MPRI-JSD | INTERNATIONAL JOURNAL OF AFRICAN SUSTAINABLE DEVELOPMENT
VOL. 13 NO.2 MAR-2021 ISSN: 2760-4106

DNA COMPUTING BASED ON INFORMATION SECURITY TECHNOLOGY

OFUALAGBA MAMUYOVWI HELEN
Department Of Computer Science, Delta State Polytechnic, Otefe-Oghara, Delta State

Abstract
The world of information security looks in new directions to protect the data it transmits. Using DNA computing in the fields of cryptography, steganography and authentication has been identified as a possible technology that may bring forward a new hope for unbreakable algorithms. Computing is far from any kind of efficient use in today's security world. DNA authentication on the other hand has exhibited great promise with real world examples already surfacing on the marketplace today. DNA authentication practices will grow as the need for fool proof identification of individuals and items grows as well. This paper examine the concept of DNA computing and also improved security through information technology and to appreciate its benefits and challenges in our society today.

KEYWORDS: *DNA, computing, security, information and encryption*

Introduction

The world of encryption appears to be ever shrinking. Several years ago the thought of a 56 bit encryption technology seemed forever safe, but as mankind's collective computing power and knowledge increases, the safety of the world's encryption methods seems to disappear equally as fast. Mathematicians and physicists attempt to improve on encryption methods while staying within the confines of the technologies available to us.

INTERNATIONAL JOURNAL – ASD
VOL. 13 NO.2 MAR-2021 ISSN: 2760-4106

Existing encryption algorithms such as RSA have not yet been compromised but many fears the day may come when even this bastion of encryption will fall by the way side as have its predecessors. There is hope for new encryption algorithms on the horizon utilizing mathematical principles such as Quantum Theory however the science of our very genetic makeup is also showing promise for the information security world. The concepts of utilizing DNA computing in the field of data encryption and DNA authentication methods for thwarting the counterfeiting industry are subjects that have been surfacing in the media of late. How realistic are these concepts and is it feasible to see these technologies changing the security marketplace of today?

DNA computing is a branch of computing which uses DNA, biochemistry, and molecular biology hardware, instead of the traditional silicon-based computer technologies. Research and development in this area concerns theory, experiments, and applications of DNA computing. The term "molectronics" has sometimes been used, but this term had already been used for an earlier technology, a then unsuccessful rival of the first integrated circuits this term has also been used more generally, for molecular-scale electronic technology.

DNA computing is a form of parallel computing in that it takes advantage of the many different molecules of DNA to try many different possibilities at once. For certain specialized problems, DNA computers are faster and smaller than any other computer built so far. Furthermore, particular mathematical computations have been demonstrated to work on a DNA computer.

Related Work on DNA Computing

Gupta, G. (2013), noted. DNA computing or molecular computing are terms used to describe utilizing the inherent combinational properties of DNA for massively parallel computation. The idea is that with an appropriate setup and enough DNA, one can potentially solve huge mathematical problems by parallel search. Basically this means that you can attempt every solution to a given problem until you came across the right one through random calculation.

INTERNATIONAL JOURNAL – ASD
VOL. 13 NO.2 MAR-2021 ISSN: 2760-4106

Utilizing DNA for this type of computation can be much faster than utilizing a conventional computer, for which massive parallelism would require large amounts of hardware, not simply more DNA.

Adleman, L. (2013), noted a computer scientist at the University of Southern California was the first to pose the theory that the makeup of DNA and it's multitude of possible combining nucleotides could have application in brute force computational search techniques.

Friedman, Y. (2012), noted, Computers with undreamed of storage capacity will be needed to handle an "explosion" of genetic data in the next decade, experts have warned.

Computers with undreamed of storage capacity will be needed to handle an "explosion" of genetic data in the next decade, experts have warned. The amount of information packed into just a few molecules of DNA is enough to fill a whole computer hard drive.

Given the pace at which genetics is progressing, the amount of available genomic data will reach the "exobyte" scale - billions of gigabytes - by 2025, scientists predict. The US team compared the needs of genomics with those of three of the leading big data players today - astronomy, Twitter and YouTube.

Sharing and storing genomic data is highly complex because it assumes different formats, said the scientists. They estimate that the field of genomics has already produced data on the megabyte scale. A megabyte is a million gigabytes, while a gigabyte represents a billion bytes - individual units of digital information. By 2025, genomics was expected to be in the exobyte league, surpassing YouTube - the data storage title holder among the different domains studied. Blahere, K. (2007)

Professor G. (2012), director of the Carl R Woese Institute for Genomic Biology at the University of Illinois, said: "As genome-sequencing technologies improve and costs drop, we are expecting an explosion of genome sequencing that will cause a huge flood of data.

METHOD AND DISCUSSION

METHOD

The method used for this paper is to examine the different stages of information security in DNA computing e.g. DNA cryptography, DNA steganography, DNA authentication

INTERNATIONAL JOURNAL – ASD
VOL. 13 NO.2 MAR-2021 ISSN: 2760-4106

WHAT IS DNA COMPUTING

According to Wikipedia DNA computing is an emerging branch of computing which uses DNA, biochemistry, and molecular biology hardware, instead of the traditional electronic computing. Research and development in this area concerns theory, experiments, and applications of DNA computing.

Fig1: DNA Computing source: https://foglets.com/dna-computing/

DNA CRYPTOGRAPHY

Cryptography is the branch of science which deals with the encoding of information for the purpose of hiding messages. It plays a vital role in the infrastructure of communication security. DNA Cryptography is one of the rapidly evolving technologies in the world. Surprisingly, one gram of DNA contains 1021 DNA bases which is equivalent to 108 TB of data. Hence can store all the data in the world in a few milligrams.

DNA STEGANOGRAPHY

DNA steganography methodology was developed to hide messages in variable regions (single nucleotide polymorphisms) of the genome to create hidden messages and thereby prevent from hacking. Steganography works by changing bits of useless or bot used data in regular computer files

EDITOR-IN-CHIEF
Prof. A.I. Mteiye [MALAWI]

INTERNATIONAL JOURNAL – ASD
VOL. 13 NO.2 MAR-2021 ISSN: 2760-4106

(such as graphics, sound, text, HTML) with bits of different, invisible information. This hidden information can be plain text, cipher text, or even images.

DNA AUTHENTICATION

The biometric **authentication** technologies, typified by fingerprint, face recognition and iris scanning, have been making rapid progress. Among the various possible types of biometric personal identification system, deoxyribonucleic acid (**DNA**) provides the most reliable personal identification.

The basic steps of **DNA** profiling include: Isolate the **DNA** (sample can originate from blood, saliva, hair, semen, or tissue) Section the **DNA** sample into shorter segments containing known variable number tandem repeats (VNTRs)—identical repeat sequences of **DNA**.

FIG2: Types of biometrics: source:https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics

CONCLUSION

The world of information security technology is always on the lookout for unbreakable encryption to protect the data that we transmit but it appears that every encryption technology meets its endgame as the computing technology of our world evolves. DNA computing methods on the other hand have shown great promise in the marketplace of today and it is hoped that its applications will continue, The beauty of both these DNA computing

research trends is found in the possibility of mankind's utilization of its very life building blocks to solve its most difficult problems. and the use of DNA computing with a greater security focus other than in merchandise authentication methods is a long way off.

REFERENCE

Ashiq JA (2015) DNA Cryptography and Information Security April 1, 2015 Received 2021-3-13

Adleman, L. (2013), "Molecular computation of solutions to combinatorial problems". Science 266, 1021-1024. November 11, 1994

Blahere, K. (2007), "DNA Computing". CNET. April 26, 2007. Received 2021-02-13

Friedman, Y. (2012)"DNA Based Computers". Retrieved March 20.2016

Gehani, A. (2011), La Bean, Thomas H. Reif, John H. "DNA-Based Cryptography". Department of Computer Science, Duke University. June 1999, Received 2020-11-17.

Gupta.G (2013) "DNA Computing".TheIndian Programmer. June 12, 2001. Received 2020-11-17

Professor G.(2012) "Algorithmic Self-Assembly of DNA Tiles and its Application of Cryptanalysis". October 2, 20001.Received 2017-3-13

Peterson, I. (2012), "Hiding in DNA".Science News Online. April 8, 2000. Received 2021-3-13