DrillBit

The Report is Generated by DrillBit Plagiarism Detection Software

Submission Information

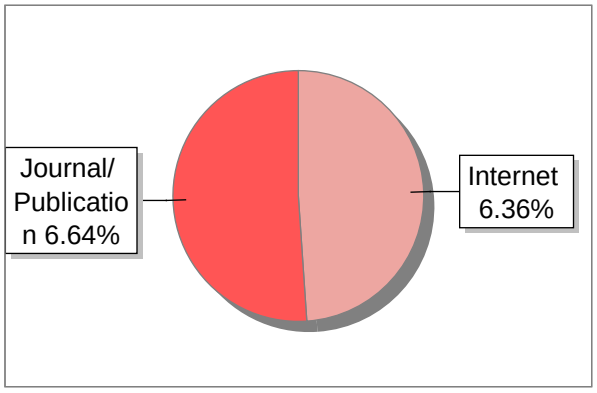
Author Name	Pranjali S
Title	A biometrics based safe system for encryption
Paper/Submission ID	748206
Submission Date	2023-05-22 11:37:34
Total Pages	6
Document type	Research Paper

Result Information

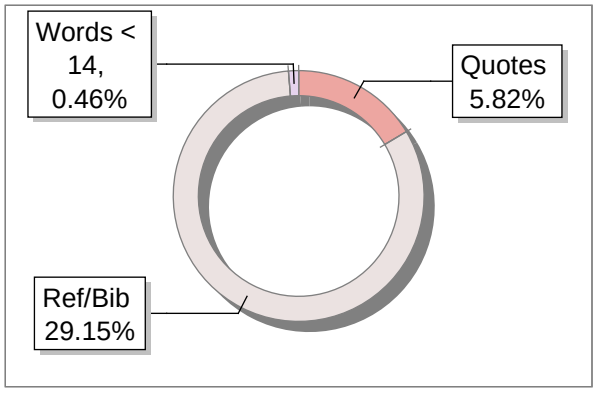
Similarity **13 %**

1 10 20 30 40 50 60 70 80 90

Sources Type



Report Content



Exclude Information

Quotes	Excluded
References/Bibliography	Not Excluded
Sources: Less than 14 Words Similarity	Not Excluded
Excluded Source	**0 %**
Excluded Phrases	Not Excluded

A Unique QR Code use to View/Download/Share Pdf File

DrillBit

DrillBit Similarity Report

13	16	B
SIMILARITY %	MATCHED SOURCES	GRADE

A-Satisfactory (0-10%)
B-Upgrade (11-40%)
C-Poor (41-60%)
D-Unacceptable (61-100%)

LOCATION	MATCHED DOMAIN	%	SOURCE TYPE
1	pdfs.semanticscholar.org	3	Publication
2	www.researchgate.net	3	Internet Data
3	docplayer.net	1	Internet Data
4	Thesis Submitted to Shodhganga Repository	1	Publication
5	ijece.iaescore.com	1	Publication
6	hict.edu.vn	1	Internet Data
7	docplayer.net	1	Internet Data
8	www.freepatentsonline.com	<1	Internet Data
9	www.comsoc.org	<1	Internet Data
10	dsatm.edu.in	<1	Publication
11	Software Defined Wireless Networking Opportunities and Challenges for by Sood-215	<1	Publication
12	Thesis Submitted to Shodhganga Repository	<1	Publication
13	moam.info	<1	Internet Data

14	Alleviating Heterogeneity in SDN-IoT Networks to Maintain QoS and Enha by Sood-2019	<1	Publication
15	biomedcentral.com	<1	Internet Data
16	DOPIV Post-quantum Secure Identity-based Data Outsourcing with Public by Zhang-2019	<1	Publication

A Biometrics based safe system for encryption

[1]Srividya Ramisetty,[2]Pranjali S,[3]S Disha Adiga,[4]Vani B Telagade,
CMR Institute of Technology Bengaluru, India
[1] srividya.ramisetty@gmail.com ,[2] spranjali2001@gmail.com ,[3]dishasaligrama@gmail.com, [4] vanibtelagade1236@gmail.com

***Abstract*—As technology continues to advance, data has become an increasingly important element in the field of Information Technology. However, the large volume of data generated by devices presents a major challenge in handling it in real time. Data encryption is a crucial component in ensuring data privacy and security during transmission and processing. Unfortunately, many applications disregard data encryption in order to achieve higher performance. This paper proposes a solution to this problem by introducing a novel data encryption approach called the Dynamic Data Encryption Strategy (DDES) and Deoxyribonucleic Acid(DNA) computing, a revolutionary cryptographic method that might improve information security by preventing unauthorised access to sensitive data, could be used. Information security is improved by the DNA symmetric cryptography being suggested. The outcomes show that plain-text encryption is a very secure procedure. . The DDES approach is designed to improve privacy protection within the constraints of real-time processing. By implementing the DDES approach, data privacy and security can be significantly enhanced without compromising performance.**

I. Introduction

The Internet has connected the world like never before, and mobile computing will be the future of technology as it allows us to access the Internet and data on-the-go. Mobile cloud computing techniques have enabled diverse applications, but concerns remain about data security and privacy. Among the key privacy concerns is caused by unencrypted data transmissions since the large volume of data. This can result in privacy leakage issues, as plaintext data is easily captured by adversaries through methods namely jamming, monitoring, and spoofing. To address this problem, this paper proposes the use of a Dynamic Data Encryption Strategy (DDES) model, This is intended to safeguard the privacy of data owners using applicable devices and networking facilities. Fig 1 Depicts the Cloud computing in simple understandable way.

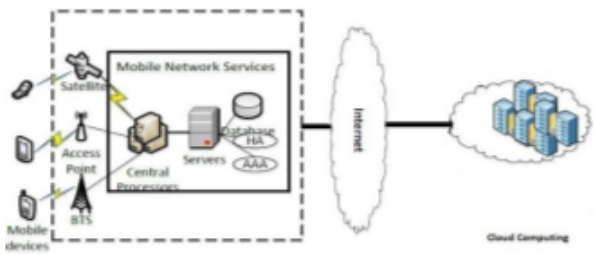


Fig. 1: Cloud Computing

The DDES model includes two crucial terms for implementing the data encryption strategy: Paired Data and Pairs Matching Collision. Additionally, two crucial algorithms, the Weight Modularization (WM) Algorithm and S Table Generation (STG) Algorithm, are proposed to support the implementation of the DED algorithm. These two new algorithms further identify the methods of identifying privacy values when making a determination on encrypting the input data. The primary benefits of work are threefold: First, the proposed approach selectively encrypts data packages to maximize the degree of privacy protection in huge data under time constraints. Two working modes are considered when creating the transmission strategy, including encryption and non-encryption modes. Second, the proposed algorithm offers an optimal solution providing the maximum value of total privacy weights. Two involved constraints are execution time and privacy levels. Third, the results of this study offer big data-based options using an adaptive transmission strategy that prioritises privacy protection..

Many scientists in numerous domains have used DNA computing to offer protection for the enormous quantity of data depicted in figure 2 by performing DNA computing. The term "DNA-BASED cryptographic approaches" refers to a variety of cryptographic techniques. DNA computing also acquired certain desirable qualities in its work, such as large storage capacity, maximum energy efficiency, and high parallelism, which is highly advantageous for idea of data concealing. The programme may offer a remedy for clustering, forecasting, and optimisation issues in addition for signal processing. 108 TB of data might fit into one gramme of DNA. The equivalent DNA base number is 1021.

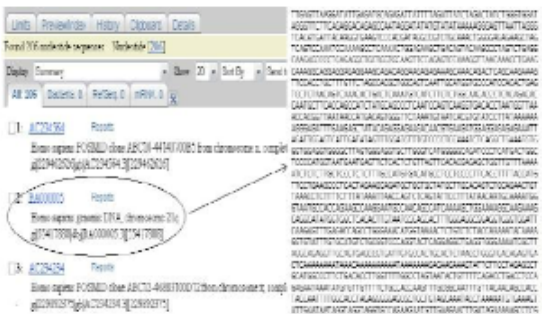


Fig 2: Chromosomal Sequences from a Genetic Database

The following is what this document aims to provide:

- To provide a comparative analysis of several DNA cryptography methods.

- To provide a strong ciphertext using the improved cryptographic technique.
- To provide cutting-edge data concealing techniques with the improved strategy.

Deoxyribonucleic Acid

The natural mega particle known as DNA (Deoxyribonucleic Acid), which is created when nucleotides combine, is the source plasma of all living things. Deoxyribonucleotides are supposedly thought of as the DNA monomer unit. DNA has four different kinds of nucleotides bases, including

- Adenine (A),
- Cytosine (C),
- Thymine (T), and
- Guanine (G)

The DNA has two nitrogen bases: 1. Purines Pyrimidines, second. The single ring molecules, which have the bases C and T, are referred to as pyrimidines whereas the double ring molecules, A and G, are believed to be purines. The vast industries that might be used for picture and data encryption, data concealment, steganography, etc. may be identified using DNA's capabilities. While performing DNA operations in various laboratories, consideration ought to be supplied to a number of factors, including temperature, pressure, oxygen ratio, etc. (identical conditions of a number of parameters should be maintained).

Given that the DNA is a sensitive module, this might have a variety of outputs depending on the surroundings. Consequently, it may be claimed that the environmental factors depicted in figure 3 completely determine how DNA computations are performed. The term "binary coding scheme" refers to binary conversion of the DNA sequence. In this study, the binary values 00, 11, 01, and 10 were represented by DNA bases A, T, C, and G. For instance, the binary sequence for the DNA sequence "AATCGGAT" is 0000110110100011. The major bases of RNA (ribonucleic acid) are same as in DNA, with the exception that Uracil (U) is used instead of thymine (T).

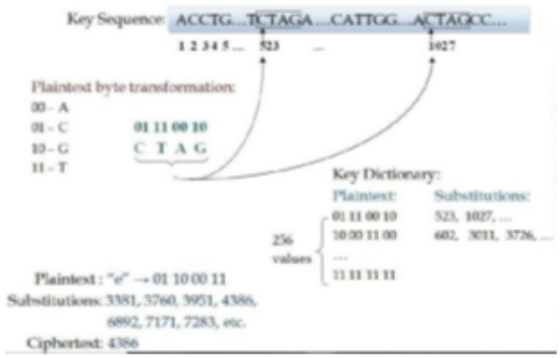


Fig 3: DNA Indexing Algorithm's encryption process

Overall, this paper proposes a novel and effective approach for safeguarding privacy in mobile cloud computing. By implementing the DNA cloud computing, data privacy and security can be significantly enhanced without compromising performance.

II. LITERATURE SURVEY

Many applications disregard data encryption to achieve compliance. This work expresses privacy concerns about data and proposes Dynamic Data Encryption Strategy (DDES), a revolutionary data encryption method. The goal of this addition is to broaden the breadth of privacy protection while minimising time limitations[1].

Numerous cutting-edge applications in Cyber-Physical Systems (CPSs), such as Intelligent Transportation Systems (ITSs), are being driven by the anticipated enhanced network explorations and the rising need for mobile data sharing and transferring. However, the tensions between security and communication effectiveness limit the use of ITS today. The SecurityAware Efficient Data Sharing and Transferring (SA-EAST) paradigm, which is intended for safeguarding cloud-based ITS deployments, is proposed in this article as a solution to this problem. We want to achieve safe real-time multimedia data sharing and transferring by using this method. Our experimental assessment has demonstrated that our suggested paradigm performs well at safeguarding communications for ITS[3].

In the data from fusion reactors, a brand-new technique and its application for real-time blobfilament detection and tracking are provided. Numerous additional uses, such as ignition kernels in combustion and tumour cells in a diagnostic picture, depend on similar temporal properties. The method for obtaining these characteristics is presented in this study by breaking down the total process into three steps: local feature cell verification, grouping feature cells into extended characteristics, and monitoring feature motion through spatial overlaying. [4]

DDoS attack source traceback is an unsolved and difficult issue. A straightforward and efficient traceback approach is deterministic packet marking (DPM), however existing DPM-based traceback schemes are impractical because of their scaling limitations. The fact that just a few computers and routers are participating in an assault session is something we discovered. Therefore, instead of designating every Internet node as the current techniques do, we simply need to label specific involved nodes for traceback purposes. We suggest a novel marking on demand (MOD) traceback approach based on the DPM mechanism in light of this discovery. We must use the conventional DPM method to designate these implicated ingress routers to be able to identify the involved attack source.[5]

The idea of DNA computing has gave a way to development of several algorithms. In the past 20 years, DNA computing has been used to tackle challenging problems like SAT and DES. DNA computing has been used by Lipton [6] to solve the NP-complete SAT problem. He also developed a DNA-based encoding system, and the author used the fewest possible variables to answer the SAT issue. Data Encryption

Standard (DES) cracking was proposed by Boneh et al [7] using DNA computing. With their suggested approach, every cryptosystem might be broken with a key size of only 64 bits or less. Additionally, its encryption circuit is compact and could be broken in 916 steps. Each phase is equivalent to 32 extractions, and processing takes a minimum of one entire day each of the 10 extractor stages. To break DES using their suggested technique would take at least four months. The DNA computing approaches developed by Chen et al. [8] might be used to address challenging problems. With the use of DNA technology, they also cracked DES. The predicted algorithm by Chen et al. has three different functions: 1) The key space should be initialised with every possible using the initial function. 2) The encryption procedure; and 3) Finding the appropriate related key. The molecular sticker algorithm also includes tubes and short memory strands.

Symmetric-key MingXin et al. [9] proposed the DNA cryptosystem, which incorporates DNA biotechnology with cryptography techniques. This technique for encryption and decryption was developed with the use of DNA probes, and the ciphertext was then included into the DNA chip (microarray). The development of DNA chips results in the method's privacy. A suggested approach for the effective, dependable, and secure transfer of data was recently made by Kar et al. [10]. The method makes use of DNA keys, which comprised three keys: two for encryption and one for communicating the encryption key to the recipient. In this approach, the text itself will be transformed to binary sequence through a process called string to binary transformation.

The massive DNA pattern is converted to binary data using binary coding algorithm as the encryption key. Performing XOR and adding procedures to the 64-bit raw and 64-bit key would provide the ciphertext. Shiu et al. has made several cryptographic technique suggestions [11]. The following are the cryptographic methods that employ the DNA method: a) Insertion technique Methods two and three are replacement and complementing pair. They also demonstrated that the replacement strategy is more effective than the other two. By encrypting ciphertext in a word file with the DNA sequence, Liu et al. [12] put out a data concealing technique. Their approach turns the plaintext into a DNA sequence by using DNA coding. Chebyshev maps construct one time key using the desired DNA sequence key and two pseudorandom DNA sequences, XXOR and YPrimer. The YPrimer and the XXOR are included in the output, respectively, for the DNA messaging sequence. They might be turned into ciphertext by using the shift procedures on the result that had been generated earlier. Following the encryption of the ciphertext into the word file, the word file might be transformed to PDF. The created PDF will be delivered to the recipient. Mandge et al. [13] had suggested a powerful ciphertext method that combined key generation technology with matrix insertion modification in the encryption process. The several shifting and XOR operations will first turn the plaintext into a mini-cipher. It is claimed that because this procedure incorporates safe key creation, if it were applied to plaintext each time, we might acquire different miniciphers for the same plaintext. After using number of biotechnologies, including DNA primers, to transform this minicipher into a final ciphertext. The table lookup substitution method (TLSM), put out by Taur et al. [14], has improved the substitution approach using the single bit complementary rule of Shiu et al. They expanded to include the replacement method's two bits complementing rule. TLSM, which makes use of lookup tables [15][16], converts the two-bit message to the matching letter. Shiu et al.'s rule, contrasted with, could only translate one bit at a time. Additionally, the TLSM technique uses highly good ciphertext compression [17].

III. SYSTEM ANALYSIS

For cloud-based Cyber Physical Social Systems (CPSS), Zhang et al. presented a technique called SCLPV to fend off nefarious auditors. This method simultaneously provided resilience to malevolent audits and certificateless open validation to check accuracy of outsourcing data in CPSS. Wang et al. concentrated on creating a method enabling a secure cloud system that could facilitate public audits while protecting privacy. The approach of defining adversaries from the data storage side was investigated this paper study. Although consumers attempted to link via gadgets, one piece of work built up a two-dimensional paired connections over the Radio Frequency for Consumer Electronics (FR4CE) for both devices and gadgets. User-machine interface problems were also covered in a separate investigation, albeit from an entirely distinct perspective. The approach of defining adversaries from the data storage side was investigated in this paper study. Although consumers attempted to link via gadgets, one piece of work built up a two-dimensional paired connections over the Radio Frequency for Consumer Electronics (FR4CE) for both devices and gadgets. User-machine interface problems were also covered in a separate investigation, albeit from an entirely distinct perspective. developed an investigative strategy that concentrated on the weaknesses brought on by the abuse of Graphical User Interface (GUI) elements. In the setting of Ui-based applications, this strategy took abuses of GUI element properties into account. Building a safe finding engine in the setting of huge data requires an effective technique for determining if confidentiality agreements are being followed. The absence of ability to monitor in internet browsers might cause privacy problems because the latest platforms do not allow for surveillance of enemies. The pace at which threats are amplified can also be decreased with an effective safe networking infrastructure. Nevertheless, despite the creation of a variety of access control models, there are numerous flaws. created text document. You may now utilise the scroll to customise your document.

IV. CONCEPTS AND PROPOSED APPROACHES

The following section shows the concepts and proposed implementation clearly the algorithm used with their diagrams

Phase1: Encryption of Secret Data Algorithm for Encryption:

Step one: Convert binary data to DNA sequences.

A=00,

T=01,

C=10, and

G=11.

Step two: Complementary pair rule.

Complementary pair rule is a unique equivalent pair which is assigned to every nucleotides base pair.

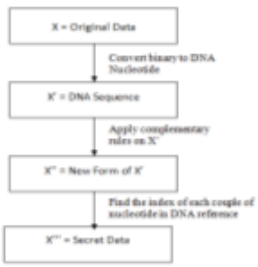
In this implementation, the admin assigns a unique DNA sequence and a unique key to every user which is later used to create the DNA reference sequence for the user using rand() function and hash set constructs.

Algorithm 1: Encryption Process

Input: File,
Output: Reference Sequence in Hexadecimal format
Start :

1. Let X be the Data
2. Convert Binary to DNA Nucleotides
3. Apply Complementary Rules on M'
4. Find Index of each Couple of Nucleotides in DNA References Sequence X''
5. Reference Sequence in Hexadecimal format is generated and this is called Secret Data X'''

Stop



The customer chooses to send the original information X to cloud computing settings across the internet. To offer the ultimate version of X, which is X'", and upload to the internet, there are 3 channel-phases. The data X is translated into binary form after it has been read as an integers.

The base pairing rules must be used to be able to translate binary information into amino acids represented as the sequence of DNA. In the actual world of biology, nucleotide synthesis follows set guidelines.

Phase2: Extracting Original data

Client2 uses certain integers to represent the secret data. Phase two and its associated subphases will retrieve the original data from the DNA reference sequence for that purpose.

Algorithm **2**: Decryption Process

Input : Reference Sequence in Hexadecimal format generated in the Encryption Process M'''
Output : Original Data
Start :

1. Find Index of each Couple of Nucleotides in DNA Reference Sequence
2. Apply Complementary Rules on M'
3. Convert Binary to DNA Nucleotides

Stop

While a user uploads a file from his local computer to a website, the file must first be forwarded to the DNA Encryption Service, which runs on a cloud server 1. Cloud server 1 will encrypt the file, and cloud the computer 1 has to transmit the encrypted file to cloud server 2, using the internet service notion, where it will be stored.

Algorithm for Decryption:

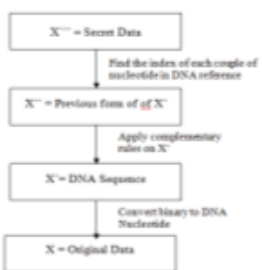
Step One: Convert numeric data to DNA sequences.

We extract the couple nucleotides in DNA reference sequence according to the index read from the file.

Step two: Complementary pair rule.

Complementary pair rule is a unique equivalent pair which is assigned to every nucleotides base pair.

Step three: Convert DNA sequences to binary data.



When the user is downloading a file from the web server the corresponding file has to fetch from cloud server 2 and it will send to DNA decryption service which is running in cloud server 1. Once the file is decrypted it shall be downloaded to the user machine [1].

V. Experimental Results

We have developed a website which enables the user give the input in form of a file. The contents of file is read and if any sensitive information is detected the file shall be encrypted .The uploaded file is split into blocks irrespective of whether it is sensitive or not and is uploaded to the FTP cloud server. Fig 4 depicts the results of DNA Encryption and DNA Decryption.

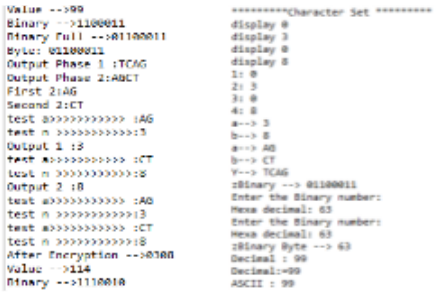


Fig 4: Results of DNA Encryption and DNA Decryption

In conclusion, our DNA cryptography performed better in many testing conditions. The results of our study satisfied our planning criteria and agreed with the predicted outcomes in theory. The dimensions used in practical assessments will be the subject of a subsequent study.

VI. CONCLUSION

Big data concerns regarding privacy were the sole subject of this essay, which also took into account actual cloud computing deployments. DDES, the suggested solution, was created to boost the effectiveness of privacy measures. The DED algorithm, which was created to provide alternate data packages for encryptions under varied scheduling limitations, was the main algorithm underlying the DDES paradigm. The results of the practical assessments demonstrated the suggested strategy's better and flexible efficacy.

References

[1] Sumit Vikram Tripathi , Ritukar 2, Prof. Murthy B3, Dr. K. S. Jagadish Gowda U.G. Student, Department of Computer Science & Engineering,Sri Krishna Institute of Technology, Bengaluru, India1 U.G. Student, Department of Computer Science & Engineering,Sri Krishna Institute of Technology, Bengaluru, India2 Assistant Professor, Department of Computer & Engineering,Sri Krishna Institute of Technology, Bengaluru, India3 Professor, Department of Computer & Engineering,Sri Krishna Institute of Technology, Bengaluru, India Privacy-Preserving Data Encryption Strategy for Big Data in Mobile Cloud Computing Environment

[2] Vikram, A., Kalaivani, S., & Gopinath, G. (2019). A Novel Encryption Algorithm based on DNA Cryptography. 2019 International Conference on Communication and Electronics Systems (ICCES). doi:10.1109/icces45898.2019.90023

[3] Gai, H. Zhao, M. Qiu, L. Qiu, and M. Chen. SA-EAST is an effective data transfer method for ITS in mobile heterogeneous cloud computing that is privacy conscious. 2017: 16(2):60, ACM Transactions on Embedded Computing Systems.

[4] A. Sim, M. Churchill, J. Choi, A. Stathopoulos, C. Chang, and S. Klasky are Wu, K. Wu, and other names. Blob-filaments in fusing plasma: approaching spatial characteristic tracing and immediate identification. 2016 issue of IEEE Transactions on Big Data.

[5] S. Guo, M. Guo, W. Zhou, and Yu. a workable architecture for IP traceback using dynamically stochastic session tagging. :1418–1427, IEEE Transactions on Computers, 2016.

[6] R.J. Lipton, "DNA solution of hard computational problems," Science, New Series, 268(5210), 542-545, 1995.

[7] D. Boneh, C. Dunworth, and R.J. Lipton, "Breaking DES Using a Molecular Computer," DIMACS workshop on DNA computing, 27, 37-51, 1995.

[8] Z. Chen, X. Geng, and J. Xu, "Efficient DNA Sticker Algorithms for DES." IEEE 3rd International Conference on Bio-Inspired Computing (BICTA), 15- 22, 2008.

[9] L. MingXin, L. XueJia, X. GuoZhen, and Q. Lei, "Symmetric-key cryptosystem with DNA technology," Science in China Series F: Information Sciences, 50(3), 324-333, 2007.

[10] N. kar, A. Majumder, A. Saha, A. Jamatia, K. Chakma, and M. C. Pal, "An Improved Data Security using DNA Sequencing," Proceedings of the 3rd ACM MobiHoc workshop on Pervasive wireless healthcare, 13-18, 2013.

[11] H.J. Shiu, K.L. Ng, J.F. Fang, R.C.T. Lee, and C.H. Huang, "Data hiding methods based upon DNA sequences," Information Sciences, 180, 2196-2208, 2010.

[12] H. Liu, D. Lin, A. Kadir, "A novel data hiding method based on deoxyribonucleic acid coding," Computers and Electrical Engineering, 39, 1164-1173, 2013.

[13] T. Mandge and V. Choudhary, "A DNA Encryption Technique Based on Matrix Manipulation and Secure key Generation Scheme," IEEE International conference on Information Communication and Embedded Systems (ICICES), 47-52, 2013.

[14] J.S. Taur, H.Y. Lin, H.L. Lee and C.W. Tao, "Data hiding in DNA sequences based on Table Lookup Substitution," International Journal of Innovative Computing, Information and Control, 8(10), 6585-6598, 2012.

[15] Y.H. Huang, C.C. Chang, C.Y. Wu, "A DNA-based data hiding technique with low modification rates," Multimedia Tools Applications, 1-13, 2012.

[16] M.R. Abbasy, P. Nikfard, A. Ordi, M.R.N. Torkaman, "DNA Base Data Hiding Algorithm," International Journal on New Computer Architectures and Their Applications (IJNCAA), 2(1), 183192, 2012.

[17] O. Tornea, M. Antonini, M. Borda, "Multimedia Data Compression and Encryption using DNA Cipher", Communications Department, Technical University of ClujNapoca, winner of 2nd Prize, album SSET 2013.

[18] W.M. Shih, J.D. Quispe, G.F. Joyce, "1.7-kilobase singlestranded DNA that folds into a nanoscale octahedron", Nature, Vol. 427, pp. 618-621, 2004.

[19] H. Shiu, K. Ng, J.F. Fang, et al., "Data hiding methods based upon DNA sequences", Elsevier Inc., pp. 2196–2208,2010.

[20] M. Reza Najaf Torkaman et al, "Innovative Approach to Improve Hybrid Cryptography by using DNA Steganography", IJNCAA 2012

[21] Zhihua Chen et el, "Efficient DNA Sticker Algorithms for DES", IEEE 3rd international conference on Bio-inspired computing, 2012

[22] A.P. Thiruthuvadoss, "Comparison and Performance Evaluation of Modern Cryptography and DNA Cryptography," M.S. Thesis, Royal Institute of Technology, 2012.

[23] G. Cui, L. Qin, Y. Wang, X. Zhang, "Information Security Technology Based on DNA Computing," International Workshop on Anti-counterfeiting, Security, Identification, 288-291, 2007

[24] M. Babaei, "A novel text and image encryption method based on chaos theory and DNA computing," Natural computing, 12(1), 101-

[25] SCLPV: Secure Certificateless Public Verification for Cloud-Based Cyber-Physical-Social Systems Against Malicious Auditors Yuan Zhang, Student Member, IEEE, ChunxiangXu, Member, IEEE, Shui Yu, Senior Member, IEEE, Hongwei Li, Member, IEEE, and Xiaojun Zhang.

[26] Privacy-Preserving Public Auditing for Secure Cloud Storage Cong Wang, Student Member, IEEE, Sherman S.-M. Chow, Qian Wang, Student Member, IEEE, KuiRen, Member, IEEE, and Wenjing Lou, Member, IEEE.