PLOS ONE

RESEARCH ARTICLE

A double encryption protection algorithm for stem cell bank privacy data based on improved AES and chaotic encryption technology

Li Wang[1☯], **Xinyi Wei**[1☯], **Yuan Zhang**[2], **Yuan Gao**[3], **Qunfeng Niu**[1☯*]

1 School of Electrical Engineering, Henan University of Technology, Zhengzhou, Asia, China, **2** School of Information Science and Engineering, Henan University of Technology, Zhengzhou, Asia, China, **3** Henan Zhengda Stem Cell Bank Technology Company Limited, Zhengzhou, Asia, China

☯ These authors contributed equally to this work.
* niuqunfeng@gmail.com

Citation: Wang L, Wei X, Zhang Y, Gao Y, Niu Q (2023) A double encryption protection algorithm for stem cell bank privacy data based on improved AES and chaotic encryption technology. PLoS ONE 18(10): e0293418. https://doi.org/10.1371/journal.pone.0293418

Editor: Omar A. Alzubi, Al-Balqa Applied University Prince Abdullah bin Ghazi Faculty of Information Technology, JORDAN

Received: April 11, 2023

Accepted: October 12, 2023

Published: October 25, 2023

Data Availability Statement: All relevant data are within the paper.

Funding: This work was supported by the Innovative Funds Plan of Henan University of Technology (No. 2022ZKCJ03) and Henan Science and Technology Research Program (No. 201300210100). The funders had no role in study design, data collection and analysis, decision to publish, or preparation of the manuscript.

Abstract

The unique infinite self-renewal ability and multidirectional differentiation potential of stem cells provide a strong support for the clinical treatment. In light of the growing demands for stem cell storage, how to ensure personal privacy security and comply with strict ethical supervision requirements is particularly important. In order to solve the problem of low security of traditional encryption algorithm, we proposed a double encryption protection (DEP) algorithm for stem cell bank privacy data based on improved AES and chaotic encryption technology. Firstly, we presented the hash value key decomposition algorithm, through the hash value dynamic coding, cyclic shift, conversion calculation to get the key of each subsystem in the built algorithm. Secondly, DEP algorithm for privacy data is realized with two level of encryption. The first level of encryption protection algorithm used AES as the main framework, adding dynamic coding and byte filling based on DNA coding, and carries out dynamic shift of rows and simplified mixing of columns. The second level of encryption protection algorithm conducted random encoding, operation, diffusion and decoding based on the results of our proposed sequence conversion algorithm. Finally, we raised two evaluation indexes, the number of characters change rate (NCCR) and the unified average change intensity of text (UACIT) to measure the sensitivity of encryption algorithms to changes in plain information. The experimental results of using DEP shown that the average values of histogram variance, information entropy, NCCR and UACIT are116.7883, 7.6688, 32.52% and 99.67%, respectively. DEP algorithm has a large key space, high key sensitivity, and enables dynamic encryption of private data in stem cell bank. The encryption scheme provided in this study ensures the security of the private information of stem cell bank in private cloud environment, and also provides a new method for the encryption of similar high confidentiality data.

Competing interests: The authors have declared that no competing interests exist.

1. Introduction

Regenerative medicine has become a hot spot and frontier in the field of life science, providing new solutions for the treatment of many diseases [1, 2]. The stem cells, as the foundation of regenerative medicine, have great potential to improve human health. As an important resource of biomaterials for basic and translational stem cell research, stem cell banks have been rapidly expanding around the world [3]. According to a data from Coherent Market Insights, the global cell cryopreservation market will be worth $8.659 billion by 2022, and the CAGR is expected to reach 22.4% in 2022 to 2030 [4]. China has also established about 100 stem cell banks [5]. The stem cell bank is not only a repository of cells, but also a huge database that contains unique marks and records for the collection, processing, storage, transportation and management of each stem cell sample. In an era when open, shared, and affordable gene detection technologies are increasingly commonplace, the use of human biomaterials for cell research and intervention have raised ongoing concerns about protecting gene privacy [6]. All the data in the stem cell bank are personal privacy information, which have hidden dangers such as data leakage, tampering and counterfeiting in information sharing [7, 8]. If the information is obtained by attackers, it will cause great security risks [9]. In an effort to better achieve the interconnection between the private data of stem cell samples storage, handling, and other links in the private cloud environment and the blockchain platform. It is extremely important to ensure the security of the private data of stem cell bank through various encryption methods and comply with strict ethical regulatory requirements.

In the current research surrounding stem cell bank related fields, the human pluripotent stem cell registry (hPSCreg) has established a freely accessible cell line database to facilitate data sharing of cell characteristics with other platforms and cell banks around the world [10]. In [11], the unified management plan of the transplant registry unified management program (TRUMP) was developed in the purpose of promoting the unification and computerization of the hematopoietic stem cell transplantation registry, in view of the inconvenient query of the traditional paper registry. In [12], the authors established a basic data set of stem cell lines consisting of 33 data fields to improve the quality of cell line data and its availability in translational studies, in response to the unsatisfactory capture of specific cell line data. In [13], the integrated collection of stem cell bank data (ICSCB) is displayed to solve the problem of lack of standardized format of stem cell line data. It helps users to collect cell line information for multiple diseases and provider the latest and accurate cell line information. However, these studies around cells have focused on collecting cell data and establishing a standard cell line data format. With the rapid growth of the number of stem cell banks, more and more private data is stored in the information system. It is an extremely important link to study the encryption of private data in the information system of stem cell bank, which ensure the secure storage and transmission of private data. At present, there is no detailed explanation about how to store private information safely in the research of stem cell bank information system, especially less research on the encryption method of private data of stem cell bank.

Encryption algorithms based on the type of key used can be divided into symmetric and asymmetric encryption algorithm [14, 15]. The commonly used symmetric encryption methods include DES and AES [16, 17]. Compared with the asymmetric encryption system represented by RSA [18], the symmetric encryption system is simple and efficient [19]. DES algorithm cannot resist computer brute force cracking because the key length is only 56 bits [20]. AES encryption can choose key length according to the required level of encryption strength [21]. The AES algorithm is known for its high security and ease of implementation, and it has become the most widely used encryption algorithm in many security applications [22, 23]. In [24], a unified algorithm based on AES is proposed, which improves the shift rows

and key expansion modules of AES algorithm, and adds a flip module. It provides the same encryption strength as AES while saving hardware resources. In [25], an enhanced AES algorithm is raised to improve the avalanche effect by modifying the substitution bytes and shift rows processes in the AES algorithm. In [26], a dynamic AES cryptosystem based on memristive neural network is projected, which realizes the dynamic encryption of 'one-time-one-secret' and provides a larger key space. Although these encryption algorithms can ensure the security of plaintext information to a certain extent, they are greatly affected by the length of plaintext information and cannot meet the requirements of high confidentiality and tight ethical supervision in the storage and transmission of privacy data in stem cell bank.

Adleman proposed the method of DNA calculation for the first time, showing the advantages of high parallelism, fast computing speed and low energy consumption in the process of DNA calculation [27]. In [28], a symmetric key cryptosystem was designed by applying modern DNA biotechnology microarrays to cryptography. Both encryption and decryption keys are formed by DNA probes. The security of this algorithm depends on biological difficulties, so it is not affected by the changes of quantum computer attacks. In [29], a fast three-level DNA cryptography technique is displayed, which converts ciphertext information into DNA sequences by key shifting, complementary codes and twice DNA encoding with high encryption efficiency. In [30], the authors presented a data hiding method based on DNA coding. The addition operation is performed on the DNA sequence of the plaintext and the key, and the data is hidden by the cyclic movement of the entire sequence. The algorithm is better able to withstand violent attacks. In [31], based on attack prevention of DES and DNA computation encryption algorithm is put forward, using 128 nucleotides key replace 64 keys in DES algorithm, improves the ability of resisting violent attacks. In [32], a Telugu encryption method based on genetic DNA algorithm is proposed, which follows the genetic process to encrypt English text into Telugu characters, and has a good avalanche effect. In [33], the authors showed an asymmetric DNA encryption and decryption technique for the Arabic plaintext. The authors utilized a mixture of RSA, dynamic encoding and DNA computing techniques to encrypt messages with good randomness. Although DNA computing can reduce the time complexity of encryption systems, these algorithms have problems such as fixed DNA coding schemes and operating rules, high dependence on biology, and strict requirements on plaintext or ciphertext language types.

The characteristics of chaotic system, such as extreme sensitivity of initial value, and unpredictability of chaotic sequence [34], are consistent with many requirements of cryptography, so it is widely used in various encryption systems. In [35], the author came up with an improved One-Time-Pad (OTP) cipher algorithm, which uses random sequence generated by chaotic systems as the key to modularly encrypt each bit or character of the text. It reduces the difficulty of key generation of OTP and improves the randomness of key. In [36], the author introduced a method of text encryption for chaos theory and DNA computing. By means of hyperchaotic mapping, the plaintext is encrypted in two stages, namely bit-level permutation process and hyperchaotic sequence DNA coding replacement, which improves the robustness and has a large key space. In [37], an encryption method based on logistic map and three-dimensional matrix is displayed. The algorithm uses the shuffle of the three-dimensional matrix to change the position of the plaintext characters, and extends the small changes in a symbol to the entire ciphertext space through the diffusion mechanism, which improves the complexity of the ciphertext and the ability to resist violent attacks. In [38], the authors mentioned a new block cipher algorithm based on chaos. The new chaotic method based on multiplicative inverse function is used to control the diffusion of block cipher by chaotic system, which enhances the performance of logistic map and has strong key sensitivity. In [39], authors revealed a text encryption method using image encryption algorithm. This method converts

text to image information, and uses the existing image encryption algorithm to encrypt, providing a new train of thought. Although the characteristics of chaotic system are reflected in the above algorithms, these algorithms are greatly influenced by the length of plaintext information as well as the high requirement of key randomness.

These encryption algorithms are rarely used in the medical field, and even less studied in stem cell bank. In order to address the issue of data leakage during the storage and transmission of private information in stem cell bank, this article proposed the double encryption protection (DEP) algorithm that based on improved AES and chaotic encryption technology. This algorithm ensures the security of privacy information storage and transmission, effectively safeguarding the confidentiality of the private data.

The main contributions of this study are as follows:

1. The key of each subsystem in the double encryption protection (DEP) algorithm is obtained by the proposed hash value key decomposition algorithm, which implements ´´´one-time-one-secret", improves the key sensitivity and extends the key space. The presented two levels encryption protection algorithm enables dynamic encryption of flexible length messages and enhances the uncertainty and unpredictability of encrypted information.
2. The evaluation indexes of text encryption algorithms against differential attacks are displayed, namely the number of characters change rate (NCCR) and the uniform average changing intensity of text (UACIT), which can be applied to estimate the high sensitivity and security effectiveness of encryption algorithms for plain information.

The rest of this paper is organized as follows: Section 2 introduces the relevant theoretical basis. Section 3 describes a double encryption protection algorithm. Section 4 presents the simulation experiment and security analysis of the algorithm. Finally, Section 5 summarizes the paper.

2. Related works

2.1 Mapping between DNA and binary

The DNA molecule consists mainly of four types of nucleotides, which are A(adenine), G(guanine), C(cytosine), T(thymine), wherein A and T, G and C are complementary pairs [40]. Data in the computer is stored in binary form. In binary coding, 0 and 1 are complementary, 00 and 11 are complementary, and 01 and 10 are complementary [41]. The number of binary codes and bases are all four, and it can be assumed that the binary codes 00, 01, 10, 11 and bases A, T, C, and G satisfy a one-to-one mapping relationship. According to the coding rules, there are 4! = 24 coding schemes, but only 4×2 = 8 coding schemes that can satisfy the principle of base complementary pairing, and these 8 coding schemes are shown in Table 1. Assuming the binary representations for bases A, T, C, and G are 00, 10, 11, and 01, respectively. In this case, base A (00) is not complementary to base T (10) in binary, and base C (11) is not complementary to base G (01) in binary. Therefore, that coding scheme is not among the eight coding schemes proposed in Table 1.

Table 1. DNA coding scheme.

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

https://doi.org/10.1371/journal.pone.0293418.t001

Table 2. DNA decoding scheme.

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

https://doi.org/10.1371/journal.pone.0293418.t002

As can be seen from Table 1, there is a one-to-one correspondence between binary sequence and base in each encoding scheme, that is, there are 8 encoding ways of binary sequence to base. Therefore, there are 8 decoding modes from base to binary sequence, which are shown in Table 2.

2.2 DNA operation

In our proposed algorithm, a total of four DNA operation rule are used. The results of DNA-ADD (+), DNA-SUB(-), DNA-XOR(⊕), and DNA-XNOR(⊙) operations with different coding schemes are also different. The results of DNA-ADD, DNA-SUB, DNA-XOR and DNA-XNOR operations using coding scheme 1 are shown in Tables 3–6.

2.3 Chaotic systems

2.3.1 Logistic map. Logistic map is a typical one-dimensional chaotic map and one of the simplest and most studied nonlinear systems [42], which can be expressed as Eq (1):

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

In Eq (1), μ is the parameter of the system. The bifurcation diagram illustrated in Fig 1 demonstrates the impact of varying the parameter μ in the logical mapping equation on the system's behavior. The horizontal axis represents the values of parameter μ, while the vertical axis represents the values of the system state x. Within the range of (3.5699,4], the system's state values exhibit chaotic behavior [43, 44], whereas in the remaining range, the system's state values display periodic behavior. In our proposed algorithm, the initial value of logistic map is obtained by the hash value key decomposition, and the generated chaotic sequence will be used in the second level of encryption protection algorithm of privacy data of stem cell bank.

Table 3. DNA-ADD operation results.

+	A	T	C	G
A	A	T	C	G
T	T	G	A	C
C	C	A	G	T
G	G	C	T	A

https://doi.org/10.1371/journal.pone.0293418.t003

Table 4. DNA-SUB operation results.

-	A	T	C	G
A	A	C	T	G
T	T	A	G	C
C	C	G	A	T
G	G	T	C	A

https://doi.org/10.1371/journal.pone.0293418.t004

Table 5. DNA-XOR operation results.

⊕	A	T	C	G
A	A	T	C	G
T	T	A	G	C
C	C	G	A	T
G	G	C	T	A

https://doi.org/10.1371/journal.pone.0293418.t005

2.3.2 Chen's hyper-chaotic system. Chen's hyper-chaotic system is widely used in encryption technology because of its unique high complexity and large key space [45]. Chen's hyper-chaotic system can be expressed as Eq (2):

$$\begin{cases} \dot{x} = a(y - x) \\ \dot{y} = -xz + dx + cy - h \\ \dot{z} = xy - bz \\ \dot{h} = x + k \end{cases} \tag{2}$$

In Eq (2), $\dot{x}, \dot{y}, \dot{z}, \dot{h}$ are the differential states, and a, b, c, d, k are the system parameters. When a = 36, b = 3,c = 28, d = 16 and $-0.7 \leq k \leq 0.7$, Chen's hyper-chaotic system is in hyper-chaotic state and can generate four chaotic sequences [46–48]. The chaotic attractor map, as depicted in Fig 2 provides valuable insights into the system's dynamic behavior. Fig 2(A)–2(C) represents the attractors of the Chen hyper-chaotic system plotted in the x-y, x-z, and y-z planes, respectively. In these plots, the x-axis represents the first state variable of the system, while the y-axis represents the second state variable. By observing the shape and structure of the attractor, we find that Chen's system exhibits good chaotic characteristics. Moreover, the properties of both the attractor and the resulting chaotic sequence are sensitive to changes in parameter values. Four initial values of Chen's hyper-chaotic system are obtained by the hash value key decomposition, and the four chaotic sequences will be used in the second level of encryption protection algorithm of privacy data of stem cell bank.

3.The proposed algorithm

The double encryption protection (DEP) algorithm is proposed based on improved AES and chaotic encryption technology for stem cell bank privacy data. Its structure is shown in Fig 3.

It can be seen from Fig 3 that the DEP algorithm is divided into three modules: key generation, the first level of encryption protection algorithm, and the second level of encryption protection algorithm. The stem cell bank privacy data encryption steps are as follows:

Step 1: The hash value of the plain information is calculated, and the key W1-W4 is obtained by hash value key decomposition, where the key W1 also requires key expansion.

Table 6. DNA-XNOR operation results.

⊙	A	T	C	G
A	T	A	G	C
T	A	T	C	G
C	G	C	T	A
G	C	G	A	T

https://doi.org/10.1371/journal.pone.0293418.t006

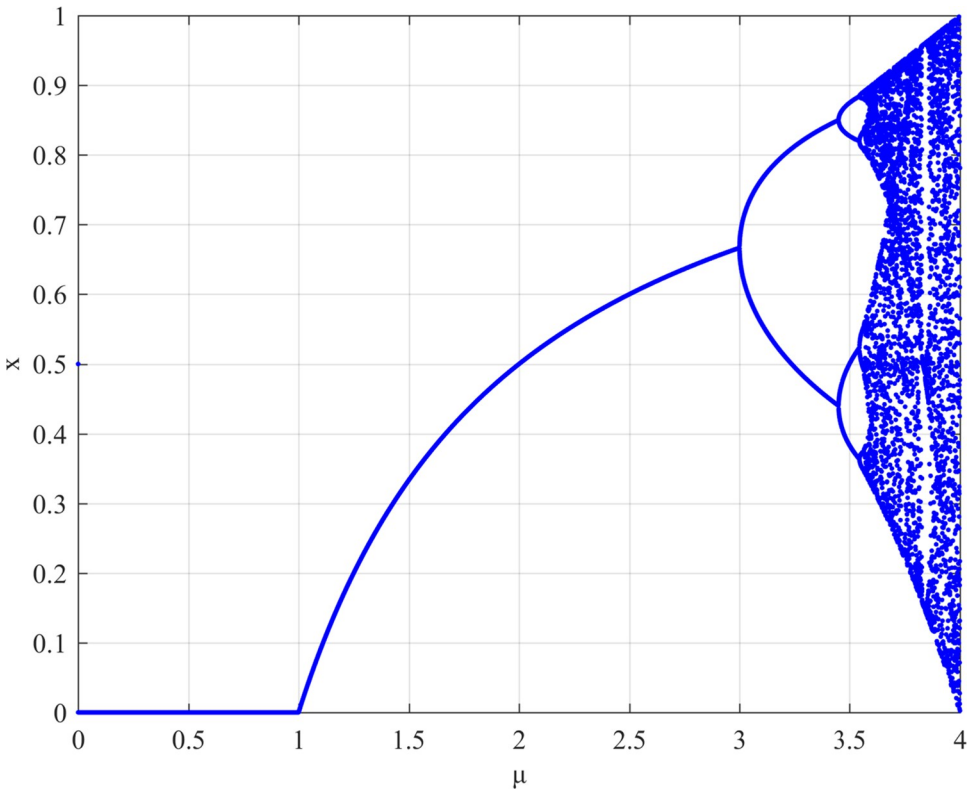

Fig 1. The bifurcation diagram of logistic map.

https://doi.org/10.1371/journal.pone.0293418.g001

Step 2: The plain information and the key W1 and W2 are used as input to participate in the first level of encryption protection operation.

Step 3: The results of step 2, the key W3 and the random logistic information generated according to the key W4 are used as input to participate in the second level of encryption protection operation to obtain cipher information.

The following subsections describe the above steps in detail.

3.1 Key generation

The hash function SHA-256 [49] can convert information of different lengths into a 64-bit hexadecimal data. After inputting the plaintext information, the hash function generates a 64-bit data called W0 based on the content of the plaintext information. W0 is used as input to perform hash value key decomposition to obtain the key from W1 to W4. Fig 4 shows an example of the hash value key decomposition process.

As indicated in Fig 4, splitting W0 into varying lengths results in Key1, Key2, Key3, and Key4. After performing dynamic DNA coding on Key1, the key matrix W1 of the round key addition process of the first level of encryption protection algorithm is obtained. After dynamic DNA coding of every two bit of hexadecimal data in Key2, four DNA sequences s1-s4 are acquired. The left fixed matrix W2 of the mix columns process of the first level of encryption protection algorithm is gained by the cyclic shift of these four DNA sequences. After Key3 through the conversion calculation 1 from hexadecimal to decimal data, Chen's hyper-chaotic system initial value W3 is acquired, in which W3 includes four data, x0, y0, z0 and h0. The

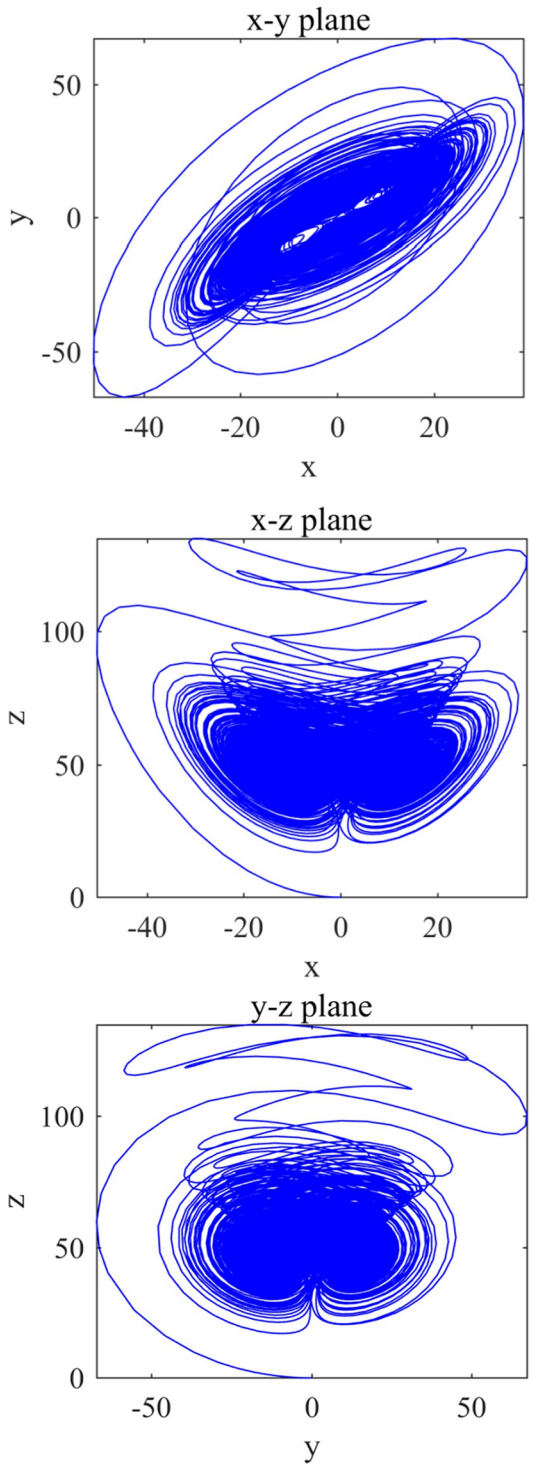

Fig 2. Attractors of Chen's hyper-chaotic system (a) x-y plane (b) x-z plane (c) y-z plane.

https://doi.org/10.1371/journal.pone.0293418.g002

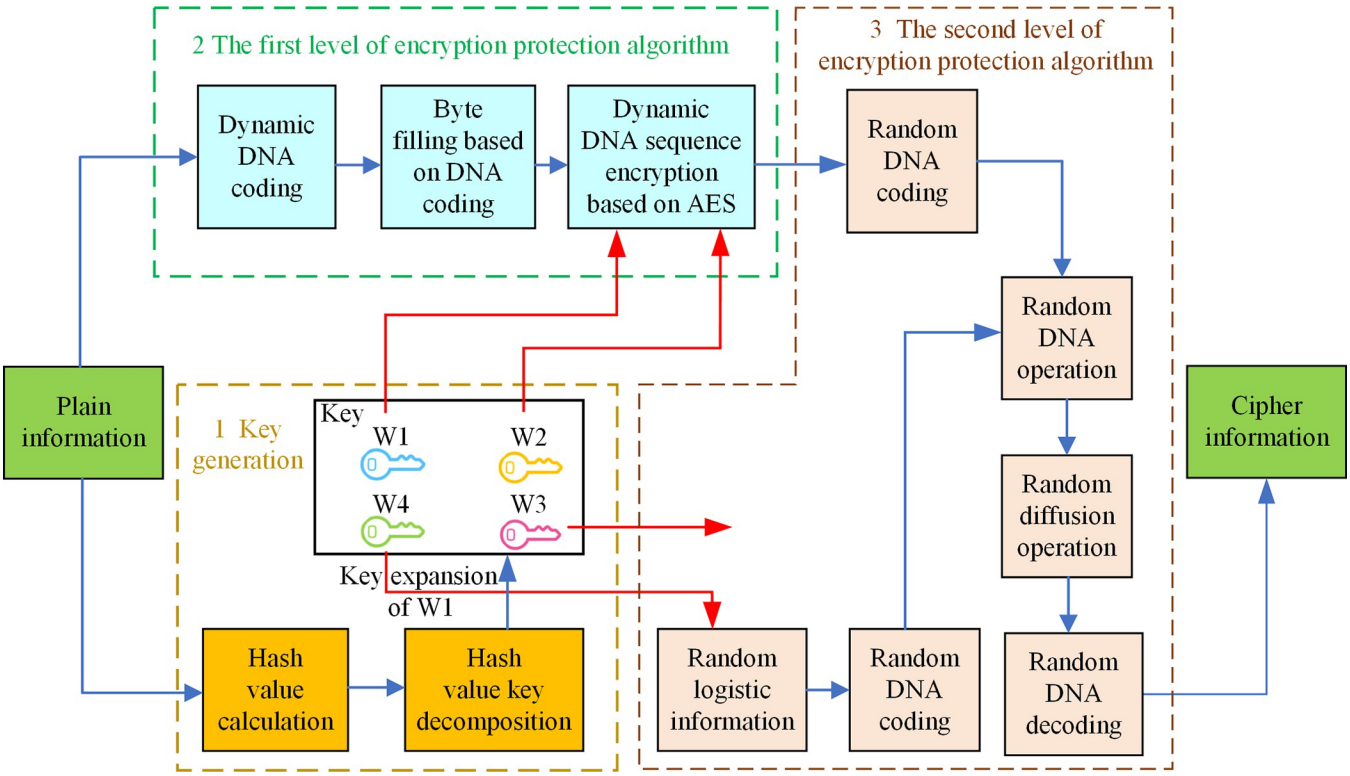

Fig 3. The structure of DEP algorithm.

https://doi.org/10.1371/journal.pone.0293418.g003

initial value W4 of the logistic map is attained by using Key4 to proceed conversion calculation 2. The hash value key decomposition algorithm is shown in Algorithm 1:

```
Algorithm 1 Hash value key decomposition
Input: W0
Step1: Key splitting
Key1 = Split(W0(1:32)); // Split is a partition function.
Key2 = Split(W0(33:40));
Key3 = Split(W0(41:56));
Key4 = Split(W0(57:64));
Step2: Dynamic DNA coding
W1 = Code(Key1,A); // Code is an coding function. A is the coding
scheme
used, ranging from 1 to 8.
Step3: Dynamic DNA coding and cyclic shift
s1 = Code(Split(Key2(1:2)),A);
s2 = Code(Split(Key2(3:4)),A);
s3 = Code(Split(Key2(5:6)),A);
s4 = Code(Split(Key2(7:8)),A);
W2(1,:) = [s1,s2,s3,s4]; // The first row of W2 is arranged in the
order of s1-s4.
W2(2,:) = [s2,s3,s4,s1];
W2(3,:) = [s3,s4,s1,s2];
W2(4,:) = [s4,s1,s2,s3];
Step4: Conversion calculation1
xt = hex2dec(Split(Key3(1:4))); //hex2dec is a conversion function
from
```

```
hexadecimal to decimal.
x0 = mod(xt,10000)×10^-4; //mod is the remainder function.
yt = hex2dec(Split(Key3(5:8)));
y0 = mod(yt,10000)×10^-4;
zt = hex2dec(Split(Key3(9:12)));
z0 = mod(zt,10000)×10^-4;
ht = hex2dec(Split(Key3(13:16)));
h0 = mod(ht,10000)×10^-4; // W3 contains x0, y0, z0, h0.
Step5: Conversion calculation2
t1 = hex2dec(Split(Key4(1:4)));
t2 = hex2dec(Split(Key4(5:8)));
W4 = mod(sum(t1+t2),10000)×10^-5; // sum is an accumulation function.
Output: W1, W2, W3, W4
```

According to the hash value key decomposition algorithm, the hash value W0 of the plain information will be divided into 4 parts. Key1 is the 1 to 32 bits of W0, Key2 is the 33 to 40 bits of W0, Key3 is the 44 to 56 bits of W0, and Key4 is the 57 to 64 bits of W0. Key1 selects a coding method from eight coding schemes and proceeds to dynamic DNA coding to obtain the key W1. Key2 also selects one of the eight coding schemes for dynamic DNA coding and performs circular left shift to get the key W2. Every four bits of data in Key3 is treated as a group,

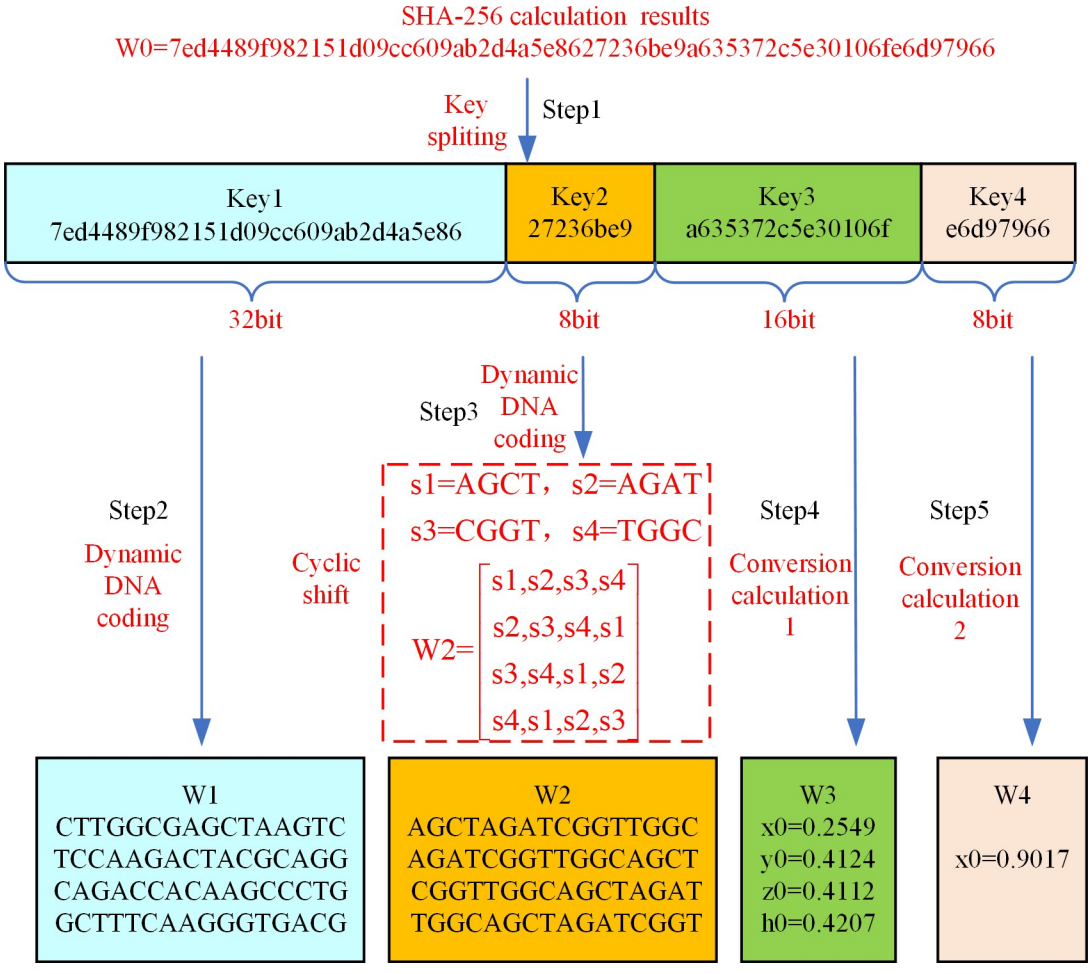

Fig 4. The process of hash value key decomposition.

https://doi.org/10.1371/journal.pone.0293418.g004

which carries out the hexadecimal to decimal conversion and the remainder operation. The resulting x0, y0, z0 and h0 are the key W3. Every four bits of data in Key4 is converted from hexadecimal to decimal as a group. The key obtained by accumulating and taking the remainder of the decimal data is W4.

Based on the key generation steps described in Fig 3, it is evident that the 4x16 matrix W1 shown in Fig 4 requires key expansion. This expansion is necessary to meet the requirements of the round key addition process in the DEP algorithm. The key expansion algorithm for W1 is shown in Algorithm 2.

```
Algorithm 2 Key expansion
Input: W1(size:4×16)
W1 = [W1[1] W1[2] W1[3] W1[4]]
for i = 5:1:44
if (i-1) mod 4 = = 0
W1[i] = W1[i-4]⊕T(W1[i-1]);
else
W1[i] = W1[i-4]⊕ W1[i-1];
end
end
Output: W1(size:4×176)
```

According to Algorithm 2, W1 is a matrix with 4 rows and 16 columns at the beginning, and each 4 columns of DNA sequence in W1 can be divided as a group to get W1[1], W1[2], W1[3] and W1[4]. The new data generated in each expansion operation is denoted as W1[*i*]. The expansion operation starts from $i = 5$ and adds 1 each time until the end of $i = 44$. If (i-1) is a multiple of 4, we need to participate in the operation of the T-function before performing the DNA-XOR operation, otherwise we can perform the DNA-XOR operation directly. After the key expansion, W1 has a total of 44 groups of data, each group of data includes four columns of DNA sequences. Consequently, the output W1 has a total of 4 rows, 44×4 = 176 columns of data. An illustration of the key extension process is displayed in Fig 5.

It can be observed form Fig 5 that after splitting the original key W1, the data size of each block is 4×4. According to the key expansion algorithm shown in Algorithm 2, when calculating the key W1[5], $i = 5$, and i-1 = 4 is a multiple of four. Therefore, W1[5] needs to perform the T-function operation first, and then perform the XOR operation with W1[1]. The T-function operation includes three processes: cyclic shift, substitution bytes, and Round Constant DNA-XOR. The cyclic shift process moves the first row of data to the last row, with the remaining rows of data moving up one row. The data after the cyclic shift process needs to be replaced by the S-Box. The specific process of substitution S-box will be given in Section 3.2.3. Taking the data 'CAGG' as an example, it becomes 'TCCG' after being replaced by the S-box. The data replaced by the S-box requires an DNA-XOR operation with the Round Constant. At this time, the Round Constant is RC[1], and the result obtained by the completion of the T-function operation is T(W1[4]). The extended key W1[5] can be obtained by DNA-XOR operation of W1[1] and T(W1[4]). When calculating the key W1[6], $i = 6$, and i-1 = 5 is not a multiple of four. Therefore, the extended key W1[6] can be obtained by DNA-XOR operations on W1[2] and W1[5]. The Round Constant (RC) used in T-function operations is shown in Table 7.

As is shown in Table 7, we know that the data of RC[j] are different when the value of variable j is different. Furthermore, the relationship between variable j and variable i in key expansion satisfies the below Eq (3):

$$j = (i - 1)/4 \tag{3}$$

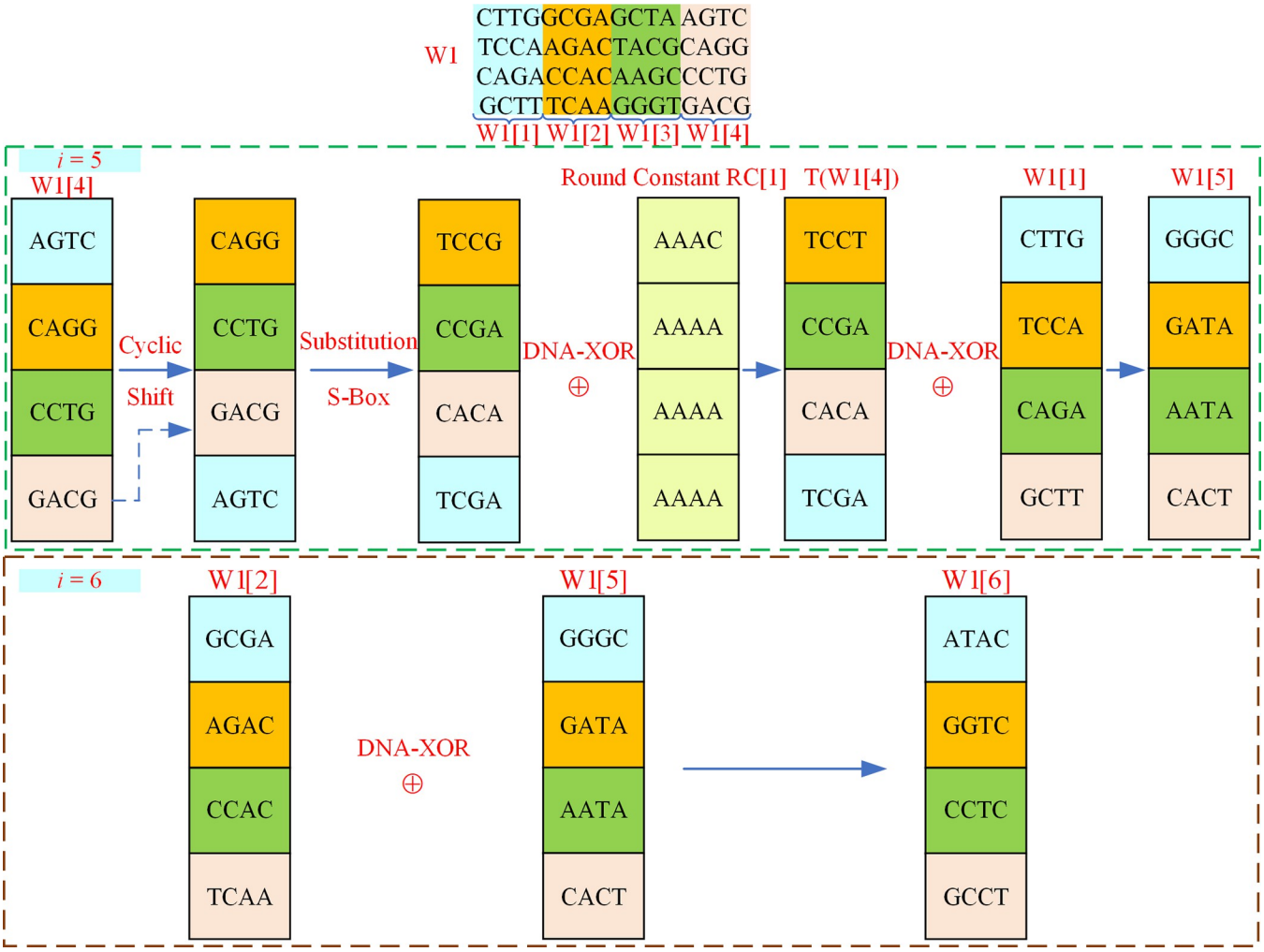

Fig 5. The process of key expansion.

https://doi.org/10.1371/journal.pone.0293418.g005

According to the value of variable *i* in T-function operation, the corresponding RC[*j*] is selected to complete the Round Constant DNA-XOR operation.

3.2 The first level of encryption protection algorithm

The first level of encryption protection algorithm includes three steps: dynamic DNA coding of plain information, byte filling based on DNA coding, and dynamic DNA sequence

Table 7. Round constant.

j	RC[*j*]	*j*	RC[*j*]	*j*	RC[*j*]	*j*	RC[*j*]	*j*	RC[*j*]
1	AAAC AAAA AAAA AAAA	2	AAAG AAAA AAAA AAAA	3	AACA AAAA AAAA AAAA	4	AAGA AAAA AAAA AAAA	5	ACAA AAAA AAAA AAAA
6	AGAA AAAA AAAA AAAA	7	CAAA AAAA AAAA AAAA	8	GAAA AAAA AAAA AAAA	9	ACGT AAAA AAAA AAAA	10	ATCG AAAA AAAA AAAA

https://doi.org/10.1371/journal.pone.0293418.t007

encryption based on AES. Among them, the dynamic DNA sequence encryption algorithm based on AES adopts the framework of AES encryption algorithm, contains four steps: substitution bytes, shift rows, mix columns, and add round key.

3.2.1 Dynamic DNA coding. Plain information (input) is the private data of stem cell bank, which is one of the inputs of the first level of encryption protection algorithm. The plain information is converted to its corresponding ASCII value. Furthermore, one of the eight coding rules is randomly selected to apply dynamic DNA coding to ASCII values, and the data obtained after dynamic DNA coding is input1.

3.2.2. Byte filling based on DNA coding. The length of data input1 encoded by dynamic DNA may not be an integer multiple of 64, and cannot participate in subsequent operations. As a consequence, before participating in dynamic DNA sequence encryption based on AES, it is necessary to do byte filling at the end to ensure that the data is 64 bits. The steps of byte filling based on DNA coding are as follows:

Step 1: The input1 encoded by dynamic DNA is grouped according to the 64-bit DNA sequence, and each block corresponds to a row of data.

Step 2: If the length of the last row of data is less than 64 bits, fill in the 4-bit DNA coding with the length divided by 4 after input1, meanwhile the remain data is filled with 'A' until the length is 64 bits. If the length of the last row of data is 64 bits, fill in 'ACAA' and sixty characters 'A' after input1, totaling 64 bits of data.

After byte filling based on DNA coding, obtain the data input1.The byte filling process illustrated is shown in Fig 6.

As can be seen from Fig 6, the original data (input1) is partitioned into two rows of data. According to DNA coding rule 1, if there are only 24 bits in the last row, DNA code 'AACG' (24/4 = 6) needs to be filled in 25 to 28 bits, and character 'A' needs to be filled in 29 to 64 bits. If the last row contains exactly 64 bits of data, fill in the first four bits of the new row with 'ACAA' and the other 60 bits with character 'A'.

3.2.3. Dynamic DNA sequence encryption based on AES.

1. Substitution bytes

The DEP algorithm redesigns the S-Box and Inverse S-Box (IS-Box) of the AES algorithm to accommodate substitution bytes in the proposed algorithm. The S-Box of the proposed algorithm is shown in Fig 7, and the IS-Box is shown in Fig 8.

From the Figs 7 and 8, it can be seen that the S-box and IS-box in the DEP correspond to the input of 4-bit DNA sequences and the output of 4-bit DNA sequences. The first two digits of the DNA sequence correspond to the number of rows, and the last two digits correspond to the number of columns. Taking 'GTAC' as an example, the result after S-box operation is 'TAGA', and the result after IS-box operation is 'GTAC', which is successfully restored to the original data. Thereby proving that the IS-box is the inverse operation of S-box. The result of substitution the byte filled data (input1) with the S-box is input2.

2. Shift rows

At the beginning of the DEP shift rows, the original data (input2) after substitution bytes must be partitioned into blocks. The 16 blocks of data (input2) gained after block processing, each of block contains a 4-bit DNA sequence. The traditional AES algorithm has a fixed row shift scheme, which includes four schemes: no shift, cyclic left shift by one-bit, cyclic left shift by two-bis, and cyclic left shift by three-bit. In an effort to increase the randomness of the first level of encryption protection algorithm, the first row shift scheme of DEP algorithm selects

The last row of original data (input1) is less than 64-bit DNA sequence

AGAA	GTGG	TATT	TATC	GGTA	GTGG	TACC	ATGG	CCGG	CACA	CACT	CTAT	CTAT	CTAT	CTAT	CTAT
CTAT	ATAG	ATAT	ATGA	ATCA	ATAA										

The result of the original data (input1) after byte filling

AGAA	GTGG	TATT	TATC	GGTA	GTGG	TACC	ATGG	CCGG	CACA	CACT	CTAT	CTAT	CTAT	CTAT	CTAT
CTAT	ATAG	ATAT	ATGA	ATCA	ATAA	AACG	AAAA	AAAA	AAAA	AAAA	AAAA	AAAA	AAAA	AAAA	AAAA

The last row of original data (input1) is 64-bit DNA sequence

AGAA	GTGG	TATT	TATC	GGTA	GTGG	TACC	ATGG	CCGG	CACA	CACT	CTAT	CTAT	CTAT	CTAT	CTAT
CTAT	ATAG	ATAT	ATGA	ATCA	ATAA	TACA	GTGA	TACT	TTCT	TCAA	TCCC	TAAG	CTGA	ATCC	ATCT

The result of the original data (input1) after byte filling

AGAA	GTGG	TATT	TATC	GGTA	GTGG	TACC	ATGG	CCGG	CACA	CACT	CTAT	CTAT	CTAT	CTAT	CTAT
CTAT	ATAG	ATAT	ATGA	ATCA	ATAA	TACA	GTGA	TACT	TTCT	TCAA	TCCC	TAAG	CTGA	ATCC	ATCT
ACAA	AAAA	AAAA	AAAA	AAAA	AAAA	AACG	AAAA	AAAA	AAAA	AAAA	AAAA	AAAA	AAAA	AAAA	AAAA

Fig 6. The process of byte filling based on DNA coding.

https://doi.org/10.1371/journal.pone.0293418.g006

	AA	AC	AG	AT	CA	CC	CG	CT	GA	GC	GG	GT	TA	TC	TG	TT
AA	CGAT	CTTA	CTCT	CTGT	TTAG	CGGT	CGTT	TACC	ATAA	AAAC	CGCT	AGGT	TTTG	TCCT	GGGT	CTCG
AC	TAGG	GAAG	TAGC	CTTC	TTGG	CCGC	CACT	TTAA	GGTC	TCCA	GGAG	GGTT	GCTA	GGCA	CTAG	TAAA
AG	GTCT	TTTC	GCAT	AGCG	ATCG	ATTT	TTCT	TATA	ATCA	GGCC	TGCC	TTAC	CTAC	TCGA	ATAC	ACCC
AT	AACA	TACT	AGAT	TAAT	ACGA	GCCG	AACC	GCGG	AACT	ACAG	GAAA	TGAG	TGGT	AGCT	GTAG	CTCC
CA	AAGC	GAAT	AGTA	ACGG	ACGT	CGTG	CCGG	GGAA	CCAG	ATGT	TCCG	GTAT	AGGC	TGAT	AGTT	GACA
CC	CCAT	TCAC	AAAA	TGTC	AGAA	TTTA	GTAC	CCGT	CGGG	TAGT	GTTG	ATGC	CAGG	CATA	CCGA	TATT
CG	TCAA	TGTT	GGGG	TTGT	CAAT	CATC	ATAT	GACC	CACC	TTGC	AAAG	CTTT	CCAA	ATTA	GCTT	GGGA
CT	CCAC	GGAT	CAAA	GATT	GCAG	GCTC	ATGA	TTCC	GTTA	GTCG	TCGG	AGAC	ACAA	TTTT	TTAT	TCAG
GA	TATC	AATA	ACAT	TGTA	CCTT	GCCT	CACA	ACCT	TACA	GGCT	CTTG	ATTC	CGCA	CCTC	ACGC	CTAT
GC	CGAA	GAAC	CATT	TCTA	AGAG	AGGG	GCAA	GAGA	CACG	TGTG	GTGA	ACCA	TCTG	CCTG	AAGT	TCGT
GG	TGAA	ATAG	ATGG	AAGG	CAGC	AACG	AGCA	CCTA	TAAG	TCAT	GGTA	CGAG	GCAC	GCCC	TGCA	CTGC
GT	TGCT	TAGA	ATCT	CGTC	GATC	TCCC	CATG	GGGC	CGTA	CCCG	TTCA	TGGG	CGCC	CTGG	GGTG	AAGA
TA	GTGG	CTGA	AGCC	AGTG	ACTA	GGCG	GTCA	TACG	TGGA	TCTC	CTCA	ACTT	CAGT	GTTC	GAGT	GAGG
TC	CTAA	ATTG	GTCC	CGCG	CAGA	AAAT	TTCG	AATG	CGAC	ATCC	CCCT	GTGC	GACG	TAAC	ACTC	GCTG
TG	TGAC	TTGA	GCGA	ACAC	CGGC	TCGC	GATG	GCCA	GCGT	ACTG	GACT	TGGC	TATG	CCCC	AGGA	TCTT
TT	GATA	GGAC	GAGC	AATC	GTTT	TGCG	CAAG	CGGA	CAAC	GCGC	AGTC	AATT	GTAA	CCCA	GTGT	ACCG

Fig 7. Substitution S-Box of DEP algorithm.

https://doi.org/10.1371/journal.pone.0293418.g007

	AA	AC	AG	AT	CA	CC	CG	CT	GA	GC	GG	GT	TA	TC	TG	TT
AA	CCAG	AAGC	CGGG	TCCC	ATAA	ATCG	GGCC	ATGA	GTTT	CAAA	GGAT	GCTG	GAAC	TTAT	TCCT	TTGT
AC	CTTA	TGAT	ATGC	GAAG	GCGT	AGTT	TTTT	GACT	ATCA	GATG	CAAT	CACA	TACA	TCTG	TGGC	TAGT
AG	CCCA	CTGT	GCCA	ATAG	GGCG	TAAG	AGAT	ATTC	TGTG	CATA	GCCC	AAGT	CAAG	TTGG	TAAT	CATG
AT	AAGA	AGTG	GGAC	CGCG	AGGA	TCGC	AGCA	GTAG	CTCG	CCGT	GGAG	CAGC	CGTC	GAGT	TCAC	AGCC
CA	CTAG	TTGA	TTCG	CGCA	GACG	CGGA	GCGA	ACCG	TCCA	GGCA	CCTA	TATA	CCTC	CGCC	GTCG	GCAG
CC	CGTA	CTAA	CAGA	CCAA	TTTC	TGTC	GTGC	TCGG	CCTG	ACCC	CACG	CCCT	GGCT	GATC	GCTC	GACA
CG	GCAA	TCGA	GGGT	AAAA	GATA	GTTA	TCAT	AAGG	TTCT	TGCA	CCGA	AACC	GTGA	GTAT	CACC	AACG
CT	TCAA	AGTA	ACTG	GATT	TAGG	ATTT	AATT	AAAG	TAAC	GGTT	GTTC	AAAT	AAAC	ACAT	GAGG	CGGT
GA	ATGG	GCAC	ACAC	CAAC	CATT	CGCT	TCTA	TGGG	GCCT	TTAG	TATT	TATG	TTAA	GTCA	TGCG	CTAT
GC	GCCG	GGTA	CTCA	AGAG	TGCT	GGTC	ATCC	GACC	TGAG	TTGC	ATCT	TGGA	ACTA	CTCC	TCTT	CGTG
GG	CACT	TTAC	ACGG	CTAC	ACTC	AGGC	TACC	GAGC	CGTT	GTCT	CGAG	AATG	GGGG	ACGA	GTTG	ACGT
GT	TTTA	CCCG	ATTG	CAGT	TACG	TCAG	CTGC	AGAA	GCGG	TCGT	TAAA	TTTG	CTGA	TATC	CCGG	TTCA
TA	ACTT	TCTC	GGGA	ATAT	GAGA	AACT	TACT	ATAC	GTAC	ACAG	ACAA	CCGC	AGCT	GAAA	TGTA	CCTT
TC	CGAA	CCAC	CTTT	GGGC	ACGC	GTCC	CAGG	AATC	AGTC	TGCC	CTGG	GCTT	GCAT	TAGC	GCTA	TGTT
TG	GGAA	TGAA	ATGT	CATC	GGTG	AGGG	TTCC	GTAA	TAGA	TGGT	GTGT	ATTA	GAAT	CCAT	GCGC	CGAC
TT	ACCT	AGGT	AACA	CTTG	GTGG	CTCT	TCCG	AGCG	TGAC	CGGC	ACCA	CGAT	CCCC	AGAC	AATA	CTTC

Fig 8. Substitution IS-Box of DEP algorithm.

https://doi.org/10.1371/journal.pone.0293418.g008

one of the four schemes, the second row shift scheme selects one of the remaining three schemes, and so on. There are 4! = 24 options. The shift rows of DEP algorithm are shown in Algorithm 3, and the value of W0 is given in Fig 4 in Section 3.1.

```
Algorithm 3 Shift rows
Input: input2, W0
Block input2
input2(1,:) = Split(input2(1:16));
input2(2,:) = Split(input2(17:32));
input2(3,:) = Split(input2(33:48));
input2(4,:) = Split(input2(49:64));
Shift rows scheme selection
A = Strcat(W0(5), W0(1)) = '47' // Strcat is a string contiguous function. The
result of extracting the fifth and first elements in W0 is A1.
A1 = mod(hex2dec(A), 24)+1 = 24 // Convert hexadecimal data A to decimal data.
The range of A1 is 1 to 24.
Shift rows according to the scheme A1
input3(1,1:16) = input2(1,1:16)
input3(2,1:16) = Strcat(input2(2,5:16), input2(2,1:4));
input3(3,1:16) = Strcat(input2(3,9:16), input2(3,1:8));
input3(4,1:16) = Strcat(input2(4,13:16), input2(4,1:12));
Output: input3
```

In the light of Algorithm 3, the input of the shift rows algorithm is the original data (input2) and W0. The new hexadecimal data A extracted and combined from the 5th and 1st characters in W0 is '47', and the A1 got by converting A into decimal and performing a remainder operation with twenty-four is 24. Thus, the 24th shift rows scheme is selected, that is, the first row is not shifted, the second row is shifted 1 bit to the left, the third row is shifted 2 bits to the left, and the third row is shifted 3 bits to the left. An example of the DEP shift rows process is shown in Fig 9.

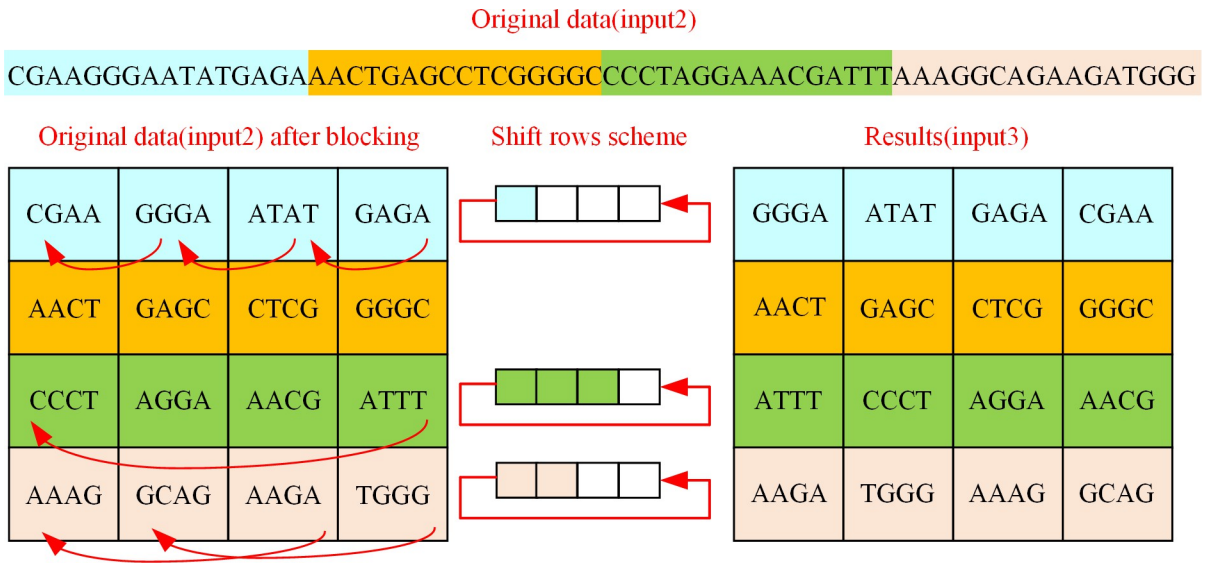

Fig 9. A kind of shift rows operation of DEP algorithm.

https://doi.org/10.1371/journal.pone.0293418.g009

As is shown in Fig 9, every 16-bit DNA sequence in the original data (input2) needs to be partitioned as a group. Among them, 1 to 16 bits of original data are used as the first row after the block, 17 to 32 bits of original data are used as the second row after the block, and so on to obtain the original data after the block (input2). At this time, the shift scheme is cyclic shift of the first row to the left by one bit, the second row without shift, the third row cyclic shift to the left by three bits, and the fourth row cyclic shift to the left by two bits. The result of the shift according to the shift rows scheme is input3.

3. Mix columns

The mix columns operation of the AES algorithm requires two types of operations: multiplication and XOR. In the cause of simplify the mix column calculation steps and improve encryption efficiency, the mix column in the DEP algorithm only requires the DNA-XOR operation. The fixed matrix on the left side during mixing columns is W2 obtained after the hash value key decomposition, and this W2 with the original data (input3) after shifting rows are used as the two inputs in the mix columns process. An explanation of the DEP algorithm for mixing columns operation is provided in Fig 10.

It is clear from Fig 10 that every 4 column of DNA data in the key W2 (size: 4×16) are chunked as a group, and a total of 16 blocks of data are acquired. The mix columns process is to conduct the DNA-XOR operation between the blocked key W2 and the original data (input3), where the value of the key W2 has been given in Fig 4 in Section 3.1. For instance, the data $P1_{2,1}$ in the mixing columns result (input4) is the result of the DNA-XOR of the base sequence 'AGAT' with position coordinates (1,2) in W2 and the data $P_{2,1}$ with position coordinates (2,1) in input3, and similarly the mix columns result (input4) of all data can be acquired.

4. Add round key

The input of adding round key in DEP algorithm are the original data (input4) received after mixing columns and the key W1, and each calculation uses 4 columns of W1 data. The add round key process described as an example is shown in Fig 11.

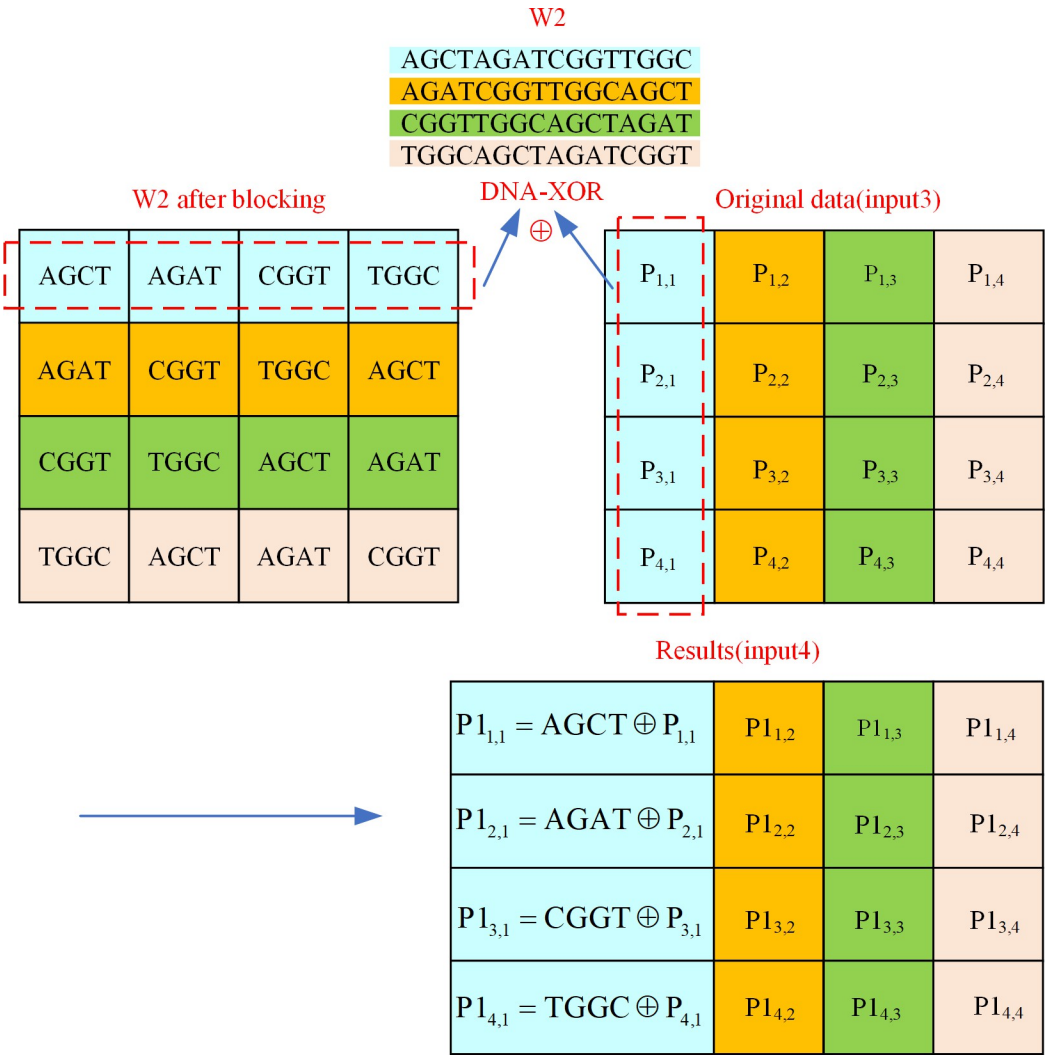

Fig 10. Mix columns operation of DEP algorithm.

https://doi.org/10.1371/journal.pone.0293418.g010

As shown in Fig 11, the data in columns 41 to 44 of key W1 are involved in this add round key operation. Consider the data $P1_{2,1}$ in the add round key result (input5) as an example, it is the result of DNA-XOR on the data $P_{2,1}$ with position coordinates (2,1) in input4 and the DNA sequence 'ACTC' with position coordinates (2,1). Accordingly, the result (input5) of the add round key of all the data is available. At this point, the first level of encryption protection algorithm ends and the resulting first level of encryption protection cipher information is input5.

3.3 The second level of encryption protection algorithm

In order to further improve the security of the privacy data of the stem cell bank, the cipher information (input5) obtained after the first level of encryption protection needs to be encrypted in the second level. The extreme sensitivity and unpredictability of initial values of chaotic systems are well suited for encryption of privacy data. However, the structure of low-dimensional chaotic graphs is relatively simple and less secure [50, 51]. In contrast, the Chen's hyper-chaotic system exhibits strong chaotic behaviour and has complex dynamic properties,

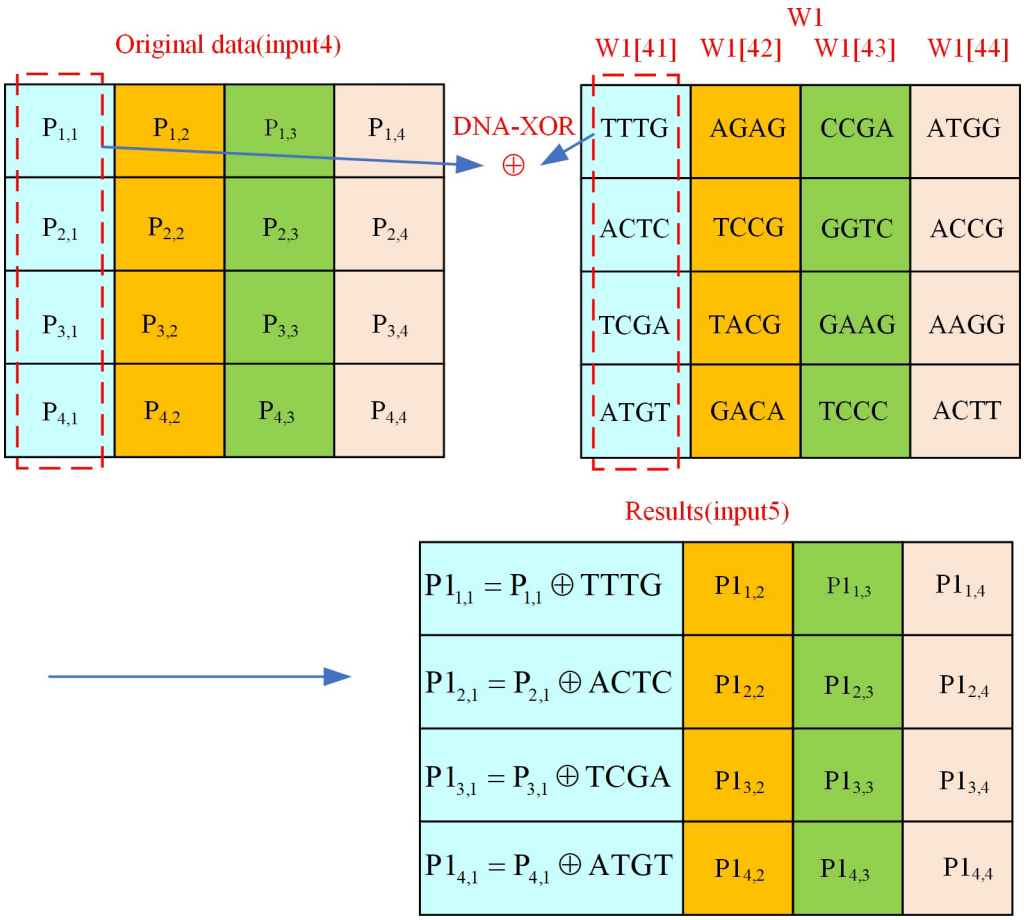

Fig 11. Add round key operation of DEP algorithm.

https://doi.org/10.1371/journal.pone.0293418.g011

which makes it a favourable choice among encryption algorithms [47, 49]. The complexity and unpredictability of Chen's hyper-chaotic system can enhance the security of the algorithm. Therefore, in the second level of the encryption protection algorithm, we use the Chen's hyper-chaotic system as the basis for encryption. The random sequence generated by the Chen's hyper-chaotic system is used to determine the exact scheme of the encoding, operation, diffusion and decoding processes of the second level of the encryption protection algorithm. This increases the security of the private data of the stem cell bank.

The key W4 generated after the hash value key decomposition is applied as the original value of the logistic mapping, and the random logistic information (input6) is generated through the logistic mapping. The algorithm for generating the random logistic information is demonstrated in Algorithm 4:

```
Algorithm 4 Random logistic information generation
Input: W4, input5
MUL = M×N; // M and N are the number of rows and columns of the input5
matrix of the first level of encryption result.
P0 = 1500;
for i = 1:1:(P0+MUL)
P(i) = Logstic(W4); // The logistic sequence P is created using Eq
(1).
```

```
end
P = Split(P(1501: end)); // Remove the first 1500 iterations of logis-
tic chaotic to
eliminate the undesirable effects.
input6 = mod(Ceil(P×10^3),256); // Ceil is an upward integer function.
The range
of input6 is 0-255.
Output: Random logistic information(input6)
```

It is known from the random logistic information generation algorithm that the logistic sequence P generated according to Eq (1) needs to discard the first 1500 terms to achieve better randomness. The ASCII range of the generated logistic sequence information (input6) is 0–255, which is the same size and ASCII range as the cipher information (input5) generated by the first level of encryption protection algorithm. The cipher information (input5), random logistic information (input6) and the key W4 generated after hash key decomposition are applied as input to the second level of encryption protection algorithm. The process of the second level of encryption protection algorithm is presented in Fig 12.

As observed from Fig 12, the second level of encryption protection algorithm needs to first create a sequence of operation modes based on the sequence conversion algorithm to confirm which operation mode is used in the subsequent encryption. The sequence conversion algorithm is shown in Algorithm 5.

```
Algorithm 5 Sequence conversion
Input: W3, input5
P1 = 1500;
R = M×N/16; // M and N are the number of rows and columns of the input5
matrix of the first level of encryption result.
for i = 1:1:(P1+R)
A(i, :) = Chen_chaotic(W3); // The Chen's hyper-chaotic sequence A is
created
using Eq (2).
end
X1 = A(:,1); // X1 is all the elements of the first column of the
matrix A.
Y1 = A(:,2);
Z1 = A(:,3);
H1 = A(:,4);
X1 = Split(X1(1501:end)); // Remove the first 1500 iterations of
hyper-chaotic to
eliminate the undesirable effects.
Y1 = Split(Y1(1501:end));
Z1 = Split(Z1(1501:end));
H1 = Split(H1(1501:end));
X = mod(Floor(X1×10^4),8); // Floor is an downward integer function.
The range
of X is 0 to 7.
Y = mod(Floor(Y1×10^4),8);
Z = mod(Floor(Z1×10^4),4);
H = mod(Floor(H1×10^4),8);
Output: Operation mode sequence (X, Y, Z, H)
```

As we can see from Algorithm5, the range of X and Y after sequence conversion is 0–7 corresponding to 8 DNA coding methods, the range of Z is 0–3 corresponding to 4 DNA operation methods, and the range of H is 0–7 corresponding to 8 DNA decoding methods.

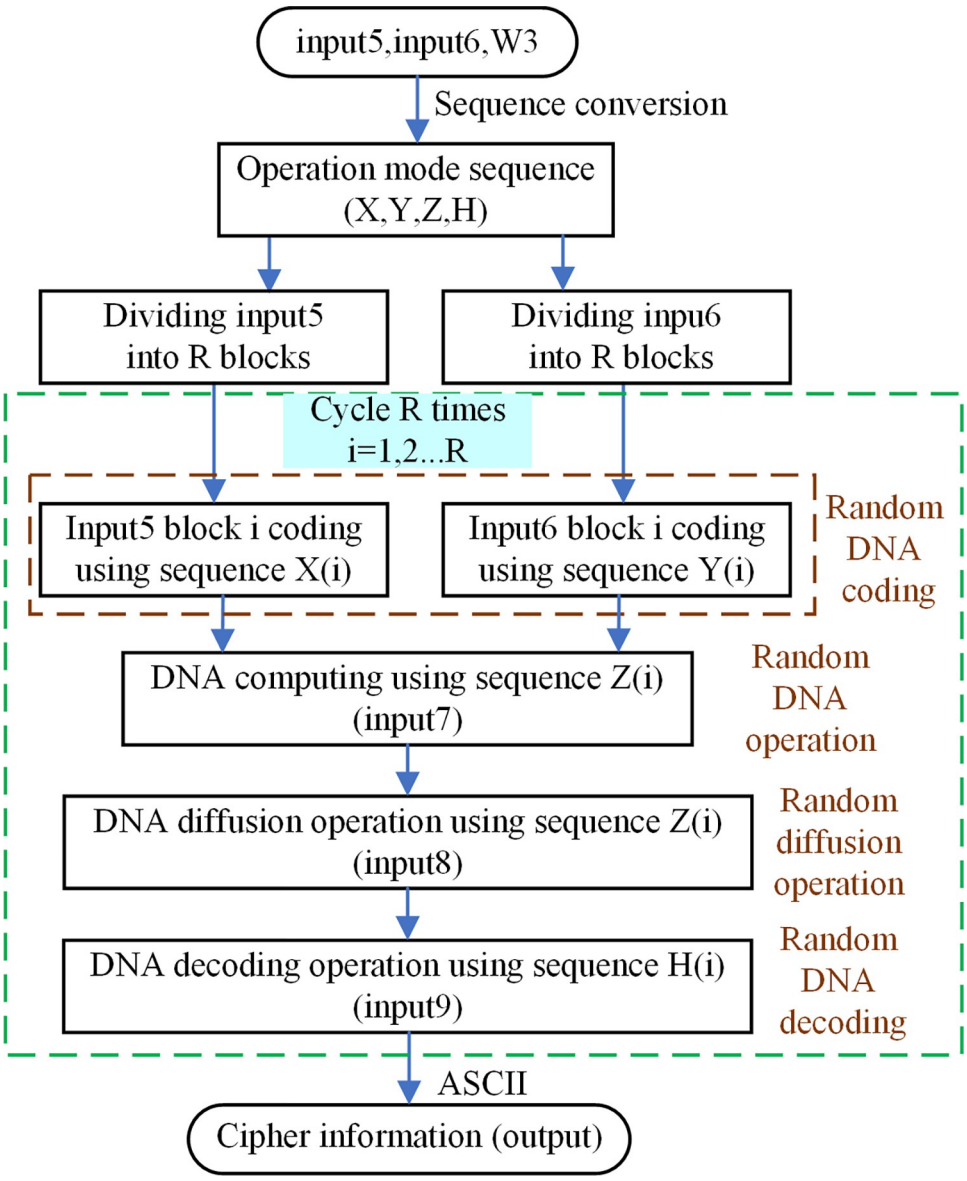

Fig 12. The second level of encryption protection algorithm of DEP.

https://doi.org/10.1371/journal.pone.0293418.g012

After sequence conversion, the cipher information (input5) generated by the first level of encryption protection algorithm and the random logistic information (input6) need to be split into blocks, both of which can be divided into *R* blocks because they are of the same size. The number of block *R* can be indicated as:

$$R = \frac{M \times N}{16} \tag{4}$$

In Eq (4), M and N refer to the number of rows and columns of input5, respectively. After splitting, input5 and input6 are scheduled for random DNA coding, random DNA operation, random diffusion and random DNA decoding, each time only for the *i-th* block of data, and a total of R cycles are necessary.

The operation mode sequence X(*i*) decide the coding method of the *i-th* block in input5, the operation mode sequence Y(*i*) determine the coding method of the *i-th* block in input6. Meanwhile, the operation mode sequence Z(*i*) dictate the operation method of the *i-th* block in input5 and the *i-th* block in input6, and the outcome is input7 after random operation. Moreover, the diffusion operation of the *i-th* segment is to diffusion operate the input7 of the *i-th* segment with the input7 of the (*i*-1)*-th* segment to get input8, where the operation mode of random diffusion is dictated by the operation mode sequence Z(*i*). The decoding mode of the *i-th* block in input8 depends on the operation mode sequence H(*i*), whose decoded value is input9. After DNA decoding, the data input9 has been converted to data in the range of [0,255], and the output of the second level of encryption protection algorithm (output) is gained by ASCII conversion of these data. At this point, the second level of encryption protection algorithm is finished, and the data (output) is the result of stem cell bank privacy data encrypted by the DEP algorithm.

4 Results and security analysis

In this section, we illustrate the security results of encryption stem cell bank privacy information using different algorithms. The privacy information is divided into three categories according to the source: the first category is the personal information of the customers who store the stem cells, the second category is the information of stem cell specimens, and the third category is the information of stem cell quality issued by the quality testing center. These three types of private information are encrypted and saved in the private cloud of the stem cell bank. The private cloud access information system for stem cell bank privacy data is displayed in Fig 13.

As can be seen from Fig 13, personal privacy information, stem cell sample privacy information as well as stem cell quality privacy information are generated by the DEP algorithm. The above information are decrypted by DEP and then the plaintext information of the corresponding privacy data can be obtained. In the following, we test the encryption of customer personal information, stem cell specimen information as well as stem cell quality information using five encryption methods: DES, AES, encryption based on DNA computation and hyperchaotic system proposed in the literature [36], AES encryption based on DNA proposed in the literature [52], and our proposed DEP encryption. The security of the algorithms is also evaluated in five aspects: histogram, information entropy, key space, key sensitivity and differential attack.

In this experiment, a laptop with Core i5-1135G7 2.4GH CPU, 16GB RAM, and Windows 10 operating system was used to simulate and evaluate the proposed algorithm using MATLAB R2017a. All the test information used in this section is displayed in Table 8. In Table 8, the three text information categorized according to the source of privacy information are Text1, Text2 and Text3.

Due to the fact that all the information in the stem cell bank is highly confidential and private, for security reasons, some symbols in Table 8 are used to replace the original content in the process of presentation to complete the de-privatization process.

4.1 Analysis of histograms

A simple measure to evaluate the security of an encryption algorithm is to perform a histogram analysis. The more uniform the histogram distribution, the more difficult it is for an attack to infer the corresponding plaintext message based on the character distribution regularities [53, 54]. In the histogram evaluation of text information, the ASCII values corresponding to the characters are presented, and the histogram of plaintext and ciphertext messages is shown in Fig 14.

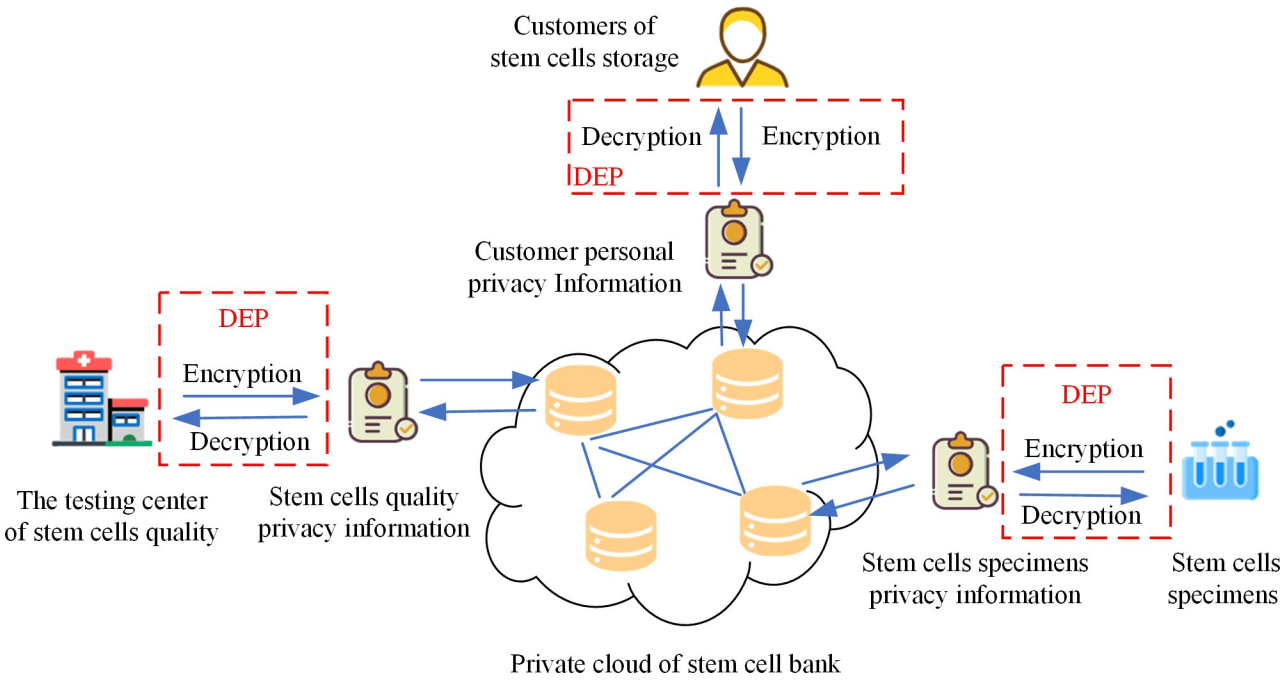

Fig 13. Private cloud access information system for stem cell bank private data.

https://doi.org/10.1371/journal.pone.0293418.g013

In Fig 14, the horizontal axis indicates the ASCII value of the character, and the vertical axis indicates the frequency of that character's appearance. Moreover, (a)-(c) are the histograms of plaintext messages, and (d)-(f) are the histograms of ciphertext messages obtained by applying DEP, respectively. From Fig 14, it can be seen that characters with ASCII values below 50 and 100–150 range appear less frequently in plaintext messages, and the histogram distribution is more discrete and has some breakpoints. The ASCII values of ciphertexts generated by the DEP are more evenly distributed in the range of [0,255], and the longer the plaintext message is, the fewer breakpoints there are in the histogram of ciphertexts after encryption. By comparing the histograms before and after encryption, it is revealed that the original information can be effectively hidden after encryption by the DEP algorithm. For more intuitive evaluation of the uniformity of the histogram distribution, we calculate the variance of the histogram using the following variance Eq (5):

$$\mathrm{var}(x) = \frac{\sum_{i=1}^{N} (x_i - \bar{x})^2}{N} \tag{5}$$

Table 8. Test information.

Text	Information
Text1	母亲姓名:李XX 联系方式:152xxxx9567 身份证号码:41578******1547607 合同号:ZDGssssss23840 (Chinese)
Text2	河南郑大干细胞库科技有限公司xxxx干细胞标本信息 采集地址:河南省****医院 标本数量:**** 新生儿出生日期:2022.09.** 标本接收时间:2022.09.** 15:04 标本接收人:李XX(Chinese)
Text3	1.冻存细胞管数:s 2.血液免疫学检测:(1)乙肝病毒表面抗原:阴性 (2)丙型肝炎病毒抗体:阴性 (3)艾滋病病毒抗体:阴性 (4)巨细胞病毒抗体:阴性 (5)梅毒螺旋体抗体:阴性 3.无菌检测:(1)需氧菌:阴性 (2)厌氧菌:阴性 4.支原体检测:阴性 5.内毒素检测:合格 6.细胞活性:98% 7.细胞形态学检测:正常 8.细胞表型:合格 9.储存温度:-196℃(Chinese)

https://doi.org/10.1371/journal.pone.0293418.t008

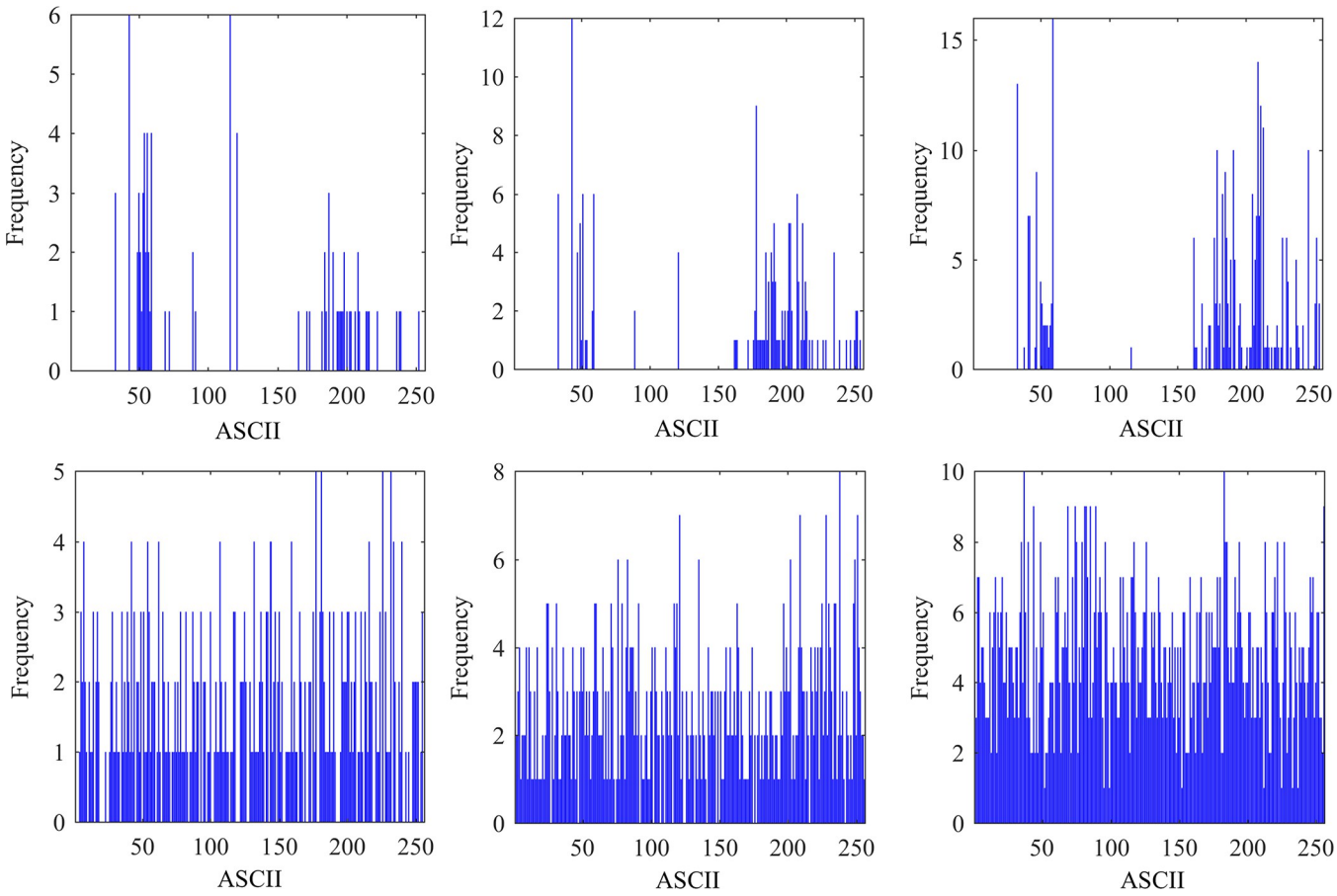

Fig 14. Histogram analysis (a)Text1 histogram (b) Text2 histogram (c)Text3 histogram (d)Text1 histogram encrypted by DEP algorithm (e)Text2 histogram encrypted by DEP algorithm (f)Text3 histogram encrypted by DEP algorithm.

https://doi.org/10.1371/journal.pone.0293418.g014

In Eq (5), x is the ASCII value of the character and N is the length of the character. The lower the variance, the more uniform the distribution of the encrypted characters, and the more unlikely it is for the attacker to break the information using statistical attacks. The variance of the cipher information obtained using the above formula is shown in Table 9.

As we can see from Table 9, the variance of the encrypted histogram is different for different lengths of text messages. With a fixed length of text message, the smaller variance of the encrypted histogram indicates the more uniform distribution of the encrypted message. When comparing the mean values of the histograms of each encryption algorithm, it can be found that the maximum variance value is 124.1792 for the DES algorithm encryption and the minimum variance value is 116.7883 for the DEP algorithm encryption, with a variance reduction

Table 9. The variance of cipher information.

Text	DES	AES	Ref [36]	Ref [52]	Proposed
Text1	126.3864	122.3542	125.2093	121.1146	119.4245
Text2	123.1875	121.1813	121.3590	120.0938	116.6641
Text3	122.9638	120.1711	120.3333	120.0757	114.2763
Average	124.1792	121.2355	122.3005	120.4280	116.7883

https://doi.org/10.1371/journal.pone.0293418.t009

Table 10. Information entropy.

Text	Plain	DES	AES	Ref [36]	Ref [52]	Proposed
Text1	5.2630	6.1412	6.2854	6.0919	6.1109	7.4375
Text2	5.5199	6.7686	6.8750	6.8943	6.8436	7.6953
Text3	5.7085	7.3553	7.3615	7.3682	7.3173	7.8736
Average	5.4971	6.7550	6.8406	6.7848	6.7573	7.6688

https://doi.org/10.1371/journal.pone.0293418.t010

of 5.95%. Consequently, the distribution of ASCII values of characters after encryption by DES algorithm is more discrete and the distribution of characters after encryption by our proposed algorithm is more uniform. As a result, it is proved that DEP algorithm is more resistant to statistical attacks and has the certain security.

4.2 Analysis of information entropy

Information entropy is considered as a measure of randomness [32, 55], with higher information entropy proving a higher degree of randomness of the encrypted message, which is calculated by the following Eq (6):

$$H(x) = -\sum_{i=1}^{N} T(x_i)\log_2 T(x_i) \tag{6}$$

In Eq (6), $T(x_i)$ is the probability of occurrence of character x_i, the probability of occurrence of a certain character ASCII value. The information entropy of the plain and cipher information obtained by the above formula is given in Table 10.

It can be seen from Table 10 that the information entropy of the plain information is lower than that any of the encryption algorithms, indicating that the ciphertext message generated by these encryption algorithms has a certain degree of randomness. From the literature [56, 57], it is known that the desirable value of information entropy is 8. When the entropy value is closer to 8, it is regarded as having good randomness. By contrasting the mean values of information entropy, it can be seen that the text encryption method of DES has low uncertainty of the encrypted message. After applying our proposed DEP algorithm to encrypt three types of text information, the information entropy is improved and is closer to the ideal value of information entropy. The average value of information entropy is improved from the lowest 6.7550 to 7.6688, which is an improvement of 13.53%. Thereby, it is proved that our proposed algorithm guarantees the generation of cipher information with high randomness.

4.3 Analysis of key space

A secure and effective algorithm for stem cell bank privacy data should have a large key space in case the attacker can successfully restore the corresponding privacy information through brute force attack methods [58, 59]. Our proposed DEP algorithm performs a total of three dynamic encodings and one shift rows scheme selection in the first level of encryption. A total of two random encodings, one random operation, and one random decoding scheme selection are performed in the second level of encryption. The actual key parameters of the algorithm and the corresponding key space are shown below:

Table 11. Key space.

DES	AES	Ref [36]	Ref [52]	Proposed
2^{56}	2^{128}	10^{26}	2^{131}	3×2^{279}

https://doi.org/10.1371/journal.pone.0293418.t011

1、Key parameter of the first level encryption S_f

$$S_f = S_{f1} \times S_{f2} = 8^3 \times 4! = 3 \times 2^{12} \tag{7}$$

2、Key parameter of the second level encryption S_s

$$S_s = S_{s1} \times S_{s2} \times S_{s3} = 8^2 \times 4 \times 8 = 2^{11} \tag{8}$$

3、Key parameters of system S_k

$$S_k = 16^{64} = 2^{256} \tag{9}$$

In summary, the total key space of algorithm is:

$$S = S_f \times S_s \times S_k = 3 \times 2^{12} \times 2^{11} \times 2^{256} = 3 \times 2^{279} \tag{10}$$

The key space for various types of encryption algorithms is shown in Table 11.

From Table 11, we can see that DES requires a maximum of 2^{56} attempts to obtain the correct key. AES algorithm using 128-bit key encryption requires a maximum of 2^{128} attempts to get the information cracked. The text encryption algorithm based on DNA computation and hyperchaotic systems takes 10^{26} attempts to break. The AES algorithm based on DNA encoding takes 2^{131} attempts to decrypt. The key space of DEP algorithm is 3×2^{279}, which has been improved to a great extent compared with several encryption algorithms mentioned above. To ensure the security of the encryption algorithm, the size of the key space should not be less than 2^{128} [60, 61]. Since the DEP algorithm has a large key space, the algorithm provides an effective defense against exhaustive attacks.

4.4 Analysis of key sensitivity

For the sake of avoiding attackers using similar keys to destroy the algorithm, the encryption system should have a certain key sensitivity to ensure that the plain data cannot be recovered correctly even after small changes. The key of DEP system is generated by hash algorithm, so it is very sensitive to the initial conditions, so any slight change will bring a big difference to the key data of each part of the system. Let's take Text1 as an instance, the result of decryption using the correct key W1 is given in Table 12, and we change the last base 'G' in the key to 'C', and the decryption result obtained is given in Table 12.

Table 12. Analysis of key sensitivity.

Key	Decryption results
CTTGGCGAGCTAAGTC TCCAAGACTACGCAGG CAGACCACAAGCCCTG GCTTTCAAGGGTGACG	母亲姓名:李XX 联系方式:152xxxx9567 身份证号码:41578******1547607 合同号:ZDGssssss23840(Chinese)
CTTGGCGAGCTAAGTC TCCAAGACTACGCAGG CAGACCACAAGCCCTG GCTTTCAAGGGTGACC	颠盪 脽嬗漆 = YF胧(貓^麾矬 鑢P*蚜夫 H稗 p埧ZI盱酮H Zx哥篤O 8苜BL 7 事翟 攙(Garbled information)

https://doi.org/10.1371/journal.pone.0293418.t012

By analyzing Table 12, we can see that decrypting the key with slight modification will result in a large number of garbled information. The key W1 plays a key role in the key expansion process and in the round key addition process. It determines the subkeys used in each encryption round, and even a slight modification of W1 will result in a completely different subkey. By changing key W2, it leads the mixing columns operation using different matrices. The key W3 is responsible for generating the Chen's hyper-chaotic sequence, which is utilized in blocking, coding, operation and decoding. Similarly, changing W4 will result in generating a different sequence of logic maps, causing changes in the data involved in DNA computing. In conclusion, the keys W1, W2, W3 and W4 have a key role in the different stages of encryption. Any modification of these keys will disrupt the corresponding procedures and sequences, making the decryption process unable to recover the original information correctly. In other words, our proposed DEP algorithm has extremely high key sensitivity.

4.5 Analysis of differential attack

Currently, the avalanche effect is used to measure the significant changes in text output results caused by the flipping of a bit of binary data in the text input data [25, 62]. However, as the length of the text message continues to increase, the complexity and computational effort of the avalanche effect calculation increases, making it unsuitable for reflecting the changes in ciphertext caused by plaintext modifications in our proposed DEP algorithm. The NPCR (Number of pixels change rate) and UACI (Uniform average change intensity) metrics are widely used to evaluate pixel differences before and after encryption in the field of image encryption [63, 64]. They can detect pixel-level changes, such as individual pixel modifications or flipping of a few pixels. This enables them to effectively assess the avalanche effect of encryption algorithms and quantify the degree of impact on images, without considering the size of the images when calculating NPCR and UACI. Therefore, we introduce the NCCR (Number of characters change rate) and UACIT (Unified average change intensity of text) metrics in our text encryption research to evaluate the impact of plaintext changes on ciphertext. The core concept is based on the widely-used evaluation metrics NPCR and UACI in the field of image encryption, which measure the differences in ciphertext information under different inputs. Compared to existing metrics, the proposed NCCR and UACIT simplify the calculation of ciphertext changes due to plaintext modifications, while also calculating the average change intensity of text data. NCCR and UACIT are calculated as follows:

$$E(i) = \begin{cases} 0 \ if \ A(i) = B(i) \\ 1 \ if \ A(i) \neq B(i) \end{cases} \tag{11}$$

$$NCCR = \frac{1}{N}\sum_{i=1}^{N} E(i) \times 100(\%) \tag{12}$$

$$UACIT = \frac{1}{N}\sum_{i=1}^{N} \frac{|A(i) - B(i)|}{255} \times 100(\%) \tag{13}$$

In the above equation, $A(i)$ represents the ASCII value of the cipher information generated from the unmodified plain, $B(i)$ represents the ASCII value of the cipher information generated from the modified plain with a small number of characters, and N is the length of the ciphertext message. NCCR and UACIT indicators reflect the sensitivity of the encryption algorithm to changes in the plaintext message, whereby higher values of these two indicators indicate that the encryption system is more resistant to differential attacks. The NCCR and

Table 13. NCCR and UACIT values of the encrypted information.

		DES	AES	Ref [36]	Ref [52]	Proposed
Text1	NCCR	54.55%	50.00%	9.30%	25.00%	99.48%
	UACIT	19.73%	16.92%	3.78%	2.26%	30.98%
Text2	NCCR	40.00%	20.00%	5.13%	12.50%	99.69%
	UACIT	11.50%	7.33%	2.01%	1.79%	32.93%
Text3	NCCR	39.14%	31.58%	5.00%	14.80%	99.84%
	UACIT	13.32%	12.25%	1.32%	1.16%	33.66%
Average	NCCR	44.56%	33.86%	6.48%	17.43%	99.67%
	UACIT	14.85%	12.17%	2.37%	1.74%	32.52%

https://doi.org/10.1371/journal.pone.0293418.t013

UACIT indicators obtained by using the above formula are shown in Table 13, where the plain information used in different algorithms is consistent with the modified plain information.

As observed from Table 13, all the five encryption algorithms are sensitive to changes in plaintext information and all have a certain degree of resistance to differential attacks. By comparing the average values of NCCR and UACIT, it can be found that the lowest average value of NCCR is 6.48% for the encryption algorithm of literature [36] and the lowest average value of UACIT is 1.74% for the encryption algorithm of literature [52]. The average values of NCCR and UACIT of our proposed DEP encryption algorithm are 99.67% and 32.52%, respectively, and both UACIT and NCCR have been significantly improved. Consequently, fewer characters differed after encryption using the AES based on DNA algorithm, while the average degree of variation was lower after encryption using the algorithms based on DNA and hyperchaotic systems. Furthermore, both methods are weak against differential attacks and less sensitive to changes in plaintext information.

When a limited number of plaintext characters are changed, our proposed DEP algorithm has the feature that the key changes dynamically with the change of plaintext, in other words, the algorithm has the advantage of 'one-time-one-secret'. Moreover, when a few characters are changed, the key generated by the hash function can be very different, and the key obtained by the hash key decomposition algorithm can also be very dissimilar for each subsystem. Therefore, DEP algorithm is more sensitive to plaintext information, which makes the differential attack more challenging and makes it more impossible for the attacker to infer the key information.

5 Conclusions

For the requirements of high confidentiality and strict ethical regulation of privacy data in stem cell bank, this article proposed a double encryption protection (DEP) algorithm for stem cell bank privacy data based on improved AES and chaotic encryption technology.

1. DEP algorithm selects the hash value of plain information as the key. Our displayed hash key decomposition algorithm can generate subkeys for each component of the system through three conversion methods: dynamic encoding, dynamic encoding and cyclic shift, and conversion calculation, in order to meet the actual demands for keys in each subsystem. It realizes the 'one-time-one-secret' encryption system, expands the key space, improves the key sensitivity and the ability to resist differential attacks.
2. In the first level of encryption, we perform three steps of dynamic DNA coding, byte filling based on DNA coding, and dynamic DNA sequence encryption based on AES. The DEP algorithm eliminates the restriction on the length of plain information, improves encryption efficiency, as well as enables dynamic encryption of private data.

3. In the second level of encryption, we put forward the sequence conversion algorithm which enable to generate operation mode sequence. The sequence of operation modes determines the subsequent encoding, operation, diffusion and decoding methods. The randomness of the cipher information and the sensitivity of the key are raised to ensure the security of private data.
4. In purpose of better evaluating the ability of text information to resist differential attacks, the number of character change rate (NCCR) and the unified average change intensity of text (UACIT) are submitted.

The DEP algorithm meets the high confidentiality requirements of private data in stem cell bank and has good application prospects in other related fields.

Acknowledgments

We thank Henan Zhengda Stem Cell Bank Technology Company Limited for providing us with the privacy information of the stem cell bank and working together to determine the encryption scheme.

Author Contributions

Conceptualization: Li Wang, Xinyi Wei, Qunfeng Niu.

Data curation: Li Wang, Xinyi Wei, Yuan Gao, Qunfeng Niu.

Formal analysis: Li Wang, Xinyi Wei.

Funding acquisition: Li Wang, Yuan Zhang, Yuan Gao, Qunfeng Niu.

Investigation: Li Wang, Xinyi Wei, Qunfeng Niu.

Methodology: Li Wang, Xinyi Wei, Yuan Zhang, Yuan Gao, Qunfeng Niu.

Project administration: Li Wang, Xinyi Wei.

Resources: Li Wang, Xinyi Wei.

Software: Li Wang, Xinyi Wei.

Supervision: Li Wang, Xinyi Wei, Qunfeng Niu.

Validation: Li Wang, Xinyi Wei, Qunfeng Niu.

Visualization: Li Wang, Xinyi Wei, Qunfeng Niu.

Writing – original draft: Li Wang, Xinyi Wei.

Writing – review & editing: Li Wang, Xinyi Wei.

References

1. Polykandriotis E, Popescu LM, Horch RE. Regenerative medicine: then and now—an update of recent history into future possibilities. Journal of Cellular and Molecular Medicine. 2010; 14(10):2350–2358. https://doi.org/10.1111/j.1582-4934.2010.01169.x PMID: 20825521
2. Ratcliffe E, Thomas RJ, Williams DJ. Current understanding and challenges in bioprocessing of stem cell-based therapies for regenerative medicine. British Medical Bulletin. 2011; 100(1):137–155. https://doi.org/10.1093/bmb/ldr037 PMID: 21852279
3. Isasi R, Knoppers BM. From Banking to International Governance: Fostering Innovation in Stem Cell Research. Stem Cells International. 2011; 2011. https://doi.org/10.4061/2011/498132 PMID: 21904557

4. China Industrial Economic Information Network [Internet]. Global cell storage market CAGR reaches 22.4%, professional storage institutions such as Boyalife in the spotlight; c2022 [cited 2022 September 16]. http://www.cinic.org.cn/zgzz/qy/1357543.html
5. Hu L, Zhao B, Wang S. Stem-Cell Therapy Advances in China. Human Gene Therapy. 2018; 29 (2):188–196. https://doi.org/10.1089/hum.2017.224 PMID: 29284300
6. Ogbogu U, Burningham S, Ollenberger A, Calder K, Du L, El-Emam K, et al. Policy recommendations for addressing privacy challenges associated with cell-based research and interventions. Bmc Medical Ethics. 2014; 15. https://doi.org/10.1186/1472-6939-15-7 PMID: 24485220
7. Ran W, Wang E, Tong Z. A double scrambling-DNA row and column closed loop image encryption algorithm based on chaotic system. PloS one. 2022; 17(7):e0267094–e0267094. https://doi.org/10.1371/journal.pone.0267094 PMID: 35819964
8. Zhuang Y, Shyu C, Hong S, Li P, Zhang L. Self-sovereign identity empowered non-fungible patient tokenization for health information exchange using blockchain technology. Computers in biology and medicine. 2023; 157:106778–106778. https://doi.org/10.1016/j.compbiomed.2023.106778 PMID: 36934533
9. Helmy M, El-Rabaie E, Eldokany I, El-Samie F. Proposed hybrid encryption framework for robust 3D image communication over wireless channels. Optik. 2023; 273. https://doi.org/10.1016/j.ijleo.2022.170205
10. Kurtz A, Mah N, Chen Y, Fuhr A, Kobold S, Seltmann S, et al. Human pluripotent stem cell registry: Operations, role and current directions. Cell Proliferation. 2022; 55(8). https://doi.org/10.1111/cpr.13238 PMID: 35522426
11. Atsuta Y, Suzuki R, Yoshimi A, Gondo H, Tanaka J, Hiraoka A, et al. Unification of hematopoietic stem cell transplantation registries in Japan and establishment of the TRUMP system. International Journal of Hematology. 2007; 86(3):269–274. https://doi.org/10.1532/IJH97.06239 PMID: 17988995
12. T' Joen V, Vaneeckhaute L, Priem S, Van Woensel S, Bekaert S, Berneel E, et al. Rationalized Development of a Campus-Wide Cell Line Dataset for Implementation in the Biobank LIMS System at Bioresource Center Ghent. Frontiers in Medicine. 2019; 6. https://doi.org/10.3389/fmed.2019.00137 PMID: 31294023
13. Chen Y, Sakurai K, Maeda S, Masui T, Okano H, Dewender J, et al. Integrated Collection of Stem Cell Bank Data, a Data Portal for Standardized Stem Cell Information. Stem Cell Reports. 2021; 16(4):997–1005. https://doi.org/10.1016/j.stemcr.2021.02.014 PMID: 33740463
14. Hossain FS, Ali ML. A Novel Byte-Substitution Architecture for the AES Cryptosystem. Plos One. 2015; 10(10). https://doi.org/10.1371/journal.pone.0138457 PMID: 26491967
15. Swann R, Stine J. Evaluation of a Modular Approach to AES Hardware Architecture and Optimization. Journal of Signal Processing Systems for Signal Image and Video Technology. 2023. https://doi.org/10.1007/s11265-022-01832-w
16. Razaq A, Ahmad M, El-Latif A. A novel algebraic construction of strong S-boxes over double GF(2^7) structures and image protection. Computational & Applied Mathematics. 2023; 42(2). https://doi.org/10.1007/s40314-023-02215-y
17. Du S, Ye G. IWT and RSA based asymmetric image encryption algorithm. Alexandria Engineering Journal. 2023; 66:979–991. https://doi.org/10.1016/j.aej.2022.10.066
18. Sabir S, Guleria V. A novel multi-layer color image encryption based on RSA cryptosystem, RP2DFrHT and generalized 2D Arnold map. Multimedia Tools and Applications. 2023. https://doi.org/10.1007/s11042-023-14829-9
19. Ping H. Network Information Security Data Protection Based on Data Encryption Technology. Wireless Personal Communications. 2022; 126(3):2719–2729. https://doi.org/10.1007/s11277-022-09838-0
20. Gong J. Plaintext recovery attack on 3DES algorithm with different byte keys. Journal of Intelligent & Fuzzy Systems. 2020; 38(6):7487–7495. https://doi.org/10.3233/jifs-179821
21. Hung CW, Hsu WT. Power Consumption and Calculation Requirement Analysis of AES for WSN IoT. Sensors. 2018; 18(6). https://doi.org/10.3390/s18061675 PMID: 29882865
22. Cho J, Soekamtoputra S, Choi K, Moon J. Power dissipation and area comparison of 512-bit and 1024-bit key AES. Computers & Mathematics with Applications. 2013; 65(9):1378–1383. https://doi.org/10.1016/j.camwa.2012.01.035
23. Luo Z, Shen K, Hu R, Yang Y, Deng R. Optimization of AES-128 Encryption Algorithm for Security Layer in ZigBee Networking of Internet of Things. Computational Intelligence and Neuroscience. 2022; 2022. https://doi.org/10.1155/2022/8424100 PMID: 35498166
24. Zhang Y, Chen A, Chen B. A unified improvement of the AES algorithm. Multimedia Tools and Applications. 2022; 81(13):18875–18895. https://doi.org/10.1007/s11042-022-12742-1

25. Abikoye OC, Haruna AD, Abubakar A, Akande NO, Asani EO. Modified Advanced Encryption Standard Algorithm for Information Security. Symmetry-Basel. 2019; 11(12). https://doi.org/10.3390/sym11121484

26. Liu YA, Chen L, Li XW, Liu YL, Hu SG, Yu Q, et al. A dynamic AES cryptosystem based on memristive neural network. Scientific Reports. 2022; 12(1). https://doi.org/10.1038/s41598-022-13286-y PMID: 35902602

27. Adleman LM. Molecular computation of solutions to combinatorial problems. Science (New York, N.Y.). 1994; 266(5187):1021–1024. https://doi.org/10.1126/science.7973651 PMID: 7973651

28. Lu M, Lai X, Xiao G, Qin L. Symmetric-key cryptosystem with DNA technology. Science in China Series F-Information Sciences. 2007; 50(3):324–333. https://doi.org/10.1007/s11432-007-0025-6

29. Srilatha N, Murali G. Fast three level DNA Cryptographic technique to provide better security. 2nd International Conference on Applied and Theoretical Computing and Communication Technology. 2016;428–432. https://doi.org/10.1109/ICATCCT2016.7912037

30. Liu H, Lin D, Kadir A. A novel data hiding method based on deoxyribonucleic acid coding. Computers & Electrical Engineering. 2013; 39(4):1164–1173. https://doi.org/10.1016/j.compeleceng.2013.01.017

31. Hagras T, Salama D, Youness H. Anti-attacks encryption algorithm based on DNA computing and data encryption standard. Alexandria Engineering Journal. 2022; 61(12):11651–11662. https://doi.org/10.1016/j.aej.2022.05.033

32. Aashiqbanu S, Krishna Murthy B, Bindu Sai G, Sowmya G, Hemaswitha K, Amirtharajan R. Telugu DNA for Safe Delivery: A Secured Text Communication. Wireless Personal Communications. 2022; 127(4):2873–2889. https://doi.org/10.1007/s11277-022-09901-w

33. Alruily M, Shahin OR, Al-Mahdi H, Taloba AI. Asymmetric DNA encryption and decryption technique for Arabic plaintext. Journal of Ambient Intelligence and Humanized Computing. 2021. https://doi.org/10.1007/s12652-021-03108-w

34. Wen HP, Ma LC, Liu LH, Huang YM, Chen ZF, Li R, et al. High-quality restoration image encryption using DCT frequency-domain compression coding and chaos. Scientific Reports. 2022; 12(1). https://doi.org/10.1038/s41598-022-20145-3 PMID: 36192488

35. Babaei M. A novel text and image encryption method based on chaos theory and DNA computing. Natural Computing. 2013; 12(1):101–107. https://doi.org/10.1007/s11047-012-9334-9

36. Oleiwituama S, Kadum SA, Hussein Z. Text Encryption Approach Using DNA Computation and Hyperchaotic System. 2nd Information Technology to Enhance e-Learning and other Application Conference. 2021;100–105. https://doi.org/10.1109/IT-ELA52201.2021.9773674

37. Kumar M, Kumar S, Budhiraja R, Das M K, Singh S. A cryptographic model based on logistic map and a 3-D matrix. Journal of Information Security and Applications. 2017; 32:47–58. https://doi.org/10.1016/j.jisa.2016.09.002

38. Alawida M, Teh JS, Mehmood A, Shoufan A, Alshoura WH. A chaos-based block cipher based on an enhanced logistic map and simultaneous confusion-diffusion operations. Journal of King Saud University-Computer and Information Sciences. 2022; 34(10):8136–8151. https://doi.org/10.1016/j.jksuci.2022.07.025

39. Lawnik M, Moysis L, Volos C. Chaos-Based Cryptography: Text Encryption Using Image Algorithms. Electronics. 2022; 11(19). https://doi.org/10.3390/electronics11193156

40. Salama GM, Omar B, El-shafai W, El-banby GM, Hamed HFA, El-Gazar S, et al. Secure biometric systems based on bio-signals and DNA encryption of optical spectrograms. Optics Express. 2023; 31(3):3927–3944. https://doi.org/10.1364/OE.478215 PMID: 36785373

41. Liu L, Zhang Q, Wei X. A RGB image encryption algorithm based on DNA encoding and chaos map. Computers & Electrical Engineering. 2012; 38(5):1240–1248. https://doi.org/10.1016/j.compeleceng.2012.02.007

42. Cheng H, Song Y, Huang C, Ding Q. Self-Adaptive Chaotic Logistic Map: An Efficient Image Encryption Method. Journal of Internet Technology. 2016; 17(4):743–752. https://doi.org/10.6138/JIT.2016.17.4.20141014a

43. Luo YQ, Yu J, Lai WR, Liu LF. A novel chaotic image encryption algorithm based on improved baker map and logistic map. Multimedia Tools and Applications. 2019; 78(15):22023–22043. https://doi.org/10.1007/s11042-019-7453-3

44. Liu LF, Miao SX. A new image encryption algorithm based on logistic chaotic map with varying parameter. Springerplus. 2016; 5. https://doi.org/10.1186/s40064-016-1959-1 PMID: 27066326

45. Gao T, Chen Z. A new image encryption algorithm based on hyper-chaos. Physics Letters A. 2008; 372(4):394–400. https://doi.org/10.1016/j.physleta.2007.07.040

46. Zhang Q, Guo L, Wei XP. A novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system. Optik. 2013; 124(18):3596–3600. https://doi.org/10.1016/j.ijleo.2012.11.018

47. El-Khamy SE, Mohamed AG. An efficient DNA-inspired image encryption algorithm based on hyper-chaotic maps and wavelet fusion. Multimedia Tools and Applications. 2021; 80(15):23319–23335. https://doi.org/10.1007/s11042-021-10527-6

48. Mohamed AG, Korany NO, El-Khamy SE. New DNA Coded Fuzzy Based (DNAFZ) S-Boxes: Application to Robust Image Encryption Using Hyper Chaotic Maps. Ieee Access. 2021; 9:14284–14305. https://doi.org/10.1109/access.2021.3052161

49. Wei D, Jiang M, Deng Y. A secure image encryption algorithm based on hyper-chaotic and bit-level permutation. Expert Systems with Applications. 2023; 213. https://doi.org/10.1016/j.eswa.2022.119074

50. Zhang SJ, Liu LF, Xiang HY. A Novel Plain-Text Related Image Encryption Algorithm Based on LB Compound Chaotic Map. Mathematics. 2021; 9(21). https://doi.org/10.3390/math9212778

51. Wen HP, Liu Z, Lai HW, Zhang CF, Liu LH, Yang JY, et al. Secure DNA-Coding Image Optical Communication Using Non-Degenerate Hyperchaos and Dynamic Secret-Key. Mathematics. 2022; 10(17). https://doi.org/10.3390/math10173180

52. Bahig HM, Nassr DI. DNA-Based AES with Silent Mutations. Arabian Journal for Science and Engineering. 2019; 44(4):3389–3403. https://doi.org/10.1007/s13369-018-3520-8

53. Murillo-Escobar MA, Cruz-Hernandez C, Abundiz-Perez F, Lopez-Gutierrez RM. Implementation of an improved chaotic encryption algorithm for real-time embedded systems by using a 32-bit microcontroller. Microprocessors and Microsystems. 2016; 45:297–309. https://doi.org/10.1016/j.micpro.2016.06.004

54. Sekar JG, Ezhumalai P, Chokkalingam A. An efficient chaotic system based hybrid radiation heat transfer sunflower optimization algorithm for securing digital image transmission. Concurrency and Computation-Practice & Experience. 2022; 34(10). https://doi.org/10.1002/cpe.6814

55. Zhang Y, Tang YJ. A plaintext-related image encryption algorithm based on chaos. Multimedia Tools and Applications. 2018; 77(6):6647–6669. https://doi.org/10.1007/s11042-017-4577-1

56. Satir E, Kendirli O. A symmetric DNA encryption process with a biotechnical hardware. Journal of King Saud University Science. 2022; 34(3). https://doi.org/10.1016/j.jksus.2022.101838

57. Wang J. Digital Image Encryption Algorithm Design Based on Genetic Hyperchaos. International Journal of Optics. 2016; 2016. https://doi.org/10.1155/2016/2053724

58. Gabr M, Younis H, Ibrahim M, Alajmy S, Khalid I, Azab E, et al. Application of DNA Coding, the Lorenz Differential Equations and a Variation of the Logistic Map in a Multi-Stage Cryptosystem. Symmetry-Basel. 2022; 14(12). https://doi.org/10.3390/sym14122559

59. Chidambaram N, Raj P, Thenmozhi K, Amirtharajan R. Advanced framework for highly secure and cloud-based storage of colour images. Iet Image Processing. 2020; 14(13):3143–3153. https://doi.org/10.1049/iet-ipr.2018.5654

60. Rani N, Mishra V, Singh B. Piecewise symmetric magic cube: application to text cryptography. Multimedia Tools and Applications. 2022. https://doi.org/10.1007/s11042-022-14153-8

61. Akhavan A, Samsudin A, Akhshani A. A novel parallel hash function based on 3D chaotic map. Eurasip Journal on Advances in Signal Processing. 2013. https://doi.org/10.1186/1687-6180-2013-126

62. Aljawarneh S, Yassein MB, Talafha WA. A resource-efficient encryption algorithm for multimedia big data. Multimedia Tools and Applications. 2017; 76(21):22703–22724. https://doi.org/10.1007/s11042-016-4333-y

63. Kamal ST, Hosny KM, Elgindy TM, Darwish MM, Fouda MM. A New Image Encryption Algorithm for Grey and Color Medical Images. Ieee Access. 2021; 9:37855–37865. https://doi.org/10.1109/access.2021.3063237

64. Chen YC, Tang CM, Ye RS. Cryptanalysis and improvement of medical image encryption using high-speed scrambling and pixel adaptive diffusion. Signal Processing. 2020; 167. https://doi.org/10.1016/j.sigpro.2019.107286