International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 22 (2018) pp. 15766-15772


# Triple Encryption Scheme with Parallel Zigzag Pattern for Cloud Data Storage Scheme

**A. Murugan**
*Associate Professor and Head, PG & Research Department of Computer Science ,*
*Dr. Ambedkar Government Arts College (Autonomous), Affiliated to University of Madras,Chennai, India.*

**R. Thilagavathy**
*Research Scholar, PG & Research Department of Computer Science,*
*Dr. Ambedkar Government Arts College (Autonomous), Affiliated to University of Madras,Chennai, India.*

**Abstract**

Cloud computing provides customer the way to share resources and IT services that belong to different organization and government. Cloud computing is an on-demand service model which gives flexible, cheaper and faster services. The cloud resources are shared at open environment between more organizations, thus it makes security related risks. In this paper we proposed a method to build a secured cloud storage system by integrating the DNA computing methodology into cloud computing. In this model, the modified Morse pattern and parallel zigzag pattern are integrated to improve the security of cloud storage.

**Keywords**: Cloud Security, DNA, Modified Morse code, Zigzag pattern.

## INTRODUCTION

The term "cloud" originates from the telecommunications world of the 1990's, when providers began using virtual private network (VPN) services for data communication. Cloud computing shares its resources among a cloud of service consumers, partners, and vendors. Every day cloud computing is widening its fundamental aspects. They are on-demand self service, broad network access, resource pooling, and rapid elasticity [1].

Security is a major element in cloud computing infrastructure, because it is necessary to ensure the secured and authorized access to cloud storage. The security issues are handled by combining cryptography with DNA computing [2]. The DNA cryptographic techniques help the cloud user and provider to protect their sensitive information from unknown access. Cloud computing has huge security risks as it deals with sensitive information [3] [4].

## LITERATURE REVIEW

L. Adelman et al. [5] proposed an algorithm based on molecules. The DNA molecules are used to solve the Hamiltonian path problem (HPP). The molecular computation problems and combinational problems are solved by DNA molecules. D. Suresh et al. [6] 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 [7] [8] [9]. The encryption algorithms are used to encrypt the original data before transmission. The cloud computing risk and challenges are discussed and solved [10] [11] [12] [13].

The Morse code is invented by Samuel F.B.Morse in the telegraphy field in the year 1836[14]. This code encodes the original text to non-English natural language called "dots" and "dashes". Honey et al. [15] describe a model for character recognition in various fonts in which the text is written. The characters are optically scanned and transformed to machine understandable language. It is used to scan and store the content in the machine. Jacob Grasha et al. [16] proposed an encryption algorithm for secure transmission of data using DNA sequence and JPEG Zigzag code. Annalakshmi et al. [17] solves the security issues of information during transmission. The proposed algorithm is based on Zigzag ciphers. These Zigzag ciphers help the user to secure to the data in the cloud environment.

The proposed work is an extension of a Cloud Storage Security Scheme using DNA Computing with Morse code and Zigzag Pattern which is published in IEEE Conference (ICPCSI) 2017[18]. In the above security model the encryption is carried with plain text and decryption is done with encrypted data.

## DNA COMPUTING

L.Adleman introduced DNA computing in the year 1994. The combinational problems in molecular computing were solved by using DNA computing. The DNA cryptography has evolved from the DNA computing [19][20]. DNA is a Deoxyribonucleic acid. This DNA molecule is unique in all the living organisms. The DNA molecule consists of genetic information. The nucleotides are basic building blocks of DNA strands. The DNA molecule consists of nucleotides which are used to store biological information. DNA consists of DNA strands which are polymer chains composed of four nucleotides called Adenine (A), Guanine (G), Cytosine(c) and Thymine (T).

The Watson-crick complementary base pair rule is used to implement the DNA computing. To convert the binary data to DNA sequence the binary numbers 0's and 1's are used. The sequences are represented as 00, 01, 10, and 11. The secure communication is achieved by using DNA cryptography. Unbreakable encryption algorithms are developed in DNA cryptography using DNA sequences [21] [22].

### DNA Cryptography

DNA sequence ATGC is the basic sequence of DNA cryptographic technique. The randomness of DNA sequence used to achieve strong encryption algorithms. The DNA computing is high in cost and time consuming. These can be overcome by using modern cryptographic techniques which is based on computer based algorithms. The complex problems can be solved by DNA cryptographic algorithms [23] [24].

### Morse Pattern

F.B. Morse code was introduced in the year 1836 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).

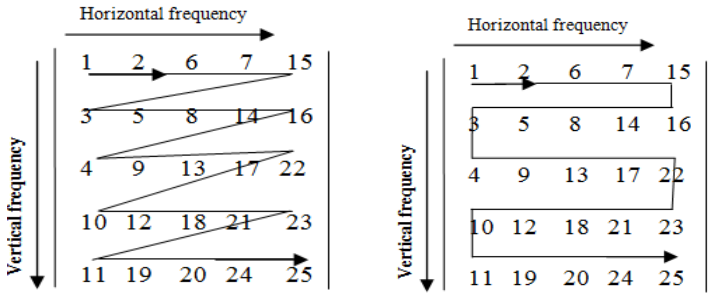
| MORSE PATTERN |
|---|
| .- |
| .. |
| -. |
| -- |

**Figure 1:** Modified Morse pattern.

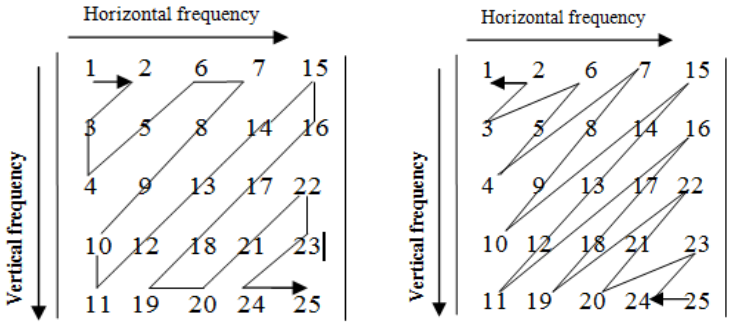
### Zigzag Pattern

The matrix structure of the $N^2$ integers which would increase sequentially along the arrays anti-diagonally is called Zigzag pattern. The different kind of zigzag patterns is shown in the Fig.1. A motive wave that travels on parallel trend is known as parallel zigzag pattern refer fig.2 (a). The motive wave that travels on diagonal trend is known as diagonal zigzag pattern refer fig.2. (b).

The proposed method is based on the parallel zigzag encryption pattern refer fig.2 (a).




(a).Parallel Pattern.




(b).Diagonal Pattern.

**Figure 2:** Various Zigzag patterns.

**Encryption Phase**

The biological information of living organism is basic of cryptographic algorithm. The encryption process is based on DNA sequence and Modified Morse code.

The sensitive data is stored at cloud environment by cloud user. The location of data is unknown by user. The original data is encrypted into cipher text by using modified Morse code and parallel Zigzag pattern. The decryption algorithm is shown below,

**Algorithm 1: Parallel Zigzag Encryption**

**Input: Original data**
**Output: Encrypted data**

```
1.   begin
2.     N ← no_of_chars;
3.     //Convert text to Binary sequence using algorithm 3.1
4.     for i = 1 to N do
5.       Read original[i];
6.       Binary[i] ← Text_to_Binary (original[i]);
7.     endfor
8.     //Convert binary to DNA sequence using algorithm 3.2
9.     for i = 1 to N do
10.  DNA[i] ← Binary_to_DNA(Binary[i]);
11.    endfor
12.    //Convert DNA sequence to modified Morse pattern using algorithm 3.3
13.    for i = 1 to N do
14.      MSE[i] ← DNA_to_Morse(DNA[i]);
15.    endfor
16.    st1 ←MSE;
17.    size←take the nearest next integer of (Math.Sqrt (st1.length());
18.     //Adding * for empty places of matrix
19.    for each i ranging from 1 to size
20.      for each j ranging from 1 to size
21.        if (pos<(string.len())
22.          matrix [i][j] ← st1.charAt(pos)+st1.charAt(pos+1);
23.        else
24.          matrix[i][j] ← **;
25.        endif
26.      endfor
27.    endfor
27.    //Arrangement of Morse code to Parallel Zigzag pattern
28.    k=1;
29.    for i = 1 to size do;
30.      if i mod 2 = 1 then
31.        for j = 1 to size do;
32.          PZigzag[k++] ← matrix[i][j];
33.      else
34.        for j = size to 1 step -1 do;
35.          PZigzag[k++] ← matrix[i][j];
36.        endfor
37.      endfor
38.    endif
39.  endfor
40. end
```

In the encryption phase the sensitive data is encrypted into cipher text. The original data is converted into binary data in the steps 4-6 and stored in the variable Binary[i]. The binary data is converted into DNA sequenced data and stored in DNA[i] in the steps 7-9. The DNA sequenced data is converted into modified Morse pattern and stored in variable matrix[i] [j], the modified Morse code data is converted into Parallel zigzag pattern in the steps 10-16. The Encrypted data is stored in the variable PZigzag[i].

**Example**

Step1:Consider the plaintext is, "SEARCH".

Step2:The above plaintext is converted to binary text using binary sequence 0's and 1's.
01110110110010101100001011100100110001101101000.

Step3:The binary sequence data is converted into DNA sequence data. The transformation operation is actually an XNOR of the DNA sequence data with intron sequence.

T A T C G C CC G A C C T A G C G A T C G G A

Step4: The converted DNA sequence is encrypted into modified Morse pattern and stored in the matrix.

-.-. - .- - -.-. --. -.-. -.-. -.-. --. .- -.-. -.-. - .- --. -.-. --. .- - -.-. --. --. .-

```
-.-.  -  .-  -  -.-.
--. --. -.-. -.-. -.-.
--.  .-  -.-.  -.- .
```

Step5: The modified Morse sequence data is converted into Parallel Zigzag pattern which is shown below,

-.-. - --. .- -.-. .- - --. -.-. --. -.-. -.-. -.-. -.-. -.-. -.-. --. - --. --. --. .- .- - .- *

Step6: The encrypted data is called as cipher text.

A rough calculation of number of steps used to execute an algorithm is known as time complexity of the algorithm. It is commonly represented with the O (n) notation where n is the size of input file. The DNA conversion with Morse code function from line number 3-11 has no nested loop. So the time complexity will be O (n). The function Convert to Morse Pattern from line 13-20 has nested loops. So the time complexity will be O ($n^2$).

```
-  -.-.  --.  --.  .-
-  -.-.  --.  --.  .-
.-  --.  -.-.  --.  .-
```

**3.4 Decryption Phase**

The decryption process is a reversal process of encryption phase. In the decryption process the parallel zigzag data is converted into modified Morse pattern. The modified Morse sequence data is converted into DNA data. The following algorithm 2 is used to decrypt the encrypted data into original data.

**Algorithm 2: Decryption**
**Input: Encrypted data**
**Output: Original data**

```
1.  begin
2.  //Arrangement of Parallel Zigzag pattern to single line Morse d
3.      Load PZigzag[i];
4.      L=1;
5.      for i = 1 to size do;
6.        for j=1 to size do;
7.          matrix[i][j]  ← PZigzag[L];
8.        endfor
9.      endfor
10.  Convert Modified Morse to DNA sequence using algorithm 3.4
11.  Convert DNA sequence to Binary using algorithm 3.5
12.  Convert Binary to original text using algorithm 3.6
13. end;
```

The decryption process embraces of following steps for decryption of encrypted text. Decryption process starts with Parallel Zigzag sequence data which is from encryption process. The decryption process is based on the above algorithm.

**Example**

Step1: The encrypted text of file is,

-.-. - --. .- -.-. .- - --. -.-. --. -.-. -.-. -.-. -.-. -.-. -.-. -.-. --. - --. --. --. .- .- - .- *

Step2: The encrypted data is converted to modified Morse sequence, and stored in matrix as shown below,

```
-.-.  -  --. .-  -.-.
.-  -  --.  -.- . --.
-.-. -.-. -.-. -.-. -.-.
-.-.  --.  -  --.  -
--.  --.  .--  .-  *
```

Step3: The modified Morse sequence is now converted into DNA sequenced data using ACGT sequences based on base pair rule.

T A T C G C CC G A C C T A G C G A T C G G A

Step4: The above DNA sequence is again decrypted into binary sequence to decrypt the data to binary sequence.

01110011011001010110000101110010011000110110100 0

Step5: Finally, The binary sequence data is converted into original data.

"SEARCH".

The convert to matrix function from line 4-6 has nested loop. So the time complexity will be O ($n^2$). Convert modified Morse pattern to DNA sequence function from line 6-8, Convert DNA sequence to binary sequence function from line 9-11 and Convert Binary sequence to original text function from line 12-15 have no nested loop. So the time complexity will be O (n).

## IMPLEMENTATION AND RESULT

The proposed algorithm is implemented in Windows XP Platform using Netbeans 8.1. The DNA sequence, modified Morse code and Zigzag pattern are used for encryption and decryption process. The accuracy of the proposed algorithm is verified using some of online tools. The tools are listed in the below table1.

**Table1:** Online Encryption Tools.

| S. No | Encryption Tools | Website Address |
|---|---|---|
| 1 | Encrypt & Decrypt Text online-toolz | http://encryption.online-toolz.com/tools/text-encryption-decryption.php |
| 2 | Tools 4 noobs | https://www.tools4noobs.com/online_tools/decrypt |
| 3 | Online Domain Tools | http://online-domain-tools.com/ |
| 4 | AES Encryption Decryption online tool | https://www.online-tools/aes-encryption-decryption |
| 5 | Online domain tools | http://online-domain-tools.com/ |

The original data is stored in the file original.txt. The original data is encrypted by DNA sequence, modified Morse pattern and Parallel Zigzag. To verify the accuracy of proposed algorithm 300 samples are tested. The comparison of encrypted data and decrypted data are done using online tool DiffNow [25] and accuracy of data is proved.

### Brute Force Attack

A process of searching key to decrypt the encrypted data is called Brute force attack. Here the attacker checks for all the possible keys to get original data. The DNA sequence and modified Morse codes are used to convert the data to encrypt the data refer Fig.2. Finding original data in bio-molecular environment is very difficult task. If hacker tries to get original file with incorrect key code, it will cause pollution of data which would lead to corruption of data.

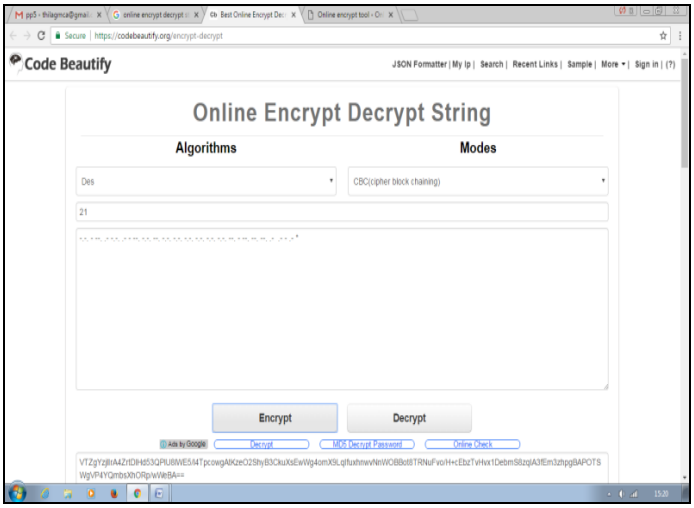



**Figure 2.** Failed attack on Encrypted data.

### Differential Attack

A small change to the sensitive data is made and the hacker tries to get the original data is called differential attack. The DNA sequence and Parallel Zigzag pattern are used to encrypt the original data. So finding original data is not an easy task by the hacker. If hacker tries to get sensitive data using wrong key will corrupt the original data refer fig.3.

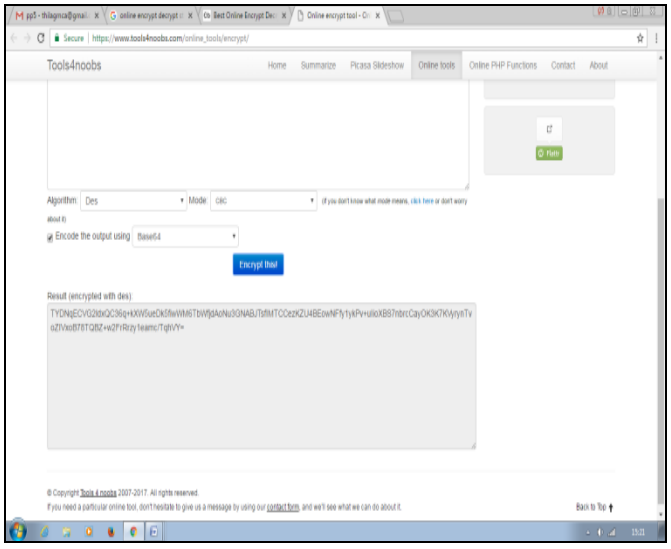



**Figure 3:** Failed attack on Encrypted data.

### Chosen/Known Plain Text Attack

The known/chosen plain text attack is trying to access original data from choosing a set of known plain text. The DNA sequences are used to encrypt sensitive data and convert it is converted to modified Morse pattern. The modified Morse pattern data is again converted to the Parallel Zigzag pattern to change original data. So finding original data through chosen/Known plain text is not an easy task by the hacker which is shown in Fig.4.

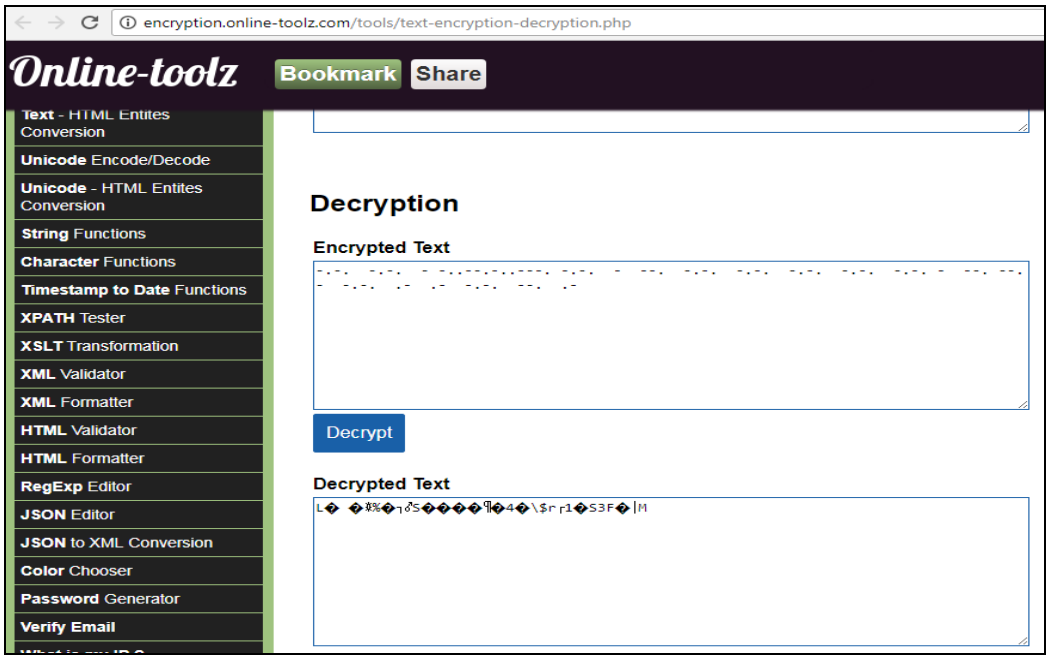



**Figure.4:** Failed attack on Encrypted data.

## CONCLUSION AND FUTURE WORK

Cloud Computing empower companies to use cloud resources at any time without a limit. The sensitive data is transmitted and stored in the cloud environment at lower cost. However, the extensiveness of cloud is hurt by its security challenges. To upgrade the security of cloud computing environment the new model has been proposed. The proposed security model is based on DNA computing. So finding original data is difficult with the existing encryption model and now the Parallel Zigzag pattern is added to tighten the security model. In the future, one can use the proposed model to transmit picture, audio and video data to cloud environment.

## REFERENCES

[1] Lizhe,W., Jie Tao, Kunze,M., Castellanos, A.C., Kramer, D., Karl, W.: Scientific Cloud Computing: Early Definition and Experience. In HPCC, Vol. 8. (2008) 825-830

[2] Paul, P.K., Ghose,M.K.: Cloud computing: possibilities, challenges and opportunities with special reference to its emerging need in the academic and working area of Information Science. In Procedia Engineering, Vol. (23) (2012) 2222-2227

[3] Kandukuri, Balachandra Reddy, Atanu Rakshit: Cloud security issues. In Services Computing, 2009. SCC'09. IEEE International Conference on IEEE, (2009) 517-520

[4] Rachna, A., Anshu, P.: Maintaining Data Confidentiality and Security over Cloud: An Overview. International Journal of Engineering Research and Applications (IJERA), Vol. (4). (2013) 1922-1926

[5] Adleman, L.: Molecular computation of solutions to combinational problems. American Association for the Advancement of Science, (1994) 1021-1024

[6] Sureshraj, D., Murali Bhaskaran, V.: Automatic DNA Sequence Generation for Secured Effective Multi-Cloud Storage. Journal of Computer Engineering (IOSR-JCE), Vol.15. (2013) 86-94

[7] Thilagavathy, R., Murugan, A.: Cloud Computing: A Survey on Security Issues and DNA, ID-base Cryptography. Indian Journal of Science and Technology (INDJST), Vol.9 (28). (2016) 1-6

[8] Borda, Monica, Olga, T.: DNA secret writing Techniques. In IEEE conferences, (2010) 451-456

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

[10] Che Jianhua, Yamin Duan, Tao Zhang, Jie Fan,: Study on the security models and strategies of cloud computing. In Procedia Engineering, Vol. (23). (2011) 586-593

[11] Legrand, A., Marchal, L., Casanova, H.: Scheduling distributed applications: The simgrid simulation framework IEEE, (2003) 138-145

[12] Dubey, 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 on, IEEE (2012)

[13] Thilagavathy, R., Murugan, A.: Secure the Cloud Data Transmission Using an Improved RSA Algorithm.

Indian Journal of Science and Technology (INDJST), Vol.10 (12). (2017) 1-6

[14] https://en.wikipedia.org/wikiMorse_code

[15] Honey, M., Sanjay, S., Aarti, M.: Optical character recognition (OCR) system for Roman script & English language using Artificial Neural Network (ANN) classifier. Research Advances in Integrated Navigation Systems (RAINS) International Conference on, (2016) 1-5

[16] Jacob Grasha, Murugan, A.: An Encryption Scheme with DNA Technology and JPEG Zigzag Coding for Secure Transmission of Images, arXiv preprint arXiv, (2013) 1305.1270

[17] Annalakshmi, Mu., Padmapriya, A.: Zigzag Ciphers: A Novel Transposition Method. International Journal of Computer Applications, Vol.3 (7). (2013) 8-12

[18] Murugan, A.,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. (2017) 226-231

[19] M.Amos, G.Paun, and G. Rozenberg,"Topics in the theory of DNA Computing:, Theoritical Computer Science 2002, 287,3-38

[20] C. Chelland, V.Risca, C.Bancroft,"Hiding messages in DNA microdots", Nature 1999, 399:533-534

[21] J. Chen,"A DNA-based, biomoleccular cryptography design," in IEEE International Symposium on Circuits and System (ISCAS),2003,822-825

[22] G.Z. Cui, L.M Qin, and Y.F. Wang," An Encryption scheme using DNA Technology",Computer Engineering and applications,(2008),37-42

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

[24] Jacob Grasha, Murugan, A.: A Hybrid Encryption Scheme using DNA Technology. The International Journal of Computer Science and Communication Security (IJCSCS), Vol. 3 (2), (2013) 61-65

[25] Comparison of two files done using online tool address: https://www.diffnow.com/