A Secure Image-Based Authentication Scheme Employing DNA Crypto and Steganography

Mohammed Misbahuddin
Computer Networks & Internet Engineering Division
C-DAC, Electronic city
Bangalore, India
mdmisbahuddin@gmail.com

Sreeja C.S.
Dept. of Computer Science
Christ University
Bangalore, India
sreejasukumaran@gmail.com

ABSTRACT
Authentication is considered as one of the critical aspects of Information security to ensure identity. Authentication is generally carried out using conventional authentication methods such as text based passwords, but considering the increased usage of electronic services a user has to remember many id-password pairs which often leads to memorability issues. This inspire users to reuse passwords across e-services, but this practice is vulnerable to security attacks. To improve security strength, various authentication techniques have been proposed including two factor schemes based on smart card, tokens etc. and advanced biometric techniques. Graphical Image based authentication systems has received relevant diligence as it provides better usability by way of memorable image passwords. But the tradeoff between usability and security is a major concern while strengthening authentication. This paper proposes a novel two-way secure authentication scheme using DNA cryptography and steganography considering both security and usability. The protocol uses text and image password of which text password is converted into cipher text using DNA cryptography and embedded into image password by applying steganography. Hash value of the generated stego image is calculated using SHA-256 and the same will be used for verification to authenticate legitimate user.

Categories and subject Descriptors
D.4.6 [Security and Protection] (K.6.5): Authentication

General Terms
Security, Human Factors, Verification, Algorithms.

Keywords
Authentication, Information security, DNA, DNA Cryptography, DNA Steganography, Image password.

1. INTRODUCTION

Information technology has revolutionized the way in which digital data are organized, processed and preserved. It also centralizes on the significance of security of information and measures to be taken to thwart the attack. Information security plays a major role in providing relevant levels of assurance for Privacy, Authenticity, Integrity and Non repudiation.

Authentication is a property which ensures proving one's identity. Generally authentication mechanisms are classified into three factors based on

- ✓ Something a user knows - Knowledge factors
- ✓ Something a user has - Ownership factors
- ✓ Something a user is – Inherence factors

For strengthening authentication, generally two or more factors are combined. Various techniques have been proposed which include two factor authentication schemes based on smart cards and biometrics. Smart card based schemes have been widely adopted in many remote authentication systems but carrying around card remains a major issue whereas biometrics based schemes have certain limitations, including higher cost and privacy issues[1] [2] [3] [4]. Huang et al. proposed a generic framework for three factor based authentication scheme by means of smart card, password and biometrics by focusing the issues of biometrics in distributed systems [5].

Password based authentication are still dominant considering cost of other authentication techniques. A strong password is usually random and hard to guess but for most users these alphanumeric passwords are difficult to remember comparing to simple passwords which are easy to remember but predictable.

To overcome memorability issues, graphical passwords have been proposed. The graphical password authentication was first described by Blonder [6], which is an image based system, replacing the traditional text input password. Graphical passwords have certain limitations, including vulnerability against certain type of attacks such as shoulder surfing[7]. Considering usability and memorability issues, various graphical password authentication techniques are proposed [8]. Lin et al. proposed graphical password authentication system based on tabular steganography which also prevents information eavesdropping during data transmission [9].

1.1 DNA

DNA, Deoxyribonucleic acid the central repository of information was first identified and isolated in 1869 by Swiss physician Friedrich Miescher. The double helix structure of DNA was first discovered by James Watson and Francis Crick. DNA, which is considered as magic code of life, has more applications other than being a genetic material because of its computational properties and massive parallelism. The DNA sequence is unique in nature.

WCI '15, August 10-13, 2015, Kochi, India

© 2015 ACM. ISBN 978-1-4503-3361-0/15/08…$15.00

DOI: http://dx.doi.org/10.1145/2791405.2791503

DNA is a double stranded helix of nucleotides. Each nucleotide containing one of four bases adenine (A), guanine (G), cytosine (C) and thymine (T), where A and T are complementary, and G and C are complementary. A, G, C, T can be represented as gray coding. Binary coding rule of DNA sequences is an advantage as 24 kinds of coding is possible for A, G, C, T which add more computational complexity to the DNA sequences[10] [11].

Table 1. Binary coding based on DNA

Bases	Gray Coding
A	00
G	01
C	10
T	11

Table 1 depicts the reflected binary representation of base pairs, they are said to be gray codes as it is a binary number system which differs only in one bit between successive values [12].

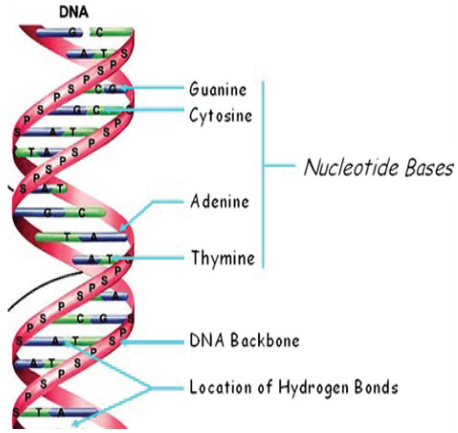


Figure1: **Structure of DNA [13]**

Figure 1 is a pictorial representation of the structure of DNA, which shows bonding between the bases (A, T, G, C) and Sugar phosphate backbone. Adenine pairs with thymine and cytosine pairs with guanine.

1.2 DNA Steganography

Computational properties on DNA was first performed by Leonard Adleman in 1994 [14], where as Steganography using DNA was first performed by Carter Bancroft by a double Steganography concealment technique by hiding a secret message encoded in DNA which further concealed into a microdot, which marked the beginning of authentication using genomic Steganography[15]. It has been developed based on background that most of the present crypto systems rely on factorization problems, so they are theoretically subject to attack by quantum computers. DNA based Steganography has an additional security of biological computation. Breaking DNA based Steganography is highly resistant to quantum computers as it is based on biochemical problem [16].

Steganography based schemes are integrated as a part of authentication techniques of which image based Steganography is a major contribution. Image based registration and authentication system proposed by Srinath Akula et al. [17] is a simple authentication system which uses image as password. Their future work aims to integrate with simple biometric system to enhance security.

The authentication framework proposed by Gunawardena S, et al.[18] is based on Image Steganography, an approach of authentication using an image with embedded user profile data. Image hash values and secret coordinates are stored during registration on which steganalysis is performed during authentication. LSB technique is used for faster execution and to ensure balance between security, integrity and availability.

DNA based Image encryption algorithm proposed by Qiang Zhang et al. [19] obtains a sequence matrix by encoding the original image and divides the original image into blocks and perform addition operation on these blocks based on DNA sequence operation followed by complement operation based on DNA sequence using logistic maps and the simulation results shows good encryption effect.

An Encryption scheme proposed by Guangzhao Cui et al. [20] is based on DNA synthesis, PCR amplification, DNA coding in addition to theory of traditional cryptography. Key generation is based on PCR amplification followed by pre-treatment, generates cipher text which is converted into DNA digital coding and flanked by PCR primers along with certain number on dummy DNA sequences. The security analysis of proposed algorithm claims high confidential strength.

Ravi Kumar B, et al. [21] proposed a method for data security and authentication using steganography for transferring large amount of encrypted data without affecting the quality of image and authenticity. Implementation has been done in JPEG and BMP images.

Sanjive Tyagi et al. [22] proposed steganography technique to ensure authenticity and integrity for embedding large amount of data. The algorithm uses LSB matching method to secure data without affecting the image quality and acceptable security.

DNA based techniques for security also getting wide attention because of its huge parallelism and vast storage capacity, which can be exploited for cryptography techniques along with complementary rules and binary coding. The Pseudo DNA Cryptography method proposed by Kang Ning, [23] based on the central dogma of molecular biology simulates critical process in central dogma rather than using real DNA for Cryptography. This method promoted lots of researchers to exploit Cryptographic techniques based on Pseudo DNA. This technique provides an alternative method instead of using real DNA as a means of Cryptography,which required high tech lab facilities and computational limitations. In our earlier work [24], an algorithm based on central dogma principle using complementary rules and binary coding along with padding and spilcing techniques has been proposed which provides bio security along with cryptography technique based on pseudo DNA concepts.

DNA secret writing techniques by Monica Borda et al.[25] presents biomolecular computation principles and algorithms based on DNA Steganography and cryptography.A brief idea on biomolecular computation elements such as DNA OTP generation, DNA Tiles, DNA XOR with tiles,Chromosomes DNA

indexing is given. Steganography technique based on DNA hybridization performs encryption using DNA based OTP as key and the encoded message is placed between the primers and hidden in a microdot.

Various DNA based methodologies have been proposed by researchers of which DNA cryptography, Pseudo DNA Cryptography and Image based DNA steganography were major breakthroughs. All these techniques have their own merits and concerns.This paper proposes a scheme based on a combination of DNA cryptography, Image steganography along with image password and textual password for authentication aims at enhanced security without affecting usability to the legitimate user.

2. PROPOSED METHODOLOGY

The objective of the proposed method is to ensure tradeoff between usability and security. This authentication protocol is a combination of image and text based passwords, DNA cryptography, steganography and message digest.

2.1 Proposed Image Based Authentication Protocol

The proposed protocol consists of three phases namely Registration Phase, Login Phase/Authentication Phase and Password Change phase. Table 2 represents the notations used in the algorithm and the workflow of all the phases are mentioned in the algorithm.

Table2: **Notations used in the algorithm**

User U, AS	i^{th} User, Authentication server
ID_U	User name or ID of U
pwd_U	Password selected by U during registration
pwd_{U1}	Password selected during password change phase by U.
CI_U	Cover image selected by U during registration.
CI_{U1}	Cover image selected during password change phase by U.
DNA Seq_U	DNA sequence selected for U during registration.

2.1.1 Registration Phase

R1: User U sends a request for registration to the authentication server AS.

R2: AS presents the registration interface to U.

R3: U sets the necessary information for registration including User ID [ID_U] and Image of her choice called as Cover Image (CI_U)

R4: U chooses a valid Password pwd_U.

R5: A gray coding method for DNA sequence is required for additional security. By default, AS selects gray coding as given in Table 1.If user wants additional security, she can define her own values for A,G,C,T. However, in this case she needs to remember these values as additional credential.

R6: AS picks a DNA sequence (DNA Seq_U) from the digital database for U.

R7: AS computes the key based on the credentials the user has selected during registration.

Key= HASH [Stego Image [U]] where,

Stego Image [U] = [padding [binary [pwd_U + DNA seq_U]]] embedded into the CI_U.

R8: AS displays registration completion message.

The registration phase is depicted in figure 2 below:

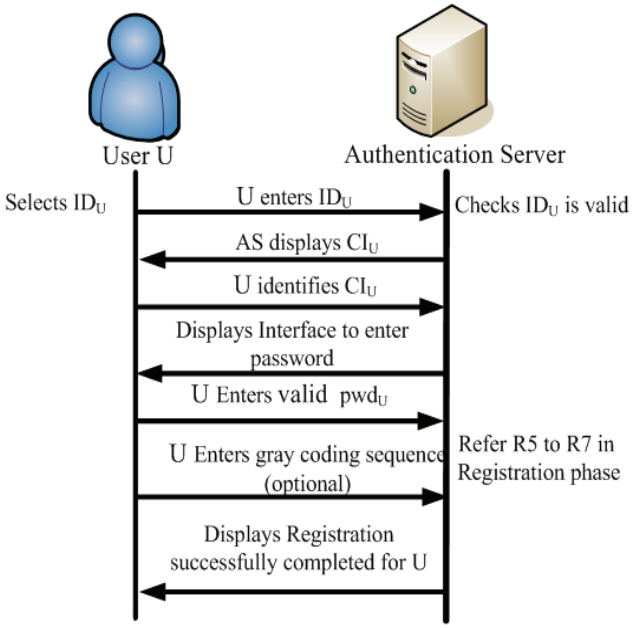


Figure2: Registration Phase

2.1.2 Login Phase/Authentication phase

L1: U enters user name – ID_U

L2: If ID_U is valid, system displays CI_U.

L3: U identifies CI_U and clicks yes on the interface.

L4: If it's valid U can enter the pwd_U else go to L1.

L5: If U had selected R5 during registration. U has to enter the binary code sequence for DNA after entering pwd_U else go to L6.

L6: Based on the ID_U, pwd_U and CI_U ,AS picks the DNA seq_U from the database and performs operations from L7 to L10.

L7: DNA Seq_U is converted into binary after padding pwd_U into the DNA Seq_U as DNA code using gray coding (by default Table 1) by AS.

L8: Padding = [binary [pwd_U + DNA seq_U]].

L9: Embedding the padded value into cover image (CI_U) using steganography technique LSB. This generates a stego image [U].

L10: Hash [Stego Image [U]] will be computed using SHA-256 and the generated digest will be compared against the hash value stored during registration. If both are same authentication granted else access denied.

Figure 3 below depicts the login and authentication phase for User U.

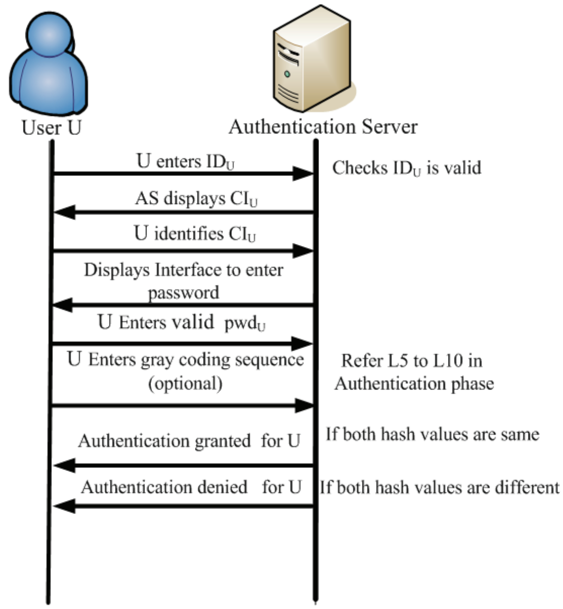


Figure 3: Authentication Phase

2.1.3 Password Change Phase

P1: U enters User ID – ID_U

P2: If ID_U is valid system displays CI_U.

P3: U identifies CI_U then clicks yes on the interface.

P4: If it is valid U can enter the pwd_U else go to P1.If user forgets pwd_U it can be recovered by means of registered mobile number or email ID.

P5: Based on the ID_U , pwd_U and CI_U AS picks the DNA Seq_U from the database and performs operations p6 to p9.

P6: DNA Seq_U is converted into binary after padding pwd_U into the DNA Seq_U as DNA code using gray coding.

P7: Padding = [binary [pwd_U + DNA seq_U]].

P8: Embedding the padded value into CI_U using steganography technique LSB. This generates Stego Image [U].

P9: Computes Hash [Stego Image[U]] using SHA-256 and the generated digest will be compared against the hash value of the stego image stored during registration. If both are same authentication granted else access denied.

P10: After successful authentication U can select either new password pwd_{U1} or new cover image CI_{U1} or both as per requirement.

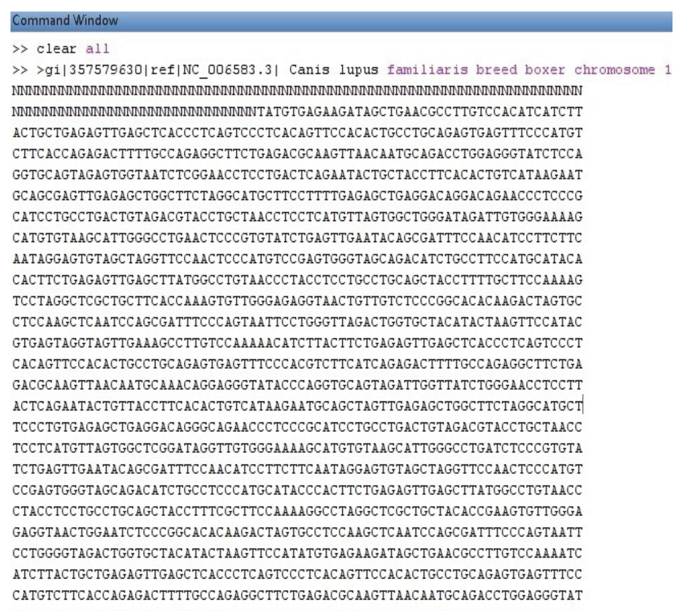
P11:After setting pwd_{U1} and CI_{U1}, AS performs operations from P5 to P9 and stores the newly generated message digest.

3. PROPOSED IMPLEMENTATION METHODOLOGY

The implementation methodology of proposed protocol is discussed in this section. To demonstrate the working of protocol, a sample image titled "Lena image" and the password as "secret" is chosen. Figure 4, Lena_image is depicted below:

Figure4: **AS displays CI_U to the User [26]**

A genome shotgun sequence is downloaded from NCBI [27] with NCBI Reference Sequence: NC_006583.3 in FASTA format. The whole downloaded genome "Canis lupus familiaris breed boxer chromosome 1" (CanFam3.1), screen shot is shown in figure 5. A fragment of DNA sequence from CanFam3.1 is selected to perform DNA Cryptography and Steganography as discussed below.



```
Command Window
>> clear all
>> >gi|357579630|ref|NC_006583.3| Canis lupus familiaris breed boxer chromosome 1
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNTATGTGAGAAGATAGCTGAACGCCTTGTCCACATCATCTT
ACTGCTGAGAGTTGAGCTCACCCTCAGTCCCTCACAGTTCCACACTGCCTGCAGAGTGAGTTTCCCATGT
CTTCACCAGAGACTTTTGCCAGAGGCTTCTGAGACGCAAGTTAACAATGCAGACCTGGAGGGTATCTCCA
GGTGCAGTAGAGTGGTAATCTCGGAACCTCCTGACTCAGAATACTGCTACCTTCACACTGTCATAAGAAT
GCAGCGAGTTGAGAGCTGGCTTCTAGGCATGCTTCCTTTTGAGAGCTGAGGACAGGACAGAACCCTCCCG
CATCCTGCCTGACTGTAGACGTACCTGCTAACCTCCTCATGTTAGTGGCTGGGATAGATTGTGGGAAAAG
CATGTGTAAGCATTGGGCCTGAACTCCCGTGTATCTGAGTTGAATACAGCGATTTCCAACATCCTTCTTC
AATAGGAGTGTAGCTAGGTTCCAACTCCCATGTCCGAGTGGGTAGCAGACATCTGCCTTCCATGCATACA
CACTTCTGAGAGTTGAGCTTATGGCCTGTAACCCTACCTCCTGCCTGCAGCTACCTTTTGCTTCCAAAAG
TCCTAGGCTCGCTGCTTCACCAAAGTGTTGGGAGAGGTAACTGTTGTCTCCCGGCACACAAGACTAGTGC
CTCCAAGCTCAATCCAGCGATTTCCCAGTAATTCCTGGGTTAGACTGGTGCTACATACTAAGTTCCATAC
GTGAGTAGGTAGTTGAAAGCCTTGTCCAAAAACATCTTACTTCTGAGAGTTGAGCTCACCCTCAGTCCCT
CACAGTTCCACACTGCCTGCAGAGTGAGTTTCCCACGTCTTCATCAGAGACTTTTGCCAGAGGCTTCTGA
GACGCAAGTTAACAATGCAAACAGGAGGGTATACCCAGGTGCAGTAGATTGGTTATCTGGGAACCTCCTT
ACTCAGAATACTGTTACCTTCACACTGTCATAAGAATGCAGCTAGTTGAGAGCTGGCTTCTAGGCATGCT
TCCCTGTGAGAGCTGAGGACAGGGCAGAACCCTCCCGCATCCTGCCTGACTGTAGACGTACCTGCTAACC
TCCTCATGTTAGTGGCTCGGATAGGTTGTGGGAAAAGCATGTGTAAGCATTGGGCCTGATCTCCCGTGTA
TCTGAGTTGAATACAGCGATTTCCAACATCCTTCTTCAATAGGAGTGTAGCTAGGTTCCAACTCCCATGT
CCGAGTGGGTAGCAGACATCTGCCTCCCATGCATACCCACTTCTGAGAGTTGAGCTTATGGCCTGTAACC
CTACCTCCTGCCTGCAGCTACCTTTCGCTTCCAAAAGGCCTAGGCTCGCTGCTACACCGAAGTGTTGGGA
GAGGTAACTGGAATCTCCCGGCACACAAGACTAGTGCCTCCAAGCTCAATCCAGCGATTTCCCAGTAATT
CCTGGGGTAGACTGGTGCTACATACTAAGTTCCATATGTGAGAAGATAGCTGAACGCCTTGTCCAAAATC
ATCTTACTGCTGAGAGTTGAGCTCACCCTCAGTCCCTCACAGTTCCACACTGCCTGCAGAGTGAGTTTCC
CATGTCTTCACCAGAGACTTTTGCCAGAGGCTTCTGAGACGCAAGTTAACAATGCAGACCTGGAGGGTAT
CTCCAGGTGCAGTAGAGTGGTAATCTCGGAACCTCCTGACTCAGAATACTGCTACCTTCACACTGTCATA
```

Figure 5: **Screen shot of Canis lupus familiaris whole genome sequence**

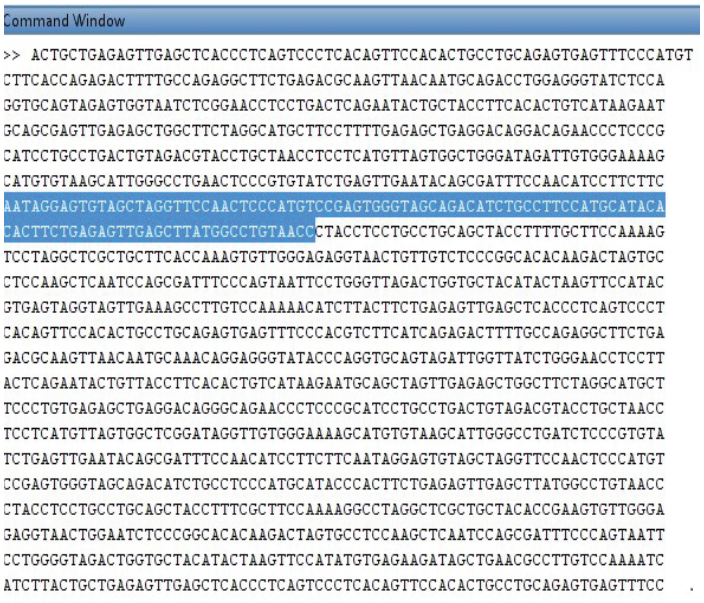


Figure6: DNA fragment selected for data hiding

The fragment selected for data hiding is given here: **AATAGGAGTGTAGCTAGGTTCCAACTCCCATGTCCG AGTGGGTAGCAGACATCTGCCTTCCATGCATACACA CTTCTGAGAGTTGAGCTTATGGCCTGTAACC**

Step1: The user enters her password: "secret"

Step2: AS performs operations from converting the password into gray coding till generation of hash value for verification.

AS converts Password "secret" into Binary value 01110011 01100101 01100011 01110010 01100101 01110100

Step3: AS converts the binary values into DNA base codes by

applying Table1 (as default value). If user wants additional security, she can define her own values for A,G,C,T based on that AS converts password into DNA base codes.

01110011 01100101 01100011 01110010 01100101 01110100
GTAT GCGG GCAT GTAC GCGG GTGA

Step4: The cipher text generated for the password "secret" is GTATGCGGGCATGTACGCGGGTGA.

By applying DNA cryptography AS embeds this cipher text into selected DNA fragment based on the primer selection and locations generates a Cipher DNA sequence

AATAGGAGTGTGTATAGCTAGGTTCGCGGCAACTCC CATGCATGTCCGAGTGGGTACGTAGCAGACAGCGGT CTGCCTTCCGTGAATCACTTCTAGAGTTGAGCTTATG GCCTGTAACC

The highlighted sequences are the cipher text.After embedding cipher text into DNA sequence the generated cipher sequence is

AATAGGAGTGTGTATAGCTAGGTTCGCGGCAACTC CCATGCATGTCCGAGTGGGTACGTAGCAGACAGCG GTCTGCCTTCCGTGAATCACTTCTAGAGTTGAGCTT ATGGCCTGTAACC

The cipher sequence generated by applying DNA cryptography will be embedded into user selected cover image (refer Figure4 for cover image) as binary value.Binary value generated for the cipher DNA sequence is

01000001 01000001 01010100 01000001 01000111 01000111
01000001 01000111 01010100 01000111 01010100 01000111
01010100 01000001 01010100 01000001 01000111 01000011
01010100 01000001 01000111 01000111 01010100 01010100
01000011 01000111 01000011 01000111 01000111 01000011
01000001 01000001 01000011 01010100 01000011 01000011
01000011 01000001 01010100 01000111 01000011 01000001
01010100 01000111 01010100 01000011 01000011 01000111
01000001 01000111 01010100 01000111 01000111 01000111
01010100 01000001 01000011 01000111 01010100 01000001
01000111 01000011 01000001 01000111 01000001 01000011
01000001 01000111 01000011 01000111 01000111 01010100
01000011 01010100 01000111 01000011 01000011 01010100
01010100 01000011 01000011 01000111 01010100 01000111
01000001 01000001 01010100 01000011 01000001 01000011
01010100 01010100 01000011 01010100 01000001 01000111
01000001 01000111 01010100 01010100 01000111 01000001
01000111 01000011 01010100 01010100 01000001 01010100
01000111 01000111 01000011 01000011 01010100 01000111
01010100 01000001 01000001 01000011 01000011

Figure7:Stego Image generated

Figure7 is the stego image generated which has the DNA cipher sequence embeded in it in binary form.Then Hash value is calculated for the stego image (Figure 7) using SHA-256 [28] and the hash value generated is

fd1f5206c237277edea61337d4a39d30698dac500d1462d8324 c10a658b04bf5

SHA-256 is a cryptographic hash function with digest length of 256 bits.The value will be stored in authentication server for verification based on which the server grants authentication for the legitimate user.If the verification failed access will be denied.

4. SECURITY ANALYSIS OF THE PROPOSED METHOD

4.1 Shoulder Surfing Attack

It is considered as a direct observation technique used by an attacker to capture passwords. Most of the graphical password authentication techniques are liable to this attack as it involves one step authentication same is applicable if using only text based password but the proposed method resists shoulder surfing attack as authentication is multi layered from valid ID_U followed by CI_U , pwd_U, DNA coding, steganography and hash function. So knowledge of an image or password alone is not enough to break into the system.

4.2 Dictionary Attack

Dictionary Attack is a technique used to surpass authentication mechanism by trying to determine the passphrase with millions of probability such as words in a dictionary .Proposed method is resistant to this attack because even if the attacker is able to calculate the pwd_U, that will not be able enough to access the account without identifying the CI_U and inserting the proper binary code of base pairs.

4.3 Server Spoofing Attack

The proposed authentication scheme supports mutual authentication to protect the system from server spoofing attack. During login session User enters valid ID_U and AS displays CI_U , which establishes a trust to User that the server is legitimate and U proceeds further by entering valid pwd_U and binary coding.AS authenticates the legitimate user. So both entities authenticates each other.

4.4 Attack on DNA Reference Sequence

This method uses DNA sequences from digital data bases such as National Center for Biotechnology Information [NCBI], European Bioinformatics Institute[EBI]. On EBI database there are 163 million DNA reference sequence are available [29]. As per binary coding rule A,G,C,T can be written in 4 different binary forms ,4!=24.So the probability of selecting the exact DNA reference of U by an unauthorized person is

$$DNA\ Seq_U = ((1/163)*(1/24)).$$

4.5 Resistance to Password File Compromise Attack

In our scheme the hash value of the password is not computed and saved as it is, instead binary [pwd_U] is camouflaged with binary[DNA Seq_U] which is then embedded into CI_U by using LSB method and generates Stego $Image_U$ then Hash[Stego Image U] is computed and saved in the AS. So the message digest generated will be

Padding(binary(pwd_U + DNA Seq_U))→(1)

Embed ((CI_U)+Padded(binary(pwd_U + DNA Seq_U))) →Stego $Image_U$ →(2)

Hash(Stego $Image_U$)→ (3)

Eqn (3) generates message digest which will be saved in AS for verification. So even if password file is compromised by a hacker, the key value will resist password file attack.

4.6 Attacks on Stego Image

Steganalysis is a technique used to determine a particular image contains hidden data or not, the embedding technique used to hide the data, length of hidden message etc. Steganalysis techniques can be broadly classified into three categories such as Visual Analysis, Image format Analysis and Statistical Analysis. The proposed method is not storing the stego image generated anywhere which prevents any steganalysis on the stego image which resist from any Steganography attack.

5. CONCLUSION

This paper proposes an authentication protocol scheme employing Image Steganography, and DNA cryptography by maintaining tradeoff between security and usability. Password authentication is the most common method of authentication used even though it is considered as least secure. The security level of the proposed protocol is better considering the computational complexity of DNA sequence along with layered security without affecting usability. This protocol can be applied to secure pharmaceutical research data where data security and information privacy are major concerns. Future work is to modify the proposed authentication scheme without using a verification table.

6. REFERENCES

[1] http://www.authenticationworld.com/Authentication-User. The business of Authentication.

[2] Nimmy, K. and Sethumadhavan M. Novel mutual authentication protocol for cloud computing using secret sharing and steganography. Fifth International Conference on the Applications of Digital Information and Web Technologies (ICADIWT), IEEE, 2014, pp. 101-106.

[3] Manjunath, M. Mr K. Ishthaq Ahamed, and Ms Suchithra. Security Implementation of 3-Level Security System Using Image Based Authentication. International Journal Of Emerging Trends And Technology In Computer Science (IJETTCS),volume 2, March 2013.

[4] Liao, Kuan-Chieh, and Wei-Hsun Lee. A novel user authentication scheme based on QR-code. Journal of Networks 5, no. 8, 2010, pp: 937-941.

[5] Xinyi Huang, Yang Xiang, Chonka A. Jianying Zhou and Deng, R.H., A Generic Framework for Three-Factor Authentication: Preserving Security and Privacy in Distributed Systems, IEEE Transactions on Parallel and Distributed Systems, Aug. 2011, pp.1390-1397.

[6] Blonder, Greg E. Graphical password. U.S. Patent 5,559,961, issued September 24, 1996.

[7] Gao, Haichang, Wei Jia, Fei Ye, and Licheng Ma. A survey on the use of graphical passwords in security. Journal of software 8, no. 7, 2013, pp.1678-1698.

[8] Biddle, Robert, Sonia Chiasson, and Paul C. Van Oorschot. Graphical passwords: Learning from the first twelve years. ACM Computing Surveys (CSUR) 44, no. 4 , 2012.

[9] Lin, Tsung-Hung, Cheng-Chi Lee, Chwei-Shyong Tsai, and Shin-Dong Guo. A tabular steganography scheme for graphical password authentication. Computer Science and Information Systems 7, no. 4 , 2010, pp.823-841.

[10] Jain, S. Bhatnagar, v, Analogy of various DNA based security algorithms using cryptography and Steganography. International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), 7-8 Feb. 2014, pp.285-291.

[11] Menaka, K., Message Encryption Using DNA Sequences. World Congress on Computing and Communication Technologies (WCCCT), Feb. 27 2014-March 1 2014, pp.182-184.

[12] http://en.wikipedia.org/wiki/Gray_code. Gray Code

[13] http://keltoncheyennepowell.weebly.com/stucture-of-dna.html.Structure of DNA.

[14] Adleman, Leonard M, Molecular computation of solutions to combinatorial problems ,Science-AAAS-Weekly Paper Edition 266.5187, vol., no 266, Nov. 1994, pp 1021-1023.

[15] Clelland, Catherine Taylor, Viviana Risca, and Carter Bancroft. Hiding messages in DNA microdots ,Nature 399.6736 , June 1999, pp 533-534.

[16] Carter Bancroft, DNA-Based Technologies: Computation, Steganography, Nanotechnology, Talk at Material Science and Engineering, Stony Brook University, 4/2011.

[17] Akula, Srinath, and Veerabhadram Devisetty. Image based registration and authentication system. In Proceedings of Midwest Instruction and Computing Symposium, vol. 4. 2004.

[18] Gunawardena, S.; Kulkarni, D.; Gnanasekaraiyer, B., A Steganography-based framework to prevent active attacks during user authentication," 8th International Conference on Computer Science & Education (ICCSE , 26-28 April 2013, pp.383-388.

[19] Zhang, Qiang, Ling Guo, Xianglian Xue, and Xiaopeng Wei. An image encryption algorithm based on DNA sequence addition operation. Fourth International Conference on In Bio-Inspired Computing, BIC-TA'09, Ieee, 2009 ,pp. 1-5.

[20] Guangzhao Cui, Limin Qin, Yanfeng Wang,Xuncai Zhang, An encryption scheme using DNA technology. 3rd International Conference on Bio-Inspired Computing:Theories and Applications, BICTA, Sept.2008, pp.37-42.

[21] Ravi Kumar. B., Murti. P.R.K., Data Security and Authentication Using Steganography International Journal of Computer Science and Information Technologies, Vol. 2 (4) , 2011, pp. 1453-1456.

[22] Sanjive Tyagi, Ajay Agarwal, Ramveer Singh, and Mr Ramveer Singh. An Approach to Secure Larger Size Data with Authenticity and Integrity,International Journal of Computer Science and Information Technologies, Vol. 1 (4), 2010 , pp.244-248.

[23] Kang Ning, A pseudo DNA cryptography Method. DBLP: journals/corr/abs-0903-2693, 2009.

[24] Sreeja C.S., Mohammed Misbahuddin, Mohammed Hashim N.P., DNA for information security: A Survey on DNA computing and a pseudo DNA method based on central dogma of molecular biology. International Conference on Computer and Communications Technologies(ICCCT), 11-13 Dec.2014 , pp.1-6.

[25] Monica Borda, and Olga Tornea DNA secret writing Techniques. In IEEE conferences 2010, pp. 451-456.

[26] http://www.cosy.sbg.ac.at/~pmeerw/Watermarking/lena.html. Peter Meerwald .Original image:Lena

[27] http://www.ncbi.nlm.nih.gov/nuccore/357579630/. Canis lupus familiaris breed boxer chromosome 1, CanFam3.1, whole genome shotgun sequence.

[28] http://hash.online-convert.com/sha256-generator. Calculate a SHA hash with 256 bits.

[29] Mohammad Reza Abbasy,Pourya Nikfard, Ali Ordi, and Mohammad Reza Najaf Torkaman. DNA Base Data Hiding Algorithm. International Journal of New Computer Architectures and their Applications (IJNCAA) 2012, pp183-192.