European Journal of Molecular & Clinical Medicine
ISSN 2515-8260 Volume 7, Issue 4, 2020

Delay Efficient Genetic Algorithm with DNA Based Cryptography for Fingerprint Authentication

S Vijayakumar[1], M Jansi[2], D Lavanya[2], V LavanyaSree[2]

[1)] Associate Professor, Department of Computer Science and Engineering, R.M.K. Engineering College, Kavaraipettai, India.

[2)] Department of Computer Science and Engineering, R.M.K. Engineering College, Kavaraipettai, India.

E-mail – svk.cse@rmkec.ac.in

Abstract. With the expeditious growth in digital technology, biometrics makes the highest level of security compared to conventional methods like passwords and PIN numbers. Biometric is the measurement and statistical analysis of a user's unique physical (Fingerprint, Iris, Hand, DNA, Face) or behavioural (Voice, Sign, Keystroke) characteristics. Among all the Biometric techniques, Fingerprint is distinctive for every person and it can be utilized as a technique for individual identification. In this paper, a fingerprint template encryption scheme based on DNA Encoding and Genetic Algorithm is proposed to secure fingerprint templates. The fingerprint template is processed by feature extraction and the features are encrypted using DNA cryptographic algorithm .XOR operation is performed for the second layer of authentication. During the decryption process, we obtain the feature vector which matches with the input feature vector and the user input image is retrieved as final output.

1.Introduction

Nowadays, Security has become a critical issue in the biometrics system. Typical security systems use methods such as passwords, pins and token based methods such as key, license, smart card. These methods are vulnerable to third parties which ease cracking the password or forging without the permission of the authorized user using effective tools. So a biometrics system is needed for reliability, identification and authentication. Biometrics can provide users with a reliable authentication process which in turn pave way for improving security. Biometrics refers to science and technique of identifying/verifying the person by measuring and analysing human characteristics. It has the potential to distinguish between an authorized and unauthorized entity. Each person has unique characteristics which are used to authenticate. Thus biometrics prevent the risk of passwords being forgotten, stolen or copied. In general, biometric characteristics are divided into two types. One is Static (Physiological) that refers shape of the body such as Fingerprints, Face, Iris, Hand geometry/ vein, Retinal pattern, DNA and the other is Dynamic (Behaviour) that refers behaviour of a person such as Signature, voice, keystroke, pulse. Here we use fingerprints as static biometric characteristics which are distinct for different fingers. Fingerprints for twins are also considered to be unique but they have the same DNA. Fingerprint uniqueness is determined by ridge patterns and valleys. A fingerprint image is read from the hardware which captures these salient biometric characteristics. The software interprets the resulting data and identifies the authenticated user. Features are extracted from the image and then template is created for comparison.

2. Existing System

Cryptography is one of the best ways to secure the information. The goals concerned are confidentiality, data integrity and availability. Senders use cryptographic algorithms for enciphering the secret data in

unreadable format and send it via the communication channel. An intended recipient only deciphers the secret data by using a decryption algorithm with a secret key so that the secret message is not altered or read by intruders. In the area of cryptography, various algorithms such as DES, AES, IDEA and Blowfish etc., were used which are not suitable for image encryption. These algorithms face issues such as when the numberof user's increases, key management becomes complicated, difficulty in hardware implementation, complex to implement with software.Nowadays, DNA cryptography (Deoxyribonucleic acid) is the spurting technology where human DNA is used for carrying information.

3. DNA Cryptography

Cryptography is the branch of science which deals with the encoding of data for hiding messages. It plays an important role within the infrastructure of communication security. DNA Cryptology combines cryptology and modern biotechnology. DNA crypto method offers fast, less storage and adequate power requirements. This DNA cryptography consumes memory of about 1bit/nm3 whereas traditional storage methods consume 1012 nm3/bit. Power is not at all needed for computing and processing the DNA. To note, a gram of DNA has 1021 DNA bases which admit 108 TB of knowledge. DNA Cryptography hides data in terms of DNA Sequence. Encoding data in an exceedingly DNA strand is especially made, from 4 nitrogenous bases namely: Adenine (A), Guanine (G), Thymine (T) andCytosine (C).

Table1. Eight kinds of DNA map rules

	1	2	3	4	5	6	7	8
A	00	00	01	01	10	10	11	11
T	11	11	10	10	01	01	00	00
G	01	10	00	11	00	11	01	10
C	10	01	11	00	11	00	10	01

The cipher text is obtained by XORing the message and key. The XORed output is provided in DNA format. In decryption process all the DNA bases are converted into bits whichare then XORed with the key to breed the first plain text. The obtained binary format is converted into a sequence of ASCII characters.

4. Proposed System

Sender uses a cryptographic algorithm for enciphering the secret data in unreadable format and sending it via the communication channel. An intended recipient only deciphers the secret by using a decryption algorithm with a secret key so that the secret message is not altered or read by intruders. Several algorithms such as DES, AES, IDEA and Blow Fish etc. have been developed in the field of cryptography over the past few years that are not suitable for image encryption. DNA (Deoxyribonucleic acid) cryptography is currently the latest evolving technique where the human DNA carries the necessary information. Although fingerprint systems have some advantages compared to conventional security systems, there are some problems with the algorithms that we choose for implementing the same. When it comes to AES, it is difficult to implement with software. With DES, the cost of execution time increases. Large numbers of weak keys makes the IDEA algorithm a difficult choice and with blowfish, key management becomes complicated.

5. Methodology

The fingerprints are collected using U.are.U 4500 sensor as digital images. U.are.U 4500 is a fingerprint sensor used to capture a digital image of the fingerprint pattern. The captured image is called a live scan. This live scan is a biometric template which is created by digitally processing the extracted features. This is how fingerprint sensors work.

Optical fingerprint imaging is the technique used here. This works like a digital camera for capturing the fingerprint input. This specialized image capturing is done with the help of visible light. The collected fingerprints are processed using MATLAB Software. MATLAB provides users with the following functionalities: creating UI, perform matrix manipulation, plot functions and data, provide program interfaces.

BLOCK DIAGRAM:

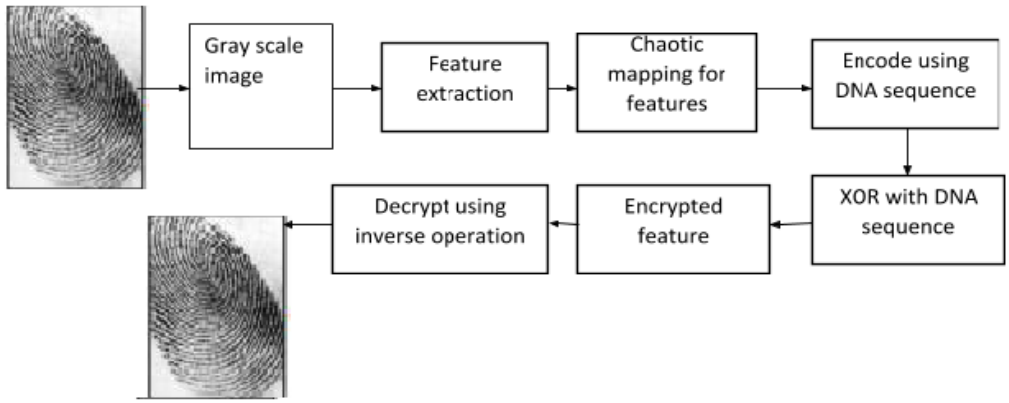

Figure 1. Process flow of DNA cryptography

The steps involved in the encryption process are as follows:
1. Image is captured as a gray scale image using U.are.U 4500 sensor.
2. The features like islands, ridges, and bifurcations are extracted.
3. Chaotic mapping
4. The extracted features are encoded using DNA cryptography for encryption.
5. The key is generated using DNA cryptography.
6. For two factor authentication, the generated sequence is further XORed for encryption.
7. Decryption is the exact reverse process of the encryption which results in the extracted feature value which matches with the initial value.

6. Conclusion

Since the authentication of biometrics techniques over an open network occurs more and more, security of such techniques is more important. DNA cryptography has been emerging technology at present. In this proposed scheme, human fingerprint is encrypted by using the properties of DNA and chaotic algorithms which ensures preserving the privacy of the template. Moreover, DNA sequences are generated randomly which is never reused and it improves the security of basic use of DNA codons. Thus, the combination of chaotic algorithm and DNA Cryptography could be used for authentication of fingerprint templates efficiently and securely.

Acknowledgment

The authors wish to thank
Mr. Saravana Kumar, Senior System Designer in Hitachi Solutions for supporting this work.

References

1. Ashbourn, Julian 2014,*and Biometrics: Advanced identity verification*.
2. Sharma and Monika, *Fingerprint Biometric System: A Survey* International Journal of Computer Science & Engineering Technology 2014.
3. Jain, Anil K, Arun Ross, and Umut Uludag. *Biometric template security: Challenges and Solutions* Signal Processing Conference,IEEE, 2005.

4. Behrouz A Forouzan, Debdeep Mukhopadhyay, *Cryptography and Network Security*, McGraw-Hill, Second edition, 2010.
5. Zhang and Mingjun, *Interactive DNA sequence and structure design for DNA nano applications NanoBioscience*, IEEE Transactions on 2004.
6. Watson J D and F H C Crick, *A structure for deoxyribose nucleic acid*,a century of Nature: Twenty-one discoveries that changed science and the world in 2003.
7. Cui and Guangzhao, *DNA computing and its application to the information securityfield* Natural Computation, 2009. ICNC'09. Fifth International Conference on. Vol. 6. IEEE, 2009.
8. Adleman and Leonard M, *Molecular computation of solutions to combinatorial problems 1994*.
9. Gehani and Ashish, Thomas LaBean, and John Reif, DNA-*based cryptography*,Aspects of Molecular Computing, Springer Berlin Heidelberg, 2003.
10. Chen andJie *A DNA-based, biomolecular cryptography designCircuits and Systems*, 2003. ISCAS'03. Proceedings of the 2003 International Symposium IEEE, 2003.
11. Amin, Sherif T, Magdy Saeb, and Salah El-Gindi, *A DNA-based implementation of YAEA Encryption algorithm*,Computational Intelligence, 2006.
12. Zhang, Qiang, *An image encryption algorithm based on DNA sequence addition operation*, 2009.
13. Sadeg and Souhila, *An encryption algorithm inspired from DNA,* Machine and Web Intelligence, 2010.
14. Archana S. Shinde and Varsha Bendre,*an Embedded Fingerprint Authentication System*, in International conference on computing communication control and automation, July 2015.
15. Arun Pratap Srivastava,Shashank Awasthi,*Fingerprint Recognition System using MATLAB* in International Conference on Automation, Computational and Technology Management (ICACTM),2019.