International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 03 | Mar 2020 www.irjet.net p-ISSN: 2395-0072

A SECURE AMR STGANOGRAPHY SCHEME BASED ON PULSE DISTRIBUTION MODEL USING DNA SEQUENCE

Dinesh Kumar M[1], Elanthiraiyan E[2], Hari Baskaran M[3], Nagarathinam N[4]

[1,2,3,4]UG Student, Department of information Technology, SRM Valliammai Engineering college, Kattankulathur, Tamil Nadu, India.

Abstract - *A steganography is basically used for hiding the data in the information or message or image or video e.t.c.. It should be used to sends the information without any cracking probability occurs to breach the receiver to reached for it. This project is basically used for many algorithms and methods that should be discriminating the function that provides more security source that should be iterated through it. By using DNA sequence algorithm that is used for the complementary rules and substitution method to provoke fake DNA sequence message that should be generated to it. They have been used to display the message with instead of using the creation of color palatte can be used for the each pair of code message. For each color that specifies to generating the key by using the RSA algorithm by containing to process alphabetical numeric characters and symbols e.t.c. the key size should be very large for instead by using the message. The concept of the binary coding rule and the extraction of the hybrid method will generate the required plain text. The hybrid method uses the concept of the substitution and the complementary pair rule. Finally the output of the module is obtained as the plain text.so the original message should be finally received to the receiver.*

Key Words: color palatte. DNA Sequence, Hybrid technique.

1. INTRODUCTION

Traditional cryptography contains the key size very large so that storage become high. A new technique for securing data using the biological structure of DNA is called DNA Cryptography. DNA Storage of Data has a wide range of capacity are Medium of Ultra-compact Information storage are very large amounts of data that can be stored in compact volume. DNA Cryptography involves three methods namely:- Insertion ,Complementary, Substitution . Steganograpghy is the process of hiding secret mesages in general multimedia data. Steganalysisis the countermeasure technology of steganography used to detect the possibility of information hiding in the multimedia files.

In the first stage the source data is converted into ASCII and changed into binary code which is made into DNA bases. In second stage random key is generated which is used for next level of encryption. In the third stage decryption process takes place which is reverse process of encryption. The most important component involved in DNA based data masking technique is employing the four nucleotides in sequence.

1.1 Literature survey

In this project, we efficiently addressed data security and user privacy issues in s-health by introducing PASH, a privacy aware s-health access control system. Which supports large universe and partially hidden access policies. In PASH, sensitive attribute values involved in access policies are hidden and generic attribute names are public. We added an efficient decryption test before full decryption to improve efficiency. The large universe construction enables public parameters of a constant number of group elements.

[2]NEW PUBLICLY VERIFIABLE DATABASES WITH EFFICIENT UPDATES

The primitive of verifiable database with efficient updates is useful to solve the problem of verifiable outsourcing of storage. However, the existing schemes either does not support the public verifiability or suffer from the forward automatic update attack. In this paper, we propose a new framework for verifiable database with efficient updates from vector commitment, which is not only public verifiable but also secure under the FAU attack. Besides, we prove that our construction can achieve the desired security properties.

2. Technology

This system is implemented over the enterprise of security purpose by using DNA sequence technique.it provide have many advantages than more compatible application has much more secured to used for it.

2.1 CLOUD COMPUTING

Cloud computing, also on-demand for computing applications, it is a kind of Internet-based computing function that provides shared processing resources applications and data to the computers and other devices on demand for it. It is a model for functioning to enable ubiquitous functions, on-demand access to a shared pool of configurable to be computing resources and appliances. Cloud computing are used to storage solutions provide users and enterprises with various capabilities to the store and process their data in third-party data centers for a certain stage. It restrain on sharing of resources to achieve the coherence and economies of scale to a system, similar to a utility (like the electricity grid) over a network.it is convenient to the system, on-demanding network access for connect to a shared pool of configurable computing

resources and application(e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort to the system.

Cloud computing allows companies to avoiding the upfront infrastructure system costs, and focus on projects that be estimate to differentiate their businesses instead of on infrastructure. it allows enterprises to get their applications up as much possible and running faster, with improved manageability and less maintenance, and enables IT to more rapidly for perform adjusting the resources to meet fluctuating and unpredictable business demand. . This can be lead to unexpectedly high charges if administrators do not adapt to the cloud pricing model system.

2.2 Infrastructure as a service (IAAS)

A good example of IAAS is dedicated servers provided by Web Hosting sites such as Bluehost, Hostgator etc. Cloud computing is making everything simpler and flexible nowadays, but there is another important aspect which is Cloud architecture with robust security implementation is the key to cloud security. Cloud is quite more complex and hence security measures are not simple too to used for. Hence it is new technlogy for devloped to early but it faces new security issues and challenges as well. Till date, most users don't trust storing their data on SASS-based cloud computing providers such as Dropbox, Skydrive and Google Drive etc. Since the outburst of Cloud Computing in the should be difficult, it uses the various methods are devised to increase the security of the data being stored over Cloud Servers. Some of which include Encryption, Decryption, Data Partitioning, Digital Signatures, random sequence key etc.

3. IMPLEMENTATION

In this project work DNA coding is used to encrypt the data. By applying the DNA cryptography the limitations in the spiral transposition and the color pallets can be rectified. The algorithm includes three modules: Encryption, random key generation and Decryption. In the first stage the source data is converted into ASCII and changed into binary code which is made into DNA bases. From the DNA bases hybrid method is implemented using substitution and complementary rule method. This is the cipher text which is further compressed into color pallets. In second stage for the random key is generated but which is used for next level of encryption. In the third stage decryption process takes place which is reverse process of encryption. The most important component involved in DNA based data masking technique is employing the four nucleotides in sequence. These nucleotides are A, C, G, and T. The binary values for A= 00, C = 01, G = 10, T = 11.

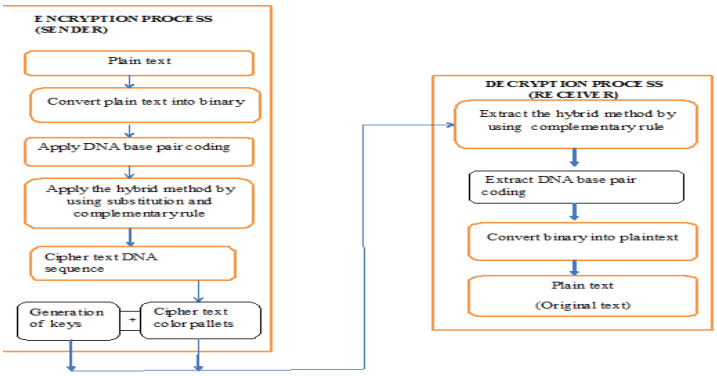


Fig-1: **Architecture**

3.1 Encryption Module

Encryption module is the one which converts plain sequence of text into cipher text. It consists of three sub modules. They are as follows:

STEP 1 : BINARY CODE CONVERSION

The first step in the module will be the conversion of the given text or the input data into its equivalent binary values. The plain text CAT is given as the input which is converted into their corresponding ASCII values as 676584 and subsequent binary code (01000011 01000001 01010100) is generated.

STEP 2: COMPLEMENTARY PAIR AND SUBSTITUTION METHOD

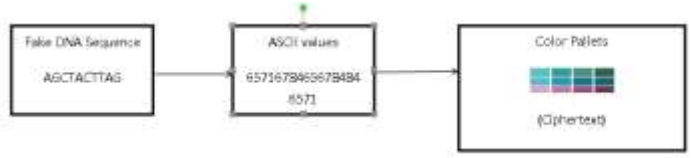
The key generation module uses the Playfair cipher. The Playfair cipher uses a 5 by 5 table containing a key word or phrase. Memorization of the keyword and 4 simple rules was all that was required to create the 5 by 5 table and use the cipher.

To encrypt a message, one would break the message into digrams (groups of 2 letters) such that, for example, "HelloWorld" becomes "HE LL OW OR LD". These digrams will be substituted using the key table. Since encryption requires pairs of letters, messages with an odd number of characters usually append an uncommon letter, such as "X", to complete the final digram. The two letters of the digram are considered opposite corners of a rectangle in the key table

The binary code which is generated in the sub module 1 is converted into DNA sequences using the DNA base pair coding rule ie.,(A= 00, C = 01, G = 10, T = 11).The DNA sequences are then hybridized using complementary pair and the substitution method. Finally fake DNA sequence is induced .

3.2 Color palatte Generation Module

In this module, get the codons from the obtained DNA sequence. Then, convert this to cipher text based on codebook [3]. Cipher text itself will be unrecognized form since each character is represented as a group of a letter and a number. As a final step, convert these characters in cipher text to colors. The red and green components of each color are generated randomly. Only the third component is formed from the cipher text character. This will again improve the security because; same character will be represented by different colors at differ- The fake DNA sequence (AGCTACTTAG) generated in the previous sub module is converted into color pallets through ASCII values which is the required cipher text.



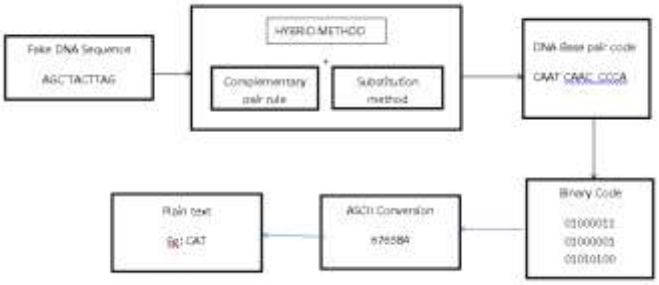
3.2.Key Generation module

The key generation module uses the Playfair cipher. The Playfair cipher uses a 5 by 5 table containing a key word or phrase. Memorization of the keyword and 4 simple rules was all that was required to create the 5 by 5 table and use the cipher.

To encrypt a message, one would break the message into digrams (groups of 2 letters) such that, for example, "HelloWorld" becomes "HE LL OW OR LD". These digrams will be substituted using the key table. Since encryption requires pairs of letters, messages with an odd number of characters usually append an uncommon letter, such as "X", to complete the final digram. The two letters of the digram are considered opposite corners of a rectangle in the key table.

3.4 Decryption Module

The fake DNA sequences is converted into DNA sequences by applying the complementary pair and substitution method. Then binary code is generated by applying the DNA base pair rule. The Binary code is then converted into ASCII and finally the plain text is obtained. The concept of the binary coding rule and the extraction of the hybrid method will generate the required plain text. The hybrid method uses the concept of the substitution and the complementary pair rule. Finally the output of the module is obtained as the plain text.



4. Conclusion

To retrieve the original information since the information is hidden with help of DNA sequence. The random selection of DNA nucleotide is implemented for providing secured transmission of messages over the network. This method provides more security to the information and hence it is not easy accessible for an hacker to crack the encrypted message. The analysis of the proposed technique shows that this is more powerful against certain attacks. This method ensures data integrity and confidentiality over data transmission.