International Journal of Reconfigurable and Embedded Systems (IJRES)
Vol. 5, No. 3, November 2016, pp. 137~142
ISSN: 2089-486

FPGA Based Data Hiding Methods using DNA Cryptography Techniques

B. Murali Krishna*, CH. Surendra*, K. Mani Varma*, K. Mani Kanta*, S.K. Shabbeer*, G.L. Madhumati**
*****ECE Department, K L University, India
*****ECE Department, Dadi Institute of Engineering & Technology, India

Article Info

Article history:

Received Apr 24, 2016
Revised Aug 3, 2016
Accepted Aug 18, 2016

Keyword:

Cipher
Cryptography
DNA
Insertion method
Mystery key

ABSTRACT

To convey the information safely DNA grouping mechanisms are used. There are many methods used by DNA sequences. The proposed method is of both encryption and information concealing utilizing a few properties of Deoxyribonucleic Acid (DNA) groupings. This technique is highlighted that DNA groupings have many more intriguing properties which are used for concealing the information. There are three strategies in this encryption strategy: the Insertion Technique, the Complimentary Pair Technique and the Substitution Strategy .For every single strategy, a specific reference DNA grouping P is chosen and then the taken sequence is changed over with the mystery message M and is consolidated, so that P0 is acquired. P0 is then sent to the collector and the beneficiary can recognize and separate the message M covered up in P. This technique is proposed to utilize INSERTION Strategy. Subsequently, the proposed plan comprises for the most part of two stages. In the principal stage, the mystery information is encoded utilizing a DNA Sequence. In the second stage the encoded information is steganographically covered up into some reference DNA grouping utilizing an insertion strategy. The effectiveness of this security algorithm is seen with many merits and limitations. A, C, G, and T are the 4 nucleotides which are taken for this project.

Corresponding Author:

CH. Surendra,
ECE Department, K L University, India.
Email: cherukurisurendra007@gmail.com

1. INTRODUCTION

Different sorts of information from the Internet turns out to be more easy in now a days, vital data must be disguised while being transmitted by means of the Internet so that just the approved collector can recover it. In this manner, information sending has become more viral and important. The vast majority of them utilize the natural properties of DNA arrangements. The information concealing technique presented by us in the project does not make utilization of organic properties; rather, utilizes different DNA groupings which will be clarified underneath.

A DNA arrangement will have four nucleotides which are named as A, C, G and T elements precisely known as nucleotides. Every letter is identified with a nucleotide. Case in point, two DNA arrangements show up as takes after: The first is the DNA sequence progression from the Litmus with 154 nucleotides taken from the European Foundation (Bioinformatics). Cryptographic applications require a few natural systems and subsequently they have turned out to be the well known as of late. In a standout amongst the most intriguing strategies information is covered up in Deoxyribo Nucleic Corrosive (DNA). In this paper we have proposed an Information Concealing Insertion Strategy based upon DNA grouping. In this strategy we shroud data information into DNA arrangement haphazardly utilizing certain methods. [2].

2. PURPOSE OF CRYPTOGRAPHY

Every security framework will be giving bundles of capacity, which can promise the information mystery of the framework. Some of the important words are given below with their description.

- Confidential: making the transmitted information is only available to a specific user on approved recipient
- Authentication: Recognizing the message beginning effectively without false.
- Integrity: making the necessary adjustments to information, which is to be transmitted, is relevant only to the approved users.
- Non Repudiation: making the sender and receiver of the message not ready to deny the correspondence.
- Access Control: making the entry only to the specific and authorized clients as it were.
- Availability: making resources like PC framework are open to the approved clients whenever they require the information. Security approaches must be adequate to handle the constantly changing information ruptures [3]. This is the place where the information security, encryption of information very still and in movement, executing client access control become possibly the most important factor.

World of Cryptography

Different cryptographic techniques are utilized for securing the information over and over. Cryptography is the specialty of changing over the message into human disjointed code, which can't be turned around to the message without proper code. Cryptography assumes an essential part in information honesty. This can be represented in the three segments of the CIA triad (Confidentiality, Integrity, Availability). CIA is the principal idea in the secured data transmission.

3. DNA CRYPTOGRAPHY

DNA cryptography is one of the fastest growing innovations which take a shot at thoughts of DNA figuring. Another framework for securing data was displayed using the regular structure of DNA called DNA Figuring or sub-nuclear preparing or natural enrolling. It was created by Leonard Max Adleman in the year 1994, for handling the brain boggling issues. Adleman is usually called as "An" in the RSA estimation – a computation which is present in a couple circles that has transformed it into an acknowledged standard for mechanical quality encryption of information sent over the Web. The technique later on reached out by different bosses for encoding and diminishing the point of confinement size of information that made the information transmission over the structure speedier and secured [4].

DNA Insertion Method:

The first method which is done with the DNA cryptography technique. We mainly concentrated in this area in which the method as this one have some more extra features and some more security than compared to others. DNA encryption and decryption techniques are vice-versa techniques. Insertion technique uses DNA sequences for sending messages securely to the receiver. The encryption is known widely as the data hiding process. Encryption technique uses the DNA sequence, which comprises of A, C, G, and T nucleotides which are the main components in the DNA sequencing technique [1].

Encryption:

Encryption is a process of hiding data from the others, which are to be viewed only by some particular and appropriate viewers. In an encryption scheme, the encrypted communication information or messages are referred to as plaintext and the encryption is done using a particular encryption algorithm technique, which generates a cipher-text that can be read only if it is decrypted. To simplify the discussion on the insertion method, the most basic version is taken and solved with the best and simple example. The most complex version is also present but this one gives you the best knowledge on the method. Every method uses a DNA sequence as reference which is Pin this case [9]. Suppose the secret message M is 01100111. Let P be AGGTCAGTCCTTA. The method works as shown below: For an clear view a flow chart is drawn for the encryption technique, shown in Figure 1.

Step 1. Convert P into the binary sequence by using the binary coding rule. Thus the sequence P will now become 0010101101 0010110101111100.

Step 2. Divide the above sequence P into segments, whereby each segment contains k bits. Suppose k is 3. Then the following are the segments we get: 001, 010, 110, 100, 101, 101, 011, 111, and 00. This can be observed in Figure 3.

Step 3. Insert the message M bits, one at a time, into the beginning of each and every segments of P. The result is as shown: 0001, 1010, 1110, 0100, 0101, 1101, 1011, 1111, 00. This can be observed in Figure 4.

The segments which do not carry any hidden message in it are to be ignored. Thus, the following segments are obtained after the elimination of all the extra bits:
0001, 1010, 1110, 0100, 0101, 1101, 1011, 1111, 00 Concatenate the above sequences, and then we get the sequence required: 000110101110010001011101101111111. This can be observed in Figure 5.
Step 4. By using the inverse binary coding function rule to produce the following faked and encrypted DNA sequence:
P01/4ACGGTGCACCTCGTTT. As the reader can see, this sequence is quite different from P. [5]
Step 5. The encrypted sequence as shown above is then sent to the receiver. Figure 6, shows the total encryption process.

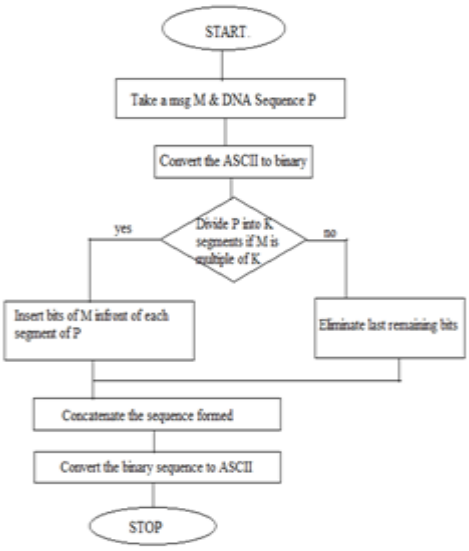

Figure 1. Flowchart for Encryption

Decryption:

The process of extracting the data from the received cipher-text from the transmitter is called as decryption. Messages are sent to the receiver by using a certain encryption process and by doing the equivalent decryption process only we can regenerate the hidden message from the received. The generated message will be the required message. This is only observed by the particular receiver to whom we send the message. There are some interrupters, who try to interrupt the data in between the transmission, this helps to send the message secure without any interrupts. For the sequence that is received, the receiver gets a subsequence out of it, using some mechanisms which receiver uses regularly for the data extraction from the transmitter\if the separated subsequence is not the prefix of the reference group of P, overlook it. In the event that it is, the recipient realizes that he has likewise effectively extricated the mystery message M as a side effect. The recuperation procedure is given in the flow chart drawn in Figure 2.
Step 1. Code got P0 into a paired grouping by utilizing the parallel coding guideline. The sequence P0 will now become: 000110101110010001011101101111111 by using the binary coding rule. The decryption is clearly shown in Figure 7.
Step 2. Remove the principal bits from every 4-bit fragment in the above portions. The outcome is as per the following partition :0,1,1,0,0,1,1,1. Separate the last three bits from every 4-bit portion. The outcome is as per the following: 001, 010, 110, 100, 101, 101, 011, and 111.
Step 3. Concatenate the separated bits and the above remaining sections, which results in the accompanying two fold arrangements: 01100111 and 00101011010010110101111100. The converse capacity of the twofold coding guideline is utilized to change the accompanying double arrangement. This final values are shown in Figure 8.
Step 4: 00101011010010110101111100. User can see, this arrangement will be changed as AGGTCAGTCCTTA. This DNA arrangement is the prefix of P and it is got back to the reference succession by decryption as indicated by P. Consequently the extracted parallel succession 01100111 is the wanted mystery message **FLOWCHART FOR DECRYPTION**

Figure 2. Flowchart for Decryption

The above drawn stream graph is the essential adaptation of the decoding strategy. In this the confounded adaptation should likewise be possible. In such confused technique, P is separated into numerous fragments which utilize a number generator. That is, the lengths of portions contrast. Rather, it is dictated by a percentage of the irregular random number seeds, which are known just to the sender and the main receiver to which the message is sent. Assume the number grouping produced by the arbitrary number seed k may be 3, 2, 4, 6, etc. At that point P is partitioned into sections with lengths 3, 2, 4 and 6, separately. Note that there is a mystery message M. additionally, the same arbitrary number generator may likewise be utilized with various irregular number seed r to partition M into fragments [6].

The sender sends P0 together with many numerous other DNA, or DNA-like groupings, to the receiver along with the original encrypted sequence. The recipient forms each succession got, removes the message arrangement and recoups the first grouping. In the event that the arrangement is not a prefix of the reference P, it implies that the receiver should test some other groupings until the recouped arrangement is precisely a prefix of P. At that point the beneficiary realizes that the mystery message has been removed. The collector utilizes the accompanying calculation to recoup the shrouded message:

Other DNA Cryptography techniques

1. Complimentary pair method
2. Substitution method

Complimentary-Pair Method:

This is one type of the method where the complimentary pairs are used for the encryption technique. The following are the complimentary pairs ((AC) (CG) (GT) (TA)). The complimentary pair of the string AACTG will be CCGAT. Complimentary pair method is the second method after the insertion method the complimentary pairs are used for the decryption technique which is a vice versa of the encryption technique [7].

Substitution Method:

This is also one of the DNA transmission process which works on substitution basis, as the name itself indicates that. Here we don't elaborate this method as it is a very lengthy one and if we start describing this it would be a very lengthy as our main topic is the Insertion method we concentrate on the method.

We mainly concentrated on the INSERTION METHOD we simulated the results using FPGA by Verilog coding. The results mentioned below are the DNA insertion method technique based results [8].

4. SIMULATION RESULTS

The below are the results obtained from the insertion method in the verilog simulation tool coding.

Encryption:

First the given ASCII DNA sequence is converted in to binary sequence and the sequence is then divided into segments using k value here K=3

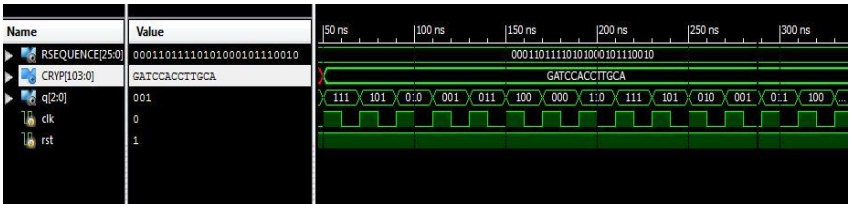

Figure 3. Encryption1, binary conversion

Insert the message into the segments every bit is to be inserted in front of the P segment bits which are divided using k value above.
q in the above figure is the segmented parts which are divided into segments using K value.

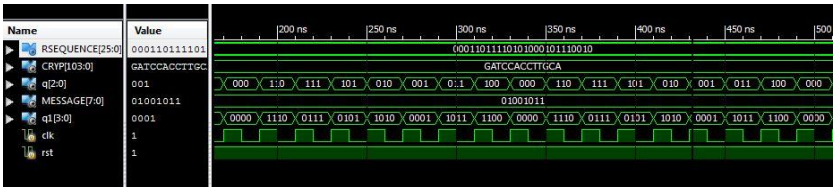

Figure 4. Message sequence insertion into sequence

Concatenate the sequences after the insertion message is intercepted into the code and now insert the message in front of every segments in q then the q now becomes q1 as seen in the above figure.

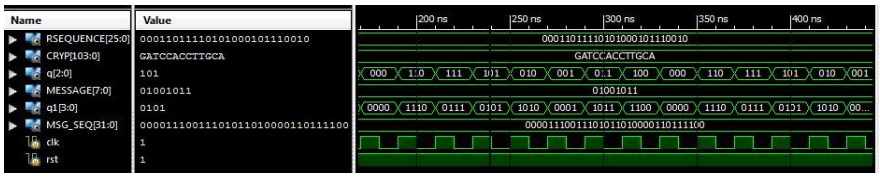

Figure 5. Concatination of segments

Concatenate the sequence q1, MSG_SEQ is generated which is a binary sequence with the hidden message in the DNA sequence.
Convert the concatenated binary sequence again to ASCII value

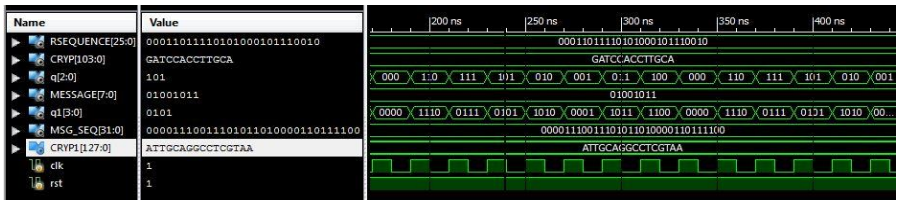

Figure 6. Conversion of concatenated sequence into binary

CRYP1 the sequence is generated by the conversion of the above MSG_SEQ into the binary sequence using the binary coding rule. This particular sequence is sent along with many other such binary sequences to the receiver.

With this the encryption part is completed the same reversal way gives you the decrypted output and the required message. Which can only done by the particular receiver.

Decryption:

Convert the ASCII values received into binary sequence

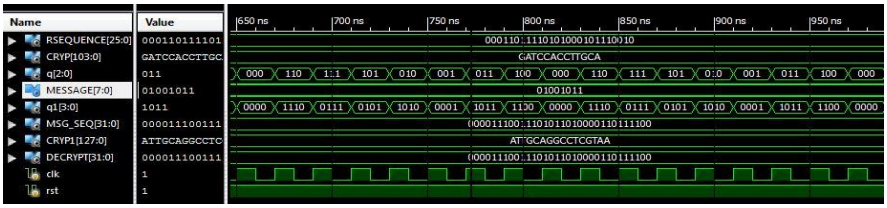

Figure 7. Decrypt, Conversion of BINARY to ASCII

the received sequences are now decrypted one after the other for getting the original and desired sequence with which they can extract the message signal. The sequence having the properties same as their deserved ones is known as their required sequence from which the message is extracted/decrypted.

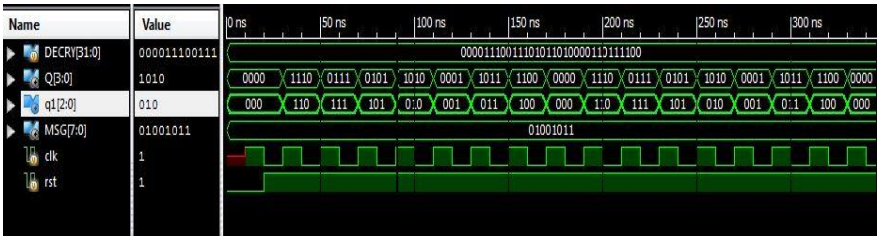

Figure 8. Final outcome separation of message bits from sequence

The sequence is divided into the segments of 4 bits. These 4 are divided into 3 bits and 1 bit. First bit of every segment is taken as message and the last 3 bits as the DNA sequence.

First bits are concatenated and that is the required message sequence which is MSG. The last 3 bits are concatenated and these are called as the DNA sequence which is used in the encryption it is q1.

The message sequence is the sequence which is visible only to the receiver. This protects the sequence from others. The message is encrypted in such a way that the interceptors who hacks the messages are kept secured.

5. CONCLUSION

DNA cryptography system approach is a new approach, which utilizes the deoxyribonucleic acid arrangement property for key encryption and cryptography method. The unusual properties of deoxyribonucleic acid succession result in usage of deoxyribonucleic acid succession for info cryptography forms. The key created within the method goes to a level cryptography method and conjointly the figure content created likewise goes 2 level cryptography methods. Elaboration and security is accomplished by irregular era of the key that is used to cypher and decipher info. Deoxyribonucleic acid cryptosystem is safer and solid than the customary cryptography systems because the process many-sided quality would possibly high for deoxyribonucleic acid innovation.

REFERENCES

[1] H.J. Shiu, K.L. Ng, J.F. Fang, R.C.T. Lee, C.H. Huang, Data hiding methods based upon DNA sequences.
[2] S. Manna S. Roy P. Roy S. K. Bandyopadhyay: Modified techniques of insertion method.
[3] C.C. Chang, T.C. Lu, Y.F. Chang and C.T. Lee, Reversible data hiding schemes for deoxyribonu- cleic acid (DNA) medium, *International Journal of Innovative Computing, Information and Control*, vol.3, no.5, pp.1145-1160,
[4] I. Rama Satya Nageswara Rao, B. Murali Krishna, Syed Shameem Habibullah Khan, G.L. Madhumati, Wireless Secured Data Transmission using Cryptographic Techniques through FPGA
[5] William Stallings "Cryptography and network security 4/E".
[6] Shizhuang Lin; Jingyu Liu; Yanjun Fang;" *ZigBee Based Wireless Sensor Networks and Its Applications in Industrial*", IEEE International Conference on Automation and Logistics, 18-21Aug. 2007, Pg1979-1983.
[7] J.D. Watson, F.H.C, Crick, "A structure for deoxyribose nucleic acid", *Nature*, Vol. 25, pp. 737-738, 1953
[8] Monica Borda, "DNA secret writing Techniques" 8th *International Conference on Communication*, 2010
[9] G. Cui, L. Qin, Y. Wang and X. Zhang, "An encryption scheme using DNA technology," *Bio-Inspired Computing: Theories and Applications*, 2008. BICTA 2008. 3rd International Conference on, Adelaide, SA, 2008, pp. 37-42.