International Journal of Research
e-ISSN: 2348-6848 & p-ISSN 2348-795X Vol-5, Special Issue-10
International Conference on Innovations in Information and Communication Technology
Held on 9th and 10th March 2018 organized by The Department of Information Technology,Meenakshi Sundararajan Engineering College Kodambakkam,Chennai, India

Passport Authentication Using DNA-Based Steganography Technique

S.Dinesh kumar [1] , J.Shalini[2] , L.Shruthi Chellammai[3]

[1]Sri Sairam Engineering College
[2]Sri Sairam Engineering College, [3]Velammal engineering College

Abstract:

Conventional , long-established passport have been substituted by the e-passport for security or safety or reliability reasons.The uniqueness of the e-passport is that it has a built in electronic microprocessor chip with special information to prove the genuinity of passport holder .The greatest threat to e-passport is forgery. Most common threat is changing the holders personal information or photo. The submitted plan brings your attention to the safety of the e-passport by utilising the DNA based Steganography technique .It is a propitious technique to establish the safety of details. The details of the passport concealed into a real DNA sequence. These are two subdivisions in this technique. The primary focus is to conceal the details of the holder by DNA Steganography technique and saving the code in RFID tag. The secondary work is to ensure the credibility of the e-passport by examining using NFC with the code of DNA based Steganography and ensuring the same with one in the RFID tag. If the key in both matches, the computer will compute a key. This key will be utilised to find about the unrevealed information in the tag. This proposed system, is very quick and it's capacity to conceal is very high so it provides higher safety.

Keywords

radio frequency identification, DNA-based Steganography, and epassport.

1. Introduction

An e-Passport is a passport that has an additional integrated circuit or chip which is embedded in any one of the passport pages. The chip contains the data which is used to verify the biometrics of the passport holder, the unique chip identification number, and a digital signature to verify the authenticity of the data stored on the chip. This chip is highly interoperable that is it can be read by any standard border control machine worldwide.This technology promise to reduce fraud, time consuming and enhance security. But At the same time, these technologies raise new risk and security constraints. The common e-Passport threats are Data leakage threats, biometric threat and Spill over.A team called "The Hacker's Choice" have already released a video showing fake e-passport being approved by the terminal and surprisingly 'no error or no alert' is raised.

2. DNA Based Steganography

To ensure the safety of the details provided by the passport holder, the provided details are protected by two dependable attributes known as cryptography and Steganography. The constraints

with Steganography is that the deep seated capacity of the picture is low and so it cannot conceal a large data inside it . To overpower the constraint of capacity the DNA Steganography is brought in. The six molecules in DNA is the Deoxyribo-nucleic acid. The encrypted codes are the chemical bases which are called as Nucleo tides: adenine (A), Guanine (G), Cy-tosine (C), and Thymine

(T).these conceal the information within the DNA. The construction contains of a two long fibers twisted around like a ladder that forms a double helix model made up of sugar and phosphate group. Since the DNA-sequence is huge in size, they provide high enclosure capacity to conceal the large data inside it. The private data is concealed inside the DNA sequence by the methods of DNA insertion algorithm, DNA substitution algorithm.\

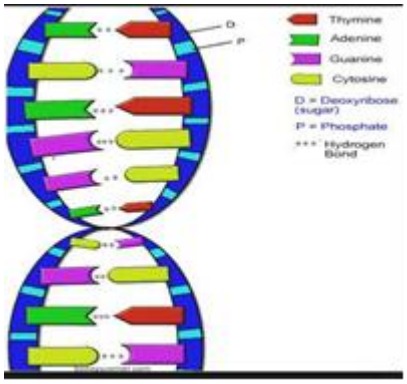

Fig 4.1

3. Literature survey

(Al-Hamami & Al-Anni, 2005B) suggested a protocol to solve e-passport verification and authentication problem. they suggested to the watermark technique that is hidden in passport , and tsuggested the Diffie–Hellman key to solve the problem of mutual authentication between the e-passport and control system.

(Dr.Alaa Hussein and muna in 2016) suggested a system to protect the e-passport against photo forgery using the Diffie-Hellman key exchange.But it has the disadvantage of the logjam attack and common domain parameters.

(Madhu and galma in 2012) proposed a system to improve the authentication by cryptography and watermarking technique.however it is time consuming and limited to single state. (Chirag and Omesh in 2014)has proposed an authentication system for face detection using Stegnography lsb algorithm.The drawback is that it allows the malicious attacker to read the data that we are sending.

(Wang & et al, 2013)proposed a method for e-passport verification depending on watermarking which consists of multimodal biometric feature to verify passport owner and the parity checker code to check integrity of passport.

4. Proposed System:

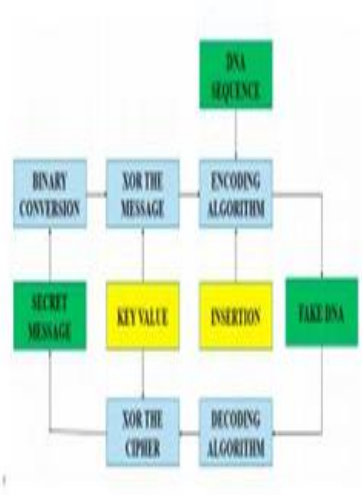

Fig 2 Proposed Architecture

The DNA bases(A,C,G,T) are converted into two digit binary format.A is assigned the value 00,C is assigned 01,G is assigned 10 and T is assigned

11.The secret messge to be hidden is first converted into ASCII format and the into the binary format.There are two keys used in this approach.the first key K1 is is the value that is used to XOR with the message which can range from 0-225.The resulting XOR value is again XORed with the next 8 bits and so on.The binary converted DNA data is partitioned using the key K2. The value of K2 is kept low to have the DNA sequence of the minimum length to hide the secret message. The resulting binary sequence is converted into DNA bases using the dictionary rule. The insertion algorithm is used here for the encoding of cipher inside the DNA. The decoding of the fake DNA is done by complementing the above steps of encoding. The fake DNA, cipher and the two random array sequences are taken. Iteratively using the random sequences the message is recovered and the string is reduced by the message and the immediate succession sample sequence. Once retrieved the messaged is converted to its binary equivalent and continuously XORed from the least significant 8 bits to the most significant 8 bits. This binary value obtained is transformed into its corresponding ASCII values and then concatenated to get the string message.

5. Algorithm for encoding:

1. Generate the ASCII value for the code or message.

2.The message ‘M’ M= {m1, m2, m3…mn}that is to be modified is split into its 8-bit binary-equivalent based upon its corresponding ASCII value

3.The last element of set M is XORed with a randomly generated key k1.

4.The result is the XORed with the code that is preceding the last one in the set M and repeated till all the elements are converted and stored in ‘S’.

5.The binary sequence in S is converted to the DNA protein sequence.

6.A sample DNA sequence ‘A’ is taken and along with a randomly generated using the key number n less than size of M.

7.Break S is divided into n partition such that each division sums up to the size of S.

8. Similarly, break down the generated DNA sequence S and insert each division of S onto the divisions of A using the DNA insertion algorithm.

9.Generate the binary form of the sample DNA sequence A by using the coding methods.

10.Generate a random number k2 so that we get to know the number of partition of the message M and Sequence S.

11.A series of random numbers (s1,s2,s3…..sP) and (r1,r2,r3,…..rP)would be generated such that the sum of all the random numbers would be equal to the size of the sequence and the message respectively for their series.
12.Now combine the corresponding splits .Now you would get a new binary string.
13.Now convert the binary string is converted intoto DNA form by the insertion algorithm to get the new DNA sequence with the message encrypted with it.

6. Algorithm for decoding:

1. Convert the encoded DNA sequence(S') into binary form. 4. Combine all the remaining s (i) strings to get the DNA sequence.

2.Divide S' sequence into parts of length s1+r1, s2+r2… sP+rP.
3.Now from all the small strings obtained from step 2 extract the first r (i) bits.
5.Join all the extracted bits in step 3 to form the message in binary.
6.Convert the binary message and sequence to ATGC form by using the coding rule.
7.Get the binary equivalent from the insertion decryption output and store in M
8. Divide M into pieces of 8 bits each {m1, m2, m3….mn-2, mn-1, mn}
9.For i=n: 2 A= (XOR mn-1 with mn) +A
10. A= (XOR m1 with key) +A Step 11: This binary is converted to its ASCII equivalent to obtain the message.

7. Conclusion:

The proposed system provides an improved authentication technique for passport verification. The proposed security method works correctly in identifying the forgery if it is existed.The authentication of the validity of the epassport is confirmed by the double checking for the hidden code. The DNA based steganography provides low cracking probability for hackers than the other existing approaches . It also provides better time performance, high data hiding capacity and huge storage capacity.

8. References:

[i] Meera, M., Malathi, P. An improved embedding scheme in compressed domain image steganography. International Journal of Applied Engineering Research 2015; 10 (55):1933-1937.

[ii] Malathi P, Gireeshkumar T. Relating the Embedding Efficiency of LSB Steganography Techniques in Spatial and Transform Domains. Procedia Computer Science 2016; 93:878-85.

[iii] Khalifa A. LSBase: A key encapsulation scheme to improve hybrid crypto-systems using DNA steganography. In 8th IEEE International Conference on Computer Engineering & Systems (ICCES) 2013; 105-1

[iv] Prof. Dr. Alaa Hussein Al - Hamami & Muna Amin Alabed Alhafez:Enhancing Security to Protect E-Passport against Photo Forgery
[v] Vaikunth Raghavana:Highly Improved DNA Based Steganography

.