International Journal of Engineering &Technology, 7 (4) (2018) 6290-6293

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet.v7i4.29057
Research paper

Cloud storage security scheme for image encryption using modified morse and zigzag pattern

R. Thilagavathy [1] *, A. Murugan [2]

[1] Research Scholar, PG & Research Department of Computer Science, Dr. Ambedkar Government Arts College (Autonomous), Affiliated to University of Madras, Chennai, India
[2] Associate Professor and Head, PG & Research Department of Computer Science, Dr. Ambedkar Government Arts College (Autonomous), Affiliated to University of Madras, Chennai, India
**Corresponding author E-mail:*

Abstract

In the research of cloud storage security, the image encryption is given much attention and a lot of encryption algorithms have been proposed. The image encryption is different from the text encryption methods owing to some of features of images such as capacity and data redundancy. So, the image encryption is comparatively difficult to handle with traditional methods. In the proposed work, the image encryption and decryption are based on modified Morse code and diagonal zigzag pattern. To begin with, the pixels of image are extracted and then converted into binary form. The binary data is replaced by DNA sequence with modified Morse code and diagonal zigzag pattern. The proposed algorithm successfully encrypts/decrypts the image with DNA and modified Morse code with diagonal zigzag pattern. The encrypted image using the proposed algorithm is absolutely different when compared to original image file. So the encrypted image is suitable for the secured transmission over the cloud data storage. Thus, this proposed model provides an additional measure to tighten the image security efficiently.

Keywords: *Cloud Security; Image Pixels; DNA Sequence; Morse Code; Diagonal Zigzag Pattern.*

1. Introduction

Every day the number of cloud users increases because of its advantages. It is an on demand online services provider for various organizations. Data storing is an important need of organizations. Cloud provides a large space for storing the data. Cloud computing provides a convenient and cheap mode for content propagation. In cloud computing every day the size of data storage is getting larger. The need of storing text and images securely over cloud environment promoted the creation of cryptography to enable the cloud user to encrypt their data.

2. Literature review

In the literature review the survey is done on the encryption algorithms in the area of cloud security based on DNA computing. It also includes the benefits of cloud computing and importance of cloud security.

Chang - Mok Shin et al. [1] proposed an image encryption with multilevel encryption using binary phase exclusive-OR operation. The image is encrypted with binary phase XOR operation. M.Zeghid et al. [2] proposed an algorithm based on AES for image encryption. In the proposed algorithm they analyze and add key stream generator to AES for better performance. Grasha Jacob et al. [3] proposed an encryption algorithm for secure transmission of data using DNA sequence and JPEG Zigzag code [4].

D. Suresh et al. [5] proposed a model to solve the cloud data storage issues. This model helps the cloud user to take decision about cloud data storage based on their budget. The data transmission is done with DNA sequences AGCT more securely. The encryption algorithms are used to encrypt the original data before transmitting to cloud [6]. The cloud computing risk and challenges are discussed and solved [7 - 9].

The proposed work is similar to Cloud Storage Security Scheme using DNA Computing with Morse code and zigzag [10]. In the proposed security model the encryption is carried with image pixel and decryption is done with encrypted pixel.

2.1. Cryptography

Cryptography is a technique of converting a data into a cryptic (non-readable) form to prevent the confidential data from the hackers.

The conversion of data from plain text to non readable form is called encryption. The decryption process reverts the data to its original form. The cryptography provides the following security,

- Data integrity
- Authentication of user
- Non-repudiation of data
- Data confidentiality

Traditional encryption algorithms such as RSA, DES, IDEA, and AES are symmetric or asymmetric key based algorithms [11]. In the symmetric and asymmetric algorithm the keys are used for encryption and decryption of plaintext. Some of other cryptography methods are substitution, transposition, concealment, block cipher, stream cipher. In the substitution method, the plaintext is converted into cipher text. Transposition method is used to encrypt the plain text by constitutes a permutation of the original text. In the concealment cipher the randomized transformation is done for encryption process. In the block cipher and stream cipher plaintext is processed by block and stream ciphers.

Many symmetric key and asymmetric algorithms exist for encryption and decryption. These algorithms are based on keys. These keys are easier to hack by trying multiple possibilities on secret keys [12]. So there is a need to develop the security algorithms with DNA sequence.

2.2. DNA based cryptography

DNA is Deoxyribonucleic acid which carries information of living organisms. The DNA composed of four nucleotides Adenine (A), Thymine (T), Cytosine (C) and Guanine (G). The helical structure is formed based on the pair rule. According to base pair rule the nucleobases would pair A-T, T-A, G-C, C-G. Cryptography is combined with DNA computing to protect and hide data.

L.Adelman introduced DNA computing in the year 1994 to solve Hamiltonian path problems (HPP) [13]. The DNA cryptography has evolved from the DNA computing. The DNA cryptography is used for secure communication. The DNA sequences ACGT are used to create encryption and decryption technology [14]. The unbreakable encryption and decryption schemes are achieved based on DNA sequence [15].

2.3. Morse and diagonal zigzag pattern

The Morse code was introduced in the year 1836 by F.B. Morse in the telegraphy field. The Morse code is used to transmit the message in the form of ‘dot’ and ‘dash’. The modified Morse code is shown in the Fig.1 (a).

The diagonal zigzag pattern is matrix structure of n^2 integers. The motive wave that travels on diagonal trend is called diagonal zigzag pattern. The diagonal zigzag pattern is shown in the Fig.1 (b).

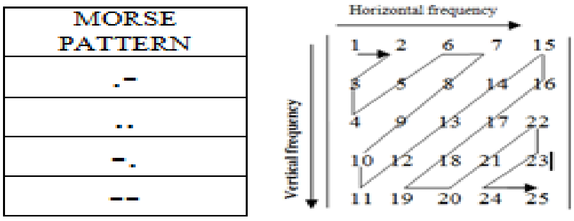

Fig. 1: A) Modified Morse Pattern. B) Diagonal Zigzag Pattern.

The diagonal zigzag pattern and modified Morse code are combined in the proposed model [16].

3. Noise identification

Noise in data communication is unwanted electrical or electromagnetic power that degrades the quality of data at data transmission. In digital communication the data is stored and processed in two states. They are,

- Positive
- Non-Positive

The positive state is represented by 1 and the non positive state is represented by 0. The different types of noise are thermal noise, shot noise, signal noise, burst noise and flicker noise.

3.1. Cyclic redundancy check algorithm

The Cyclic Redundancy Check is a technique used to detect errors and changes happened during data transmission. It is also used to detect errors when a data file is retrieved from storage. For each file in file system has checksum along with the content. The CRC check sum will differ from the received check sum if there is any miss match occurs between original file and transmitted file. CRC algorithm uses modified Morse code on both sender and receiver side to check for the error.

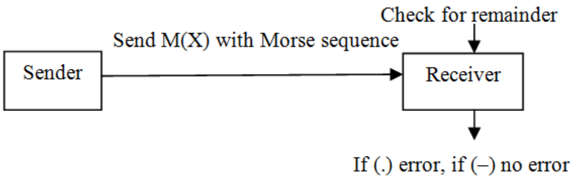

Fig. 2: CRC for Morse Code Data.

In the above Fig.2 the and – are used as an error detection code. If the CRC is . the transmission is done with error and can go for retransmission of data. If the CRC is – the data transmission is carried without error.

3.2. Modified parity check

In the telecommunication the parity check is used for error detection. The parity check is based on the bit added to the string. The two types of parity bits namely even parity and odd parity. Even parity bit occurs if parity bit value is 1. Odd parity bit occurs if parity bit value is 0. In the proposed model the two types of parity checks are used to check for errors. They are as follows,

a) Dash parity bit
b) Dot parity bit

In the dash parity the parity bit value will be – and in the dot parity the parity bit value will be (.).

Table 1: Example of Dash and Dot Parity

Data bits	Count of dash (-)	8-bit parity	
		-	.
-.-.-.-	4	.-.-.-.-	--.-.-.-
-..-.-.	3	--..-.-.	.-..-.-.
.-.-.--	4	..-.-.--	-.-.-.--
..-.-.-	3	-..-.-.-	…-.-.-

Based on the count of dash (-) in the data bits the parity bit value is set to dash parity bit (–) or dot parity bit(.). In the case of even value, the parity bit (-) is set in the dot parity bit. If the count value is odd, the parity bit (-) is set in the dash parity bit which is shown in table 1.

4. Image encryption

The proposed technique make use of all the four type of conversions like binary sequence, DNA sequence, Morse code and diagonal zigzag pattern for image encryption. In the first step, the pixel of original image is converted to binary sequence data. The second step is the conversion of DNA sequence data, where the DNA sequences AGCT are used to encrypt the binary data. The third step is the conversion of DNA sequence data into modified Morse code data, which is used to generate the dot and dash form of DNA sequence data. The diagonal zigzag pattern is applied on the modified Morse pattern data to construct the secret image.

The proposed technique is unique compared to other different image encryption algorithms in a way that the data is not in the form of image. Most of the algorithms use keys to generate encryption image. This technique generates the encrypted image based on the pixels. The modified Morse code and diagonal zigzag pattern used to achieve unbreakable image encryption system. The proposed image encryption scheme is shown in the Fig.3.

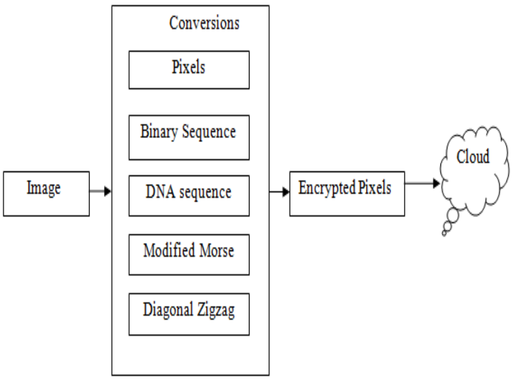

Fig. 3: Encryption Phase.

The rows and columns of the total image pixel are converted based on DNA sequence and modified Morse code. The diagonal zigzag pattern is used on rows and columns to encrypt the image pixels.

The Encryption algorithm is given below,

```
Algorithm 1: DNA based image encryption
Input: Image
Output: Encrypted image
1)  begin
2)    //convert image to pixel
3)    L ← size of the image;
4)    for i = 0 to L do;
5)      for j = 0 to L do;
6)        img[i][j] ← pixel value;
7)      endfor
8)    endfor
9)    //convert pixel to binary
10)   for i = 0 to L do;
11)     for j = 0 to L do;
12)       bindata[x] ← img[i][j];
13)     endfor
14)   endfor
15)   //convert binary to DNA sequence
16)   for x = 0 to $L^2$ do;
17)     DNA[i] ← bindata[x];
18)   endfor
19)   //convert DNA to Modified Morse code
20)   for i = 0 to $L^2$do;
21)     morsedata[j] ← DNA[i];
22)   endfor
23)   //convert Morse data to diagonal zigzag pattern
24)   for n = 0 to L do;
25)     for m = 0 to L do;
26)       matrix[n][m] ← morsedata[j];
27)       dzigzag[n] ← matrix[n][m];
28)     end for
29)   end for
30) end
```

In the above algorithm line from 4-6, 10-14 and 24-28 has nested loops. So the time complexity is O (n^2). In the encryption algorithm from line number 15-18 and 19-22 has single loop will execute till L^2. So the time complexity will be O(n^2). And the time complexity of the algorithm is O (n^2).

5. Image decryption

The decryption algorithm is a reversal process of encryption technique. The decryption algorithm has four conversions. In the decryption, first, the diagonal zigzag pattern data is converted into modified Morse pattern. The modified Morse data is converted into DNA sequence data and binary data. Finally the original image picture is constructed using the decryption technique. The decryption phase is shown in the Fig.4.

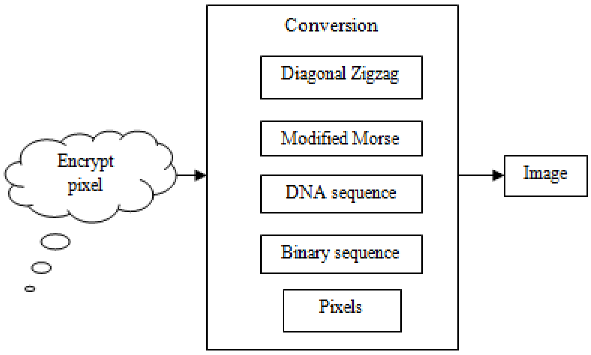

Fig. 4: Decryption Phase.

The decryption algorithm is shown below,

```
Algorithm 2: Decryption phase
Input: Encrypted Image
Output: Original image
begin
  //convert morsedata to matrix
  for n = 0 to L do;
    for m = 0 to L do;
      matrix[n][m] ← dzigzag[n];
      morsedata[i] ← matrix[n][m];
    end for
  endfor
  //convert modified morsedata to DNA sequence
  for i = 0 to L do;
    DNA[i] ← morsedata[i];
  end for
  //convert DNA sequence to binary
  for x = 0 to L do;
    binary[x] ← DNA[i];
  end for
  //convert binary to image pixel
  for i = 0 to L do;
    for j = 0 to L do;
      image[i][j] ← binary[x];
    end for
  endfor
end
```

In the above decryption algorithm is the reverse process of the encryption algorithm and it takes O(n^2) as its time complexity.

6. Performance evaluation and result

The pixel information about the image is processed based on the bits. The number of bits used in each conversion is shown in the following table 2.

Table 2: Number of Bits Used in the Encryption Phase

S. No	Number of bits	Description
1	0-3	Original image pixels
2	8	Binary conversion
3	2	DNA conversion
4	2-4	Modified Morse code
5	2-4	Diagonal zigzag pattern

The image pixels are extracted from the image. The number of bits of image pixel is starts from 0-3 bits. The binary conversion is done in eight bit binary value. The binary data is converted to DNA sequenced data based on 2 bits. The modified Morse code is based on 2-4 bit dash and dot. The diagonal zigzag pattern conversion is done based on 2-4 bits.

Net Beans IDE 8.0.1 is used to simulate the algorithms in the proposed model. The experiments are performed using 300 different images with different size to prove the efficiency of the proposed algorithm. The noise identification test is carried by applying CRC check and parity bit check.

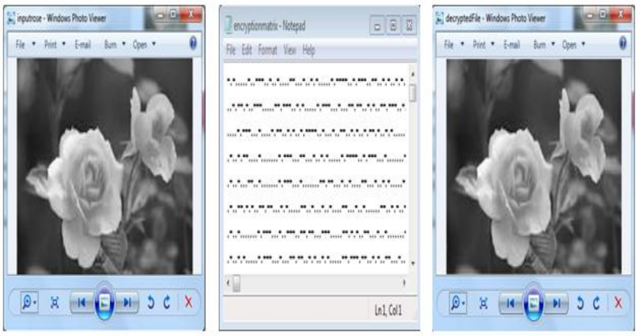
inputrose - Windows Photo Viewer
File Print E-mail Burn Open
encryptionmatrix - Notepad
File Edit Format View Help
Ln1, Col1
decryptedFile - Windows Photo Viewer
File Print E-mail Burn Open

Fig. 5: A) Original Image. B) Encrypted Image. C) Decrypted Image.

An example encryption and decryption of a picture is given in the above Fig.5. The original image is stored in rose.jpg file and encrypted encryption.txt. The encrypted file is decrypted and image is stored in decryptedimage.jpg.

6.1. Histogram analysis

The histogram is used to plot the number of pixels at each intensity level. If the histograms of the original image and decrypted image are same, then the encryption scheme is efficient. The histograms of an original and decrypted image are shown in the Fig. 6.

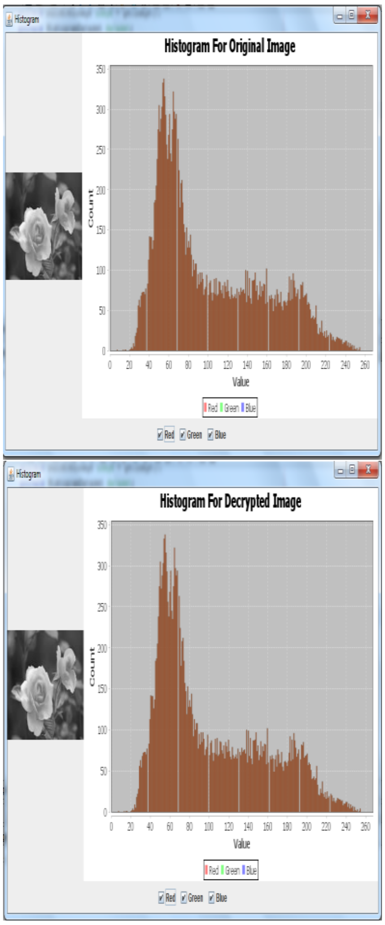

Fig. 6: A) Histogram of Original Image. B) Histogram of Decrypted Image.

The histogram of original and decrypted images is compared using a standard existing comparison algorithm.

The results obtained from the comparison algorithm shows that the proposed scheme works efficiently.

7. Conclusion and future work

Cloud computing is a utility computing that can provide convenient access to set of resources such as storage, software services, and infrastructure services with least management intervention. However the basic computing, the image encryption schemes are developed. We surveyed the existing image security models of cloud computing, and proposed image encryption scheme using DNA sequence.

To increase the level of data storage security, the modified Morse code and diagonal zigzag pattern are used. Finding original image is difficult because guessing the modified Morse pattern by hacker is nearly unachievable. In future, it is possible to extend the encryption scheme to encrypt the video and audio file.

References

[1] Chang-Mok Shin, Dong-Hoan Seo, Kyu-Bo Chol, Ha-Wmn Lee and SmJmng Kim, *Multilevel Image Encryption by Binary Phase XOR Operations*. IEEE Proceeding in the year 2003.

[2] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki, *A Modified AES Based Algorithm for Image Encryption*. Proceeding in World Academy of Science, Engineering and Technology. 27, 2007.

[3] Grasha Jacob and Murugan .A, *An Encryption Scheme with DNA Technology and JPEG Zigzag Coding for Secure Transmission of Images.* The International journal of Computer Science and Communications Security (IJCSCS). 3, 61–5, 2013.

[4] Grasha Jacob and Murugan .A, *Towards the Secured of Image on Multi-cloud System.* Elsevier Proceedings, 58-62, 2014.

[5] Sureshraj, D and Murali Bhaskaran .V, *Automatic DNA Sequence Generation for Secured Effective Multi-Cloud Storage.* Journal of Computer Engineering (IOSR-JCE), Vol.15. 86-94, 2013. https://doi.org/10.9790/0661-1528694.

[6] Fethi Belkhouche and Uvais Qidwai, *Binary image encoding using 1D chaotic maps.* IEEE Proceeding in the year 2003.

[7] Huang-Pei Xiao and Guo-Ji Zhang, *An Image Encryption Scheme Based On Chaotic Systems*, IEEE Proceedings of the Fifth International Conference on Machine Learning and Cybernetics, Dalian, 13-16, 2006.

[8] Mohammad Ali Bani Younes and Aman Jan tan, *an Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption.* International Journal of Computer Science and Network Security, Vol.8, 2008.

[9] Padmaja .N and Priyanka Koduru, *Providing data security in cloud computing using public key cryptography.* International Journal of Engineering Sciences Research, Vol.4 (1).1059-1063, 2013.

[10] Murugan .A and Thilagavathy .R, *Cloud Storage Security Scheme using DNA computing with Morse code and Zigzag Pattern.* International Conference on power, Control, Signals & Instrumentation Engineering (ICPCSI), Vol.v.226-231, 2017. https://doi.org/10.1109/ICPCSI.2017.8392120.

[11] Dubey and Ashutosh .K, *Cloud user Security based on RSA and MD5 algorithm for resource attestation and sharing in Java environment*. Software Engineering (CONSEG). 2012 CSI Sixth International Conference, 2012. https://doi.org/10.1109/CONSEG.2012.6349503.

[12] Che Jianhua, Yamin Duan, Tao Zhang and Jie Fan, *Study on the security models and strategies of cloud computing*. In Procedia Engineering, Vol. (23).586-593, 2011. https://doi.org/10.1016/j.proeng.2011.11.2551.

[13] Adleman. L, *Molecular computation of solutions to combinational problems*. American Association for the Advancement of Science, 1021-1024, 1994. https://doi.org/10.1126/science.7973651.

[14] Ephin M, Judy Ann Joy and N. A. Vasanthi, *Survey of Chaos based Image Encryption and Decryption Techniques*. Amrita International Conference of Women in Computing (AICWIC'13). Proceedings published by International Journal of Computer Applications (IJCA), 2003.

[15] Borda, Monica and Olga. T, *DNA secret writing Techniques.* In IEEE conferences, 451-456, 2010. https://doi.org/10.1109/ICCOMM.2010.5509086.

[16] Murugan .A and Thilagavathy .R, *Securing Cloud Data using DNA and Morse code: A Triple Encryption Scheme.* International Journal of Control Theory and Applications (IJCTA), Vol.10. 31-18, 2017.