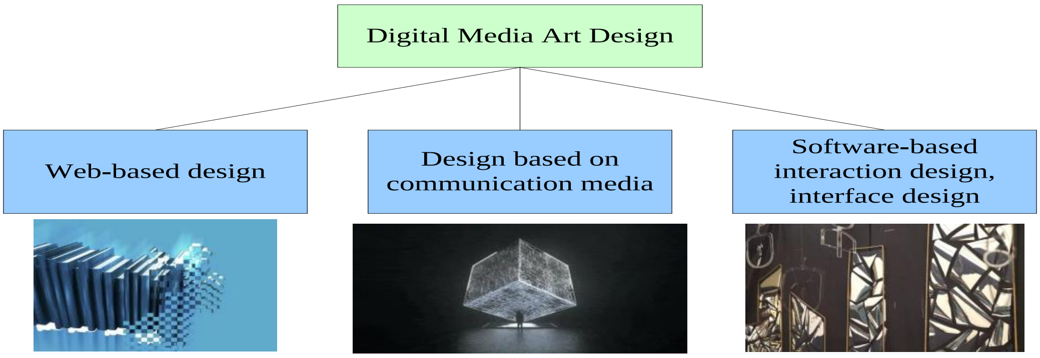

Figure 1: Classification of DMA design

(2) Blockchain technology

Blockchain is a technology based on distributed structure. It records, stores and maintains data in the form of pure digital. The rights and obligations of each node are equal, so it has the characteristics of decentralization. Once the data is successfully added to the blockchain, it cannot be changed. The retrieval and search functions provided by timestamps are combined with the chain structure to achieve traceability, and the information is difficult to tamper with. Therefore, the blockchain is traceable Information is difficult to tamper with and has high security. Relying on the open source algorithm, the blockchain has formed an open and transparent operating environment. The participation of the consensus mechanism is more helpful for building a "trust" network. Participants do not need to know the identity of each other, but only need the trust-based algorithm to reach a consensus. Therefore, the blockchain has the characteristics of transparency and de-trust.

(3) Visual presentation of information in DM

The content described by the digital image is a three-dimensional object in the real three-dimensional space, but it is recorded in a two-dimensional picture. This processing method, in terms of physical space, is dimensionality reduction processing, or planarization processing. However, due to the perception brought by human visual experience, more dimensional space can still be perceived in the image. In digital imaging techniques, such as hologram imaging and 3D models, there are virtual cameras that represent the viewer's research position in the final visual rendering output. The field of view presented by the camera is the perceptual content that needs to be received by the viewer.

2.2 VRT Based on Digital Simulation

(1) Digital simulation model

3ds Max can create concrete 3D models and generate animation sequences, which are used to generate the simulated images used in the experiments. First, a model is built from the design drawings of known objects. Based on the known position, pose and velocity of the target object, the relative position, relative velocity, and relative pose are calculated. 3D Studio MAX is used to realize the modeling part of the 3D scene. MAX Script is used to import the position and attitude information of the target. The animation trajectory in the 3D scene is calculated and the simulation video is rendered.

(2) Virtual reality (VR) technology

VR technology uses computers to bring people a virtual environment with a sense of reality, which has three characteristics of immersion, interactivity and emotion. VR technology takes high-performance PC as the main hardware. VR technology not only differentiates the system from the user environment, but also breaks the limitations of traditional thinking, enabling users to realize and interact with the imagined environment [13].

2.3 Chaos Theory and DNA Computing

(1) Chaos theory

Chaos describes a definite complex and irregular motion that is ubiquitous in nature. There is no precise definition for the non-dynamic motion of chaos. Until 1975, chaos had a simple mathematical description as follows:

If the continuous self-map $f(x)$ on the interval meets the following conditions, it can be determined that it has chaotic phenomenon.

Periodic points are not in the S domain.

Arbitrarily assuming $x_1, x_2 \in s(x_1 \neq x_2)$ (x_1, x_2 belongs to s and x_1 is not equal to x_2), then there are:

$$\liminf_{m\to\infty} \left| f^m(x) - f^m(y) \right| = 0 \tag{1}$$

$$\limsup_{m\to\infty} \left| f^m(x) - f^m(y) \right| \succ 0 \tag{2}$$

Given any periodic point $q \in I$ of $x_1 \in s$ and f, there are:

$$\limsup_{m\to\infty} \left| f^m(q) - f^m(x_1) \right| \succ 0 \tag{3}$$

Then f is said to be chaotic on s.

Typical chaotic system:

Logistic mapping: Although its structure is simple, it has very complex dynamic characteristics. It is precisely because of its simple structure and easy implementation that Logistic mapping is widely used in various researches [14]. Its mathematical definition is as follows:

$$x_{m+1} = \alpha x_m (1 - x_m) \qquad m = 1,2,3,... \tag{4}$$

Lorenz chaotic system: It is a three-dimensional chaotic system discovered in thermal convection experiments [15]. It is defined as follows:

$$\begin{cases} \dot{x} = -d(x-y) \\ \dot{y} = fx - zx - y \\ \dot{z} = xy - ez \end{cases} \tag{5}$$

Here d, e, f are system control parameters. When d=10, e=8/3, f=28 or d=16, e=4, f=40, the system is in a chaotic state.

Chen's hyperchaos: The Lorenz chaotic system is improved, and a new hyperchaotic system is obtained, which is Chen's hyperchaos. Its definition is as follows:

$$\begin{cases} \dot{x} = d(y-x) \\ \dot{y} = -xz + gx + fy - p \\ \dot{z} = xy - ez \\ \dot{p} = x + k \end{cases} \tag{6}$$

When d=36, e=3, f=28, g=-16, $k \in [-0.7, 0.7]$, the system enters a hyperchaotic state. Taking k=0.2, the Lyapunov exponent of the system can be obtained, which are $\lambda_1 = 1.55$, $\lambda_2 = 0.02$, $\lambda_3 = 0$, and $\lambda_4 = -12.5$ respectively. Obviously, two of its Lyapunov exponents are positive, which satisfies the definition of hyperchaos. Therefore, it is a hyperchaotic system.

(2) Performance evaluation index of image encryption algorithm

Blockchain technology is an advanced database mechanism that allows transparent information sharing in enterprise networks. Blockchain databases store data in blocks, while databases are linked together in a chain. The data is consistent in time, because the chain cannot be deleted or modified without network consensus. Therefore, blockchain technology can be used to create unalterable ledgers to track orders, payments, accounts and other transactions.

The chaos-based digital image encryption algorithm belongs to the symmetric cryptosystem. Thus, only one key is required for cryptographic operations. Generally speaking, the encryption process and the decryption process are inverse of each other. At present, the research of image encryption mainly improves the algorithm from the aspects of scrambling method, diffusion method, bit plane operation, key correlation and selection of chaotic system, so as to improve the efficiency and security of image encryption.

To evaluate the quality of an algorithm, it must be tested through certain indicators to measure the performance of the algorithm. For encryption algorithms, its security is the first and foremost. The second is the performance in terms of speed, that is, the real-time performance of the algorithm.

Key space: It refers to the entire set of available keys for an algorithm. If the key space is too small, it is not able to resist exhaustive attacks, which means that the security of the algorithm cannot be guaranteed. Conversely, the larger the key space, the higher the security of the algorithm and the longer the key.

Statistical properties: Histograms and chi-square tests are commonly used to perform statistical analysis on images. The histogram is easy to intuitively display the distribution relationship between the gray level of the image and its occurrence probability. It is easy to get the pixel distribution characteristics of the image by observing the histogram. In the deciphering of the image encryption system, the ciphertext is often analyzed by the histogram to find out the weaknesses of the algorithm. If the ciphertext histogram shows a flat and uniform distribution, it means that the ciphertext image is very close to a random image, and the encryption effect is good. The chi-square test is a statistical analysis of the gray level distribution of an image by means of mathematics. For an 8-bit grayscale image, the chi-square test is calculated as follows:

$$\chi^2 = \sum_{j=0}^{255} \frac{(f_j - h)^2}{h} \tag{7}$$

Here, the significance level $\alpha = 0.05$ is often selected for test analysis. $\chi^2_{0.05}(255) = 293.24783$. If the chi-square test result is less than 293.24783, it can be considered that the ciphertext has the characteristics of approximately uniform distribution.

Correlation: One of the biggest characteristics of digital images is the strong correlation between adjacent pixels. One of the purposes of encryption is to eliminate the adverse effects of strong correlation as much as possible, so that the correlation coefficient is infinitely close to 0. The formulas for calculating the correlation coefficient are as follows:

$$r_{xy} = \frac{\operatorname{cov}(a,b)}{\sqrt{D(a)}\sqrt{D(b)}} \tag{8}$$

$$\mathrm{cov}(a,b)=\frac{1}{M}\sum_{j=1}^{M}\left(x_j-E(a)\right)\left(y_j-E(b)\right) \tag{9}$$

Information Entropy: Information entropy is a measure of the uncertainty of information. The information entropy is also used to measure the distribution of gray value of the ciphertext image in the evaluation of the image encryption algorithm.

(3) DNA calculation

Image encryption system based on DNA sequence is very important for image encryption. DNA sequences have four types of nucleic acid bases, namely A (adenine), T (thymine), G (guanine), and C (cytosine). The coding rule table of DNA is shown in Table 1.

Table 1: Table of coding rules for DNA

	Rule 1	Rule 2	Rule 3	Rule 4	Rule 5	Rule 6	Rule 7	Rule 8
A	11	11	01	01	10	00	00	00
T	00	00	10	10	01	01	11	11
C	01	10	11	00	00	11	01	10
G	10	01	00	11	11	10	10	01

In DNA computing, in addition to encoding the plaintext sequence, it is also necessary to perform DNA operations on the encoded DNA sequence. Among them, commonly used operations include addition operation, subtraction operation, and XOR operation.

When encrypting an image, the R, G, and B components of the color image use different rules to encode DNA and then perform different DNA operations, thereby improving the security of the encryption algorithm.

Hamming distance between DNA

The Hamming distance is calculated as follows:

$$G(x,y)=\sum_{j=1}^{m} g\left(x_j,y_j\right) \tag{10}$$

$$g(x_1,y_1)=\begin{cases}0, x_j=y_j\\ 1, x_j\neq y_j\end{cases} \tag{11}$$

$G(x,y)$ represents the Hamming distance between sequence x and sequence y. x_1, y_1 represents a single character within the sequence x, y, respectively. The Hamming distance increases by 1 when they are not equal.

(4) TDES algorithm

Data Encryption Standard (DES) is an encryption algorithm. The plaintext and ciphertext of DES are both 64 bits, and the key is also 64 bits. The DES algorithm is a typical representative of modern cryptography and an important symmetric cryptographic algorithm. Therefore, its variant algorithm is still widely used.

TDES is a variant of the DES algorithm. Because it executes the DES algorithm three times, it is also called the triple data encryption standard.

Since TDES is a block encryption algorithm, the plaintext image data must be grouped when used for image encryption. Here, the plaintext image data is divided into 64-bit data blocks. The data block to be encrypted is encrypted by using ciphertext block chaining (CBC) mode. Figure 2and Figure 3 show the encryption and decryption processes in CBC mode, respectively.

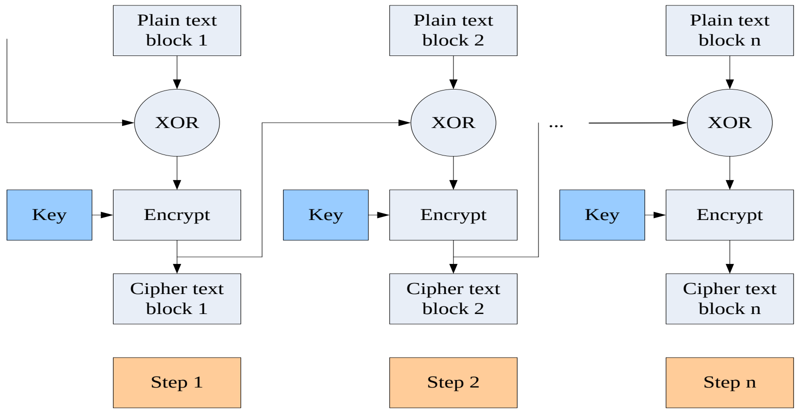

Figure 2: CBC mode encryption process

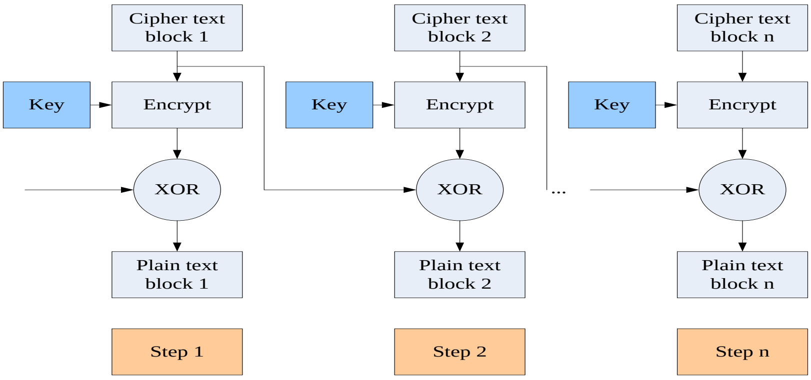

Figure 3: CBC mode decryption process

(5) AES algorithm

The AES algorithm is selected from the family of block cipher algorithms, including AES-128, AES-192 and AES-256. Different key lengths mean different encryption rounds, which of course also means higher security.

AES is similar to TDES. It is just that the length of the plaintext input by AES is 128 bits, that is, the processing of the plaintext image is to divide it into 128-bit plaintext data blocks. Similarly, the commonly used CBC mode is also used for encryption processing.

3. Comparative Experiment of DMA Design Image Encryption Algorithm

Blockchain technology is regarded as the most subversive technological innovation since the invention of the Internet. It relies on the clever distributed algorithm of cryptography and mathematics. On the Internet where trust relationship cannot be established, participants can reach a consensus without the intervention of any third-party center, and the reliable transmission of trust and value can be solved at a very low cost.

This paper constructs digital images based on VRT. Based on the performance tests of TDES, AES and chaos-based image encryption algorithm, the performance of the three algorithms is compared and analyzed. This paper mainly focuses on three aspects: real-time performance, information entropy and sensitivity of the algorithm. The performance test data of the three algorithms are shown in Figures 4, 5, and 6.

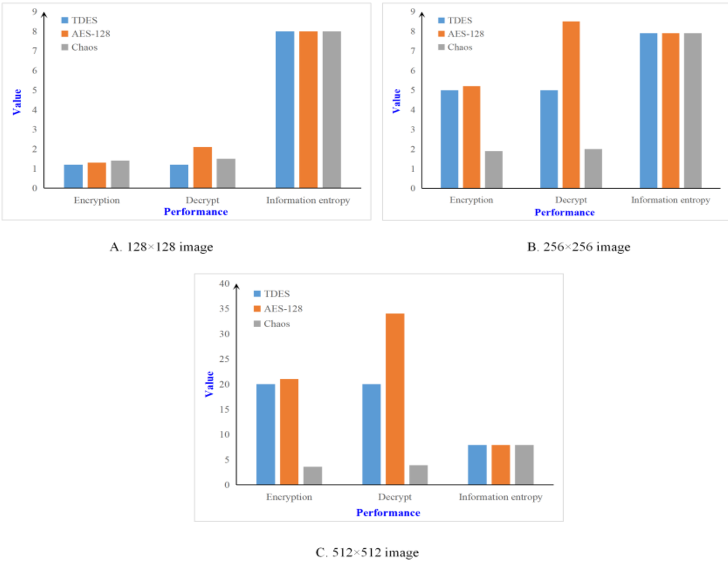

Figure 4: Comparison of real-time performance and information entropy of different algorithms

Figure 4A is a comparison diagram of algorithm real-time performance and information entropy under 128×128 images. Figure 4B is a comparison diagram of the real-time performance and information entropy of the algorithm under the 256×256 image. Figure 4C is a comparison diagram of the real-time performance and information entropy of the algorithm under the 512×512 image. It can be found from Figure 4 that under the 512×512 image, the encryption time and decryption time of the chaos-based image encryption algorithm are much lower than the other two algorithms, which are 3.6s and 3.9s respectively. The chaos-based image encryption algorithm has more advantages in real-time performance. The real-time performance of TDES image encryption system is greatly affected by the amount of encrypted data, and the real-time performance is poor. The real-time performance of AES image encryption system is slightly better than TDES image encryption system. However, compared with the chaos-based image encryption algorithm, the real-time performance is poor. In terms of information entropy, the performance of the three algorithms is almost the same, and there is no significant difference.

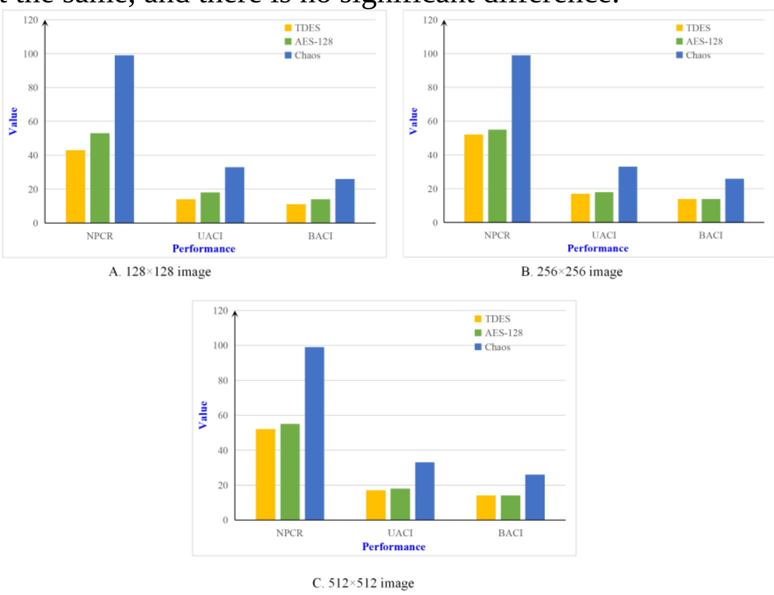

Figure 5: Comparison of plaintext sensitivity of different algorithms

Figure 5A is a comparison diagram of plaintext sensitivity of different algorithms under a 128×128 image. Figure 5B is a comparison diagram of plaintext sensitivity of different algorithms under a 256×256 image. Figure 5C is a comparison chart of plaintext sensitivity of different algorithms under a 512×512 image. It can be seen from Figure 5 that TDES and AES image encryption systems perform poorly in terms of plaintext sensitivity. It shows that the slight change of the plaintext image cannot make the encrypted ciphertext image change significantly. The algorithm lacks in resisting chosen-plaintext attack or known-plaintext attack, and the security is weak. However, the plaintext sensitivity test data of the chaos-based algorithm are very close to the expected value.

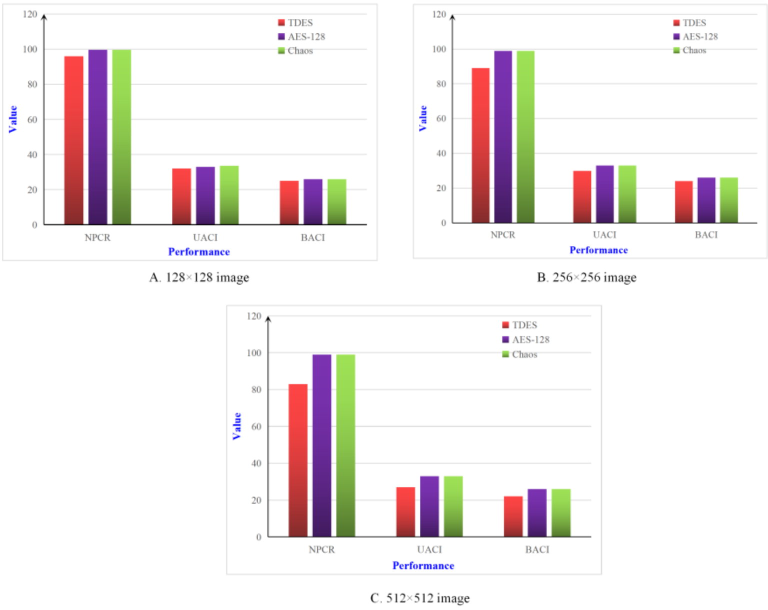

Figure 6: Comparison of key sensitivity of different algorithms

Figure 6A is a comparison diagram of key sensitivity of different algorithms under a 128×128 image. Figure 6B is a comparison chart of the key sensitivity of different algorithms under a 256×256 image. Figure 6C is a comparison chart of key sensitivity of different algorithms under a 512×512 image. From Figure 6, it can be seen that in terms of key sensitivity, the performance of TDES and AES image encryption systems is significantly stronger than its performance in terms of plaintext sensitivity. However, the test results of the encryption system of the TDES system are still far from the expected value. The test results of the AES image encryption system and the algorithm based on chaos are relatively close to the expected value. It shows that the AES image encryption system and the proposed algorithm have good key sensitivity. It has better performance against chosen ciphertext attack or known ciphertext attack.

In short, through data comparison, it can be found that the problems existing in traditional encryption algorithms TDES and AES in image encryption are mainly due to poor real-time performance. Especially when encrypting large-sized image data, the performance is poor. At the same time, the algorithm has some defects in sensitivity, which leads to the low reliability of image encryption. Of course, due to the short key of the TDES algorithm, its security is also difficult to guarantee. The chaos-based image encryption algorithm has certain advantages over TDES and AES image encryption system in real-time and sensitivity. It also has good performance in terms of correlation and information entropy. It shows that the algorithm based on chaos is very suitable for image data encryption and has a wide application prospect.

4. Conclusions

This paper studied the development and practice of DMA design based on VRT based on digital simulation. It has provided more scientific and efficient algorithms for digital image encryption. This paper used VRT to construct digital images. Then, the performance of TDES, AES and chaos-based image encryption algorithm was compared. The result was that the image encryption algorithm based on chaos had better performance. This paper used the VRT of digital simulation to find algorithms that help digital image encryption. It has improved the security of digital images, which has laid the foundation for the development and practice of DMA design. However, technology is always improving, and there are still problems that cannot be overcome at present. It is hoped that the digital image encryption technology would continue to innovate and make breakthroughs in the future. With the rapid development of artificial intelligence and Internet of Things technologies, blockchain technology can be extensively and deeply combined with them. The future era of "blockchain +" will definitely change the way of human life and bring profound changes to social development.

References

[1] Moreno L. Museums and digital era: preserving art through databases[J]. Collection Building, 2019, 38(4):89-93.

[2] Li H. Mode and practice of innovation and entrepreneurship education in the major of digital media art design[J]. IPPTA: Quarterly Journal of Indian Pulp and Paper Technical Association, 2018, 30(5):219-226.

[3] Kong W. Digital media art design based on human-computer interaction technology in the background of big data [J]. Revista de la Facultad de Ingenieria, 2017, 32(14):485-489.

[4] Lucas T. From Analog to Virtual: Visual Stylizations of Humanoid Characters Across Media[J]. Journal of Visual Art and Design, 2020, 12(1):38-55.

[5] Guo S, Li X. Computer Aided Art Design and Production Based on Video Stream[J]. Computer-Aided Design and Applications, 2020, 18(S3):70-81.

[6] Maples-Keller J L, Bunnell B E, Kim S J, Rothbaum B O. The Use of Virtual Reality Technology in the Treatment of Anxiety and Other Psychiatric Disorders[J]. Harvard Review of Psychiatry, 2017, 25(3):103-113.

[7] Liang Z, Shuang R. Research on the value identification and protection of traditional village based on virtual reality technology[J]. Boletin Tecnico/Technical Bulletin, 2017, 55(4):592-600.

[8] Zhang H, Zheng H. Research on interior design based on virtual reality technology[J]. Boletin Tecnico/Technical Bulletin, 2017, 55(6):380-385.

[9] Liu Y, Zhou Y, Wang S. Research on the primary and secondary combined digital simulation system of distribution network relay protection[J]. Power System Protection and Control, 2017, 45(13):124-129.

[10] Verkuyl M, Betts L, Sivaramalingam S. Nursing Students' Perceptions Using an Interactive Digital Simulation Table: A Usability Study[J]. Simulation & Gaming, 2019, 50(2):202-213.

[11] Kim Ji, Hyun Cho, Jae Kyung. Aesthetic Keywords in Expressing Digital Narrative Using Image Media, Coexistence - Mainly Focussed on the Movie "The Walk' -[J]. Journal Of The Korean Society Design Culture, 2017, 23(3):205-215.

[12] Seyfi M, Sivgin Z M. Research On The Relationship Between The Perception Of Social Media Marketing Activities And The Fear Of COVID19[J]. The Turkish Online Journal of Design Art and Communication, 2021, 11(2):606-616.

[13] Doan S, Nalan D. Otc Medicine Marketing In Social Media: Indicative Scientific Analysis Of Pharmaton And Supradyn Advertisements[J]. The Turkish Online Journal of Design Art and Communication, 2021, 11(1):247-267.

[14] Li P. Research on Visual Art Design Method Based on Virtual Reality[J]. International Journal of Gaming and Computer-Mediated Simulations, 2021, 13(2):16-25.

[15] Wlfel M. Rethinking Text: Unleashing the Full Potential of Media to Provide a Better Reading Experience[J]. International Journal of Art Culture and Design Technologies, 2018, 7(2):1-11.