Indian Journal of Science and Technology, *Vol 9(37), DOI: 10.17485/ijst/2016/v9i37/102064, October 2016*

ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

A Simple Innovative Approach DNA-based Saliva Security System for User Authentication

R. Radha[1]*, A. John Blesswin[1] and G. Selva Mary[2]

[1]Department of Computer Science and Engineering, SRM University, Chennai - 603203, Tamil Nadu, India;
radha.ra@ktr.srmuniv.ac.in, johnblesswin.a@ktr.srmuniv.ac.in
[2]Department of Information Technology, SRM University, Chennai - 603203, Tamil Nadu, India;
selvamary.g@ktr.srmuniv.ac.in

Abstract

Objectives: User authentication is an indispensable element for secured network service. Due to the rapid advancement of Internetworking technologies, it is easy for attackers to access confidential data by compromising authentication methods. Traditional methods of biometric authentication have a weakness, especially in high-security systems because it gives chances for any attacker to obtain the system information. There is a strong desire to develop and implement more secure authentication method to protect such information against security threats. **Methods:** From the existing Biometric authentication methods, DNA (Deoxyribo Nucleic Acid) is said to be the best method due to its high accuracy and allows both identification and verification. At present DNA techniques are used mainly in Law enforcement, there is feasibility to extend this in real life system security. **Findings:** The proposed D-SSS is an innovative and new idea of DNA pattern extraction and pattern matching approach. **Applications:** The proposed (D-SSS) DNA-based biometric technique builds a new system of authentication that requires very less amount of saliva to protect the system efficiently with high-level security. The D-SSS is a user-friendly approach, which uses the unique property that the user has at the time of authentication, will lead to intensive work in the area of system security.

Keywords: Biometric system, DNA Extraction, Saliva, System Security

1. Introduction

All Information security is concerned with the assurance of confidentiality, authenticity, integrity and availability of information in all forms. Many tools and techniques are available that support the management of information security. The systems based on biometric have evolved to support some aspects of information security[1]. Authentication is the work of establishing somebody as who they declare they are. An authentication method based on biometric information offers superior safety and such systems are progressively gaining extensive use and recognition. Biometric are technologies used for measuring and analyzing a person's unique characteristics[2]. Biometric substantiation supports the aspect of recognition, confirmation, and non-repudiation in information security. Biometric substantiation has gained popularity as a way to provide personal identification. Delicate data protection against unauthorized access is a must. Computer scientists examined for new biometrics authentication systems to accomplish this. There are two types of biometrics: Behavioral and Physiological[3]. Behavioral features are in correlation with the behavior of a person. Physiological characteristics are related to the shape of the body. Some of the examples are, fingerprint, face recognition, iris recognition, DNA matching. Behavioral biometric are used for authentication while physical biometrics is for either identification or authentication. Recent advancement in technology has led to the evolution of latest Physiological authentication mechanisms. The DNA biometric is new, highly reliable and secure approach, but hardly applied in real time applica-

*Author for correspondence

tions. DNA biometric method is for applications where a high level of security is required. Forensics and law enforcement use DNA biometric method for identification since every person's DNA is unique it is impossible to fake. The reasons for less application of DNA biometric in real time applications is the cost associated with DNA analysis and complex sample collection procedure. Biometric systems such as facial, iris, voice and vein recognitions are commonly used while DNA biometric is not in practice as much. The rest of the paper is organized as follows. Section II presents the definition of System security and various techniques associated with it. Section III deals with introduction to DNA and its importance. Next three Sections describe how DNA can be extracted and used as a means to achieve system security The last section is about the brief conclusion which highlights the advantages of using DNA for security purpose.

2. System Security Methods

System security mainly focuses on securing the data residing in a system and also access to the system itself. It depends on the factors like cost, security level, accuracy and robustness. These factors are interlinked and are directly proportional to one another which form the base for the construction of security system. This section highlights few methods that are available along with their limitations. Identification and verification are the two levels that comprises of authentication. Identification uses the behavioral characteristics to identify an individual. Verification uses physiological characteristics to identify individually by pattern matching[4].

The factors about authentication are:

Knowledge based – secretive question, pin number or OTP

Possession based – Smart cards and key

Physiological based – Finger print and facial recognition

Behavioral based – Mouse dynamics (mouse move, drag and drop, point and click)

From the factors mentioned above physiological and behavior constitute biometric authentication techniques. With the enormous growth in the field of technology and information sharing, the need to secure information has escalated to great heights[5]. Obtaining the information that is shared made way to various techniques like finger print recognition, face recognition, voice recognition, bar code scanner, iris scanner etc. Even though each mechanism has its uniqueness, they suffer certain flaws that made way to advanced techniques.

2.1 Finger Print Recognition

The most price efficient, easy to install and user-friendly mechanism with lower power consumption made this widely accepted system security technique. The major limitation related to this technique is time-consuming process, rejection based on bad quality image and most easily duplicated.

2.2 Face Recognition

This technique is the easiest and widely used mechanism which uses the feature of a human face as input. It uses reference points that make it more reliable with minimal interaction between user and device. The major flaw of this approach is the source of input (human face) which changes over age or disfigured intentionally.

2.3 Voice Recognition

Voice is a unique factor that depicts both physiological and behavioral aspect of a human. Voice recognition systems that focus mainly on a physiological component, i.e., voice tract instead of voice accent is easy to install with minimal equipment requirement. The fact that health factors also influence sound quality changes over age and, it lacks user friendliness . The major risk associated with this method is a risk of unauthorized access via recording devices[6].

2.4 Iris Recognition and Scanner

The human iris which is a thin circular structure has its own pattern and color which differentiates or identifies a person from person and eye from an eye. It is easily installed with expensive equipment. It also grantees to identify a person uniquely even after an eye surgery. It is intrusive, and safety of eyes during a scan of iris or retina is major concern of users and it also requires a large database to store the scanned information which serves a source of potential threat.

2.5 Vein Recognition

This is the most recent biometric mechanism that uses vein structure which has unique physiological and behav-

Table 1. Comparative study of bio-metric methods

Parameters/ Techniques	Uniqueness	Collectability	Permanence	Performance	Acceptability	circumvention
Finger print recognition		√			√	√
Face recognition		√			√	√
Voice recognition	√	√		√	√	√
Iris recognition	√	√	√	√	√	
Vein recognition	√	√	√	√	√	
DNA pattern matching	√	√	√	√	√	√

ioral traits for every human. It provides high level of security with minimal cost and with ease. It gives accurate and reliable information compared to other techniques. Table 1 indicates comparative analysis of various bio-metric methods The major limitation of this technique is the need for large database to store the information, which again becomes a source for potential threat.

3. Importance of DNA

This section presents the definition of DNA, followed by its composition and sources of extraction of DNA. The DNA is a molecule which looks like a ladder twisted into spiral.

Each molecule of DNA contains nucleotides that consist of components namely a sugar molecule, a phosphate molecule and a nitrogenous base. This DNA's shape resembles a double helix.

DNA consists of thousands of genes and genetic information. DNA in biometric applications focuses on the nitrogenous bases while using it[7]. The four distinct bases are:

Adenine (A),
Cytosine (C),
Guanine (G),
Thymine (T).

DNA has highly unique features. This uniqueness says that each individual's DNA is different and cannot be replicated or faked. Compared to any other biometric method DNA posses 0% Failure to Enroll Rate (FTER) and its unique solution is absolute. FTER defines the probability of the system that could not extract distinctive characteristics from the given samples[8]. Based on number of base pair per turn, coiling pattern, location, structure, nucleotide sequence and number of strands DNA is classified as A, B, C and D, right handed and left handed, chromosomal DNA, cytoplasm DNA and promiscuous DNA and so on. Almost any part of body contains DNA that can be extracted. Blood and soft tissues in the human body are mainly used to extract DNA. It is also true that the DNA can also be extracted from semen, saliva, hair roots and even from several skin cells. DNA obtained from these is commonly employed in forensic analysis. The following section gives an overview of saliva and its composition.

4. DNA from Saliva

Saliva is a watery substance that protects and coats the oral mucosa is located in the mouths of human being[9]. The constituents of saliva are electrolytes, mucus; anti-bacterial and bacterial compounds amounting to 0.5% and 99.5% water. Table 2 explains the composition of saliva components Cells that are shed from the linings of the inside of mouth and lymphocytic cells (WBC) are the source of DNA in saliva. Need to construct an effective and efficient security system based on advantages of DNA in identifying a person uniquely has led to many research. Based on the study of the research article the advantage of extracting DNA from saliva has advantages over blood sample usage in the extraction process. Further DNA derived from saliva can be sampled, stored and shipped with stabilizing agent at high temperature. Self-administration is possible in extracting a sample for enrollment of the sample in database, cost is reasonable and it is approximately around $24.

Table 2. Composition of saliva

Appearance: Watery, Opalescent, tasteless secretion
Daily secretion: 1.2 – 1.5 L
Water – 99.5%
Solid constituents – 0.5%
Inorganic solids – 0.2% Organic solids – 0.3%
Inorganic constituents NaCl, KCl, NaHCO3, Na2, HPO4, CaCO3, KSCN
Organic Constituents Mucin, Serum Albumin & Globulin, enzymes. Epithelial cells and Lymphocyte are present.

5. DNA Extraction Method from Saliva

DNA is a ubiquitous substance that was considered difficult to isolate but not anymore[10]. The following are the steps to extract DNA that is available in every living cell. Saliva gets its DNA from the cells that degenerate from the inside walls of cheeks. Figure 1 shows the D-SSS approach of DNA Extraction process.

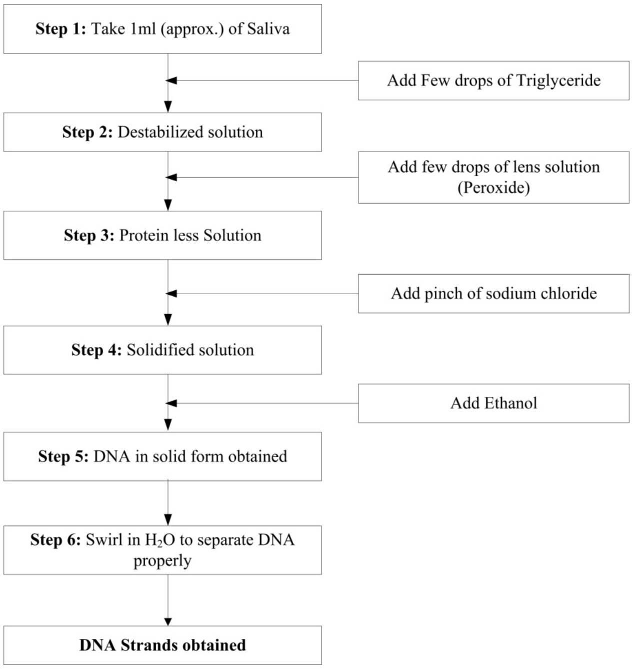
Step 1: Take 1ml (approx.) of Saliva
Add Few drops of Triglyceride
Step 2: Destabilized solution
Add few drops of lens solution (Peroxide)
Step 3: Protein less Solution
Add pinch of sodium chloride
Step 4: Solidified solution
Add Ethanol
Step 5: DNA in solid form obtained
Step 6: Swirl in H_2O to separate DNA properly
DNA Strands obtained

Figure 1. D-SSS approach - DNA extraction steps.

The following are the steps involved in separating DNA from saliva:

The device would be modeled in such a way that it absorbs saliva as input, which amounts to 1ml approximately.

Few drops of triglyceride are used to bust the cells to spill the contents into saliva. Triglyceride destabilizes the membranes of the cells, so the contents of saliva like cytoplasm and nuclear sugar, proteins and nucleic acid (RNA and DNA) gets mixed up with in the solution.

Protease is an enzyme that can break or reduce the amount of protein in any given solution. A little bit of lens solution or pineapple juice can be added to the solution (saliva +triglyceride) removes protein from the DNA precipitate.

Pinch of sodium chloride is added to solidify the solution. This process separated each DNA molecule from a nearby molecule by reducing the repulsive negatively charged force between them. The negatively charged regions of DNA get attached with some of the positively charged ions of sodium ions to shield them from the force mentioned.

Ethanol is added to the solidified substance to remove DNA in solid form from water by swirling it for few seconds.

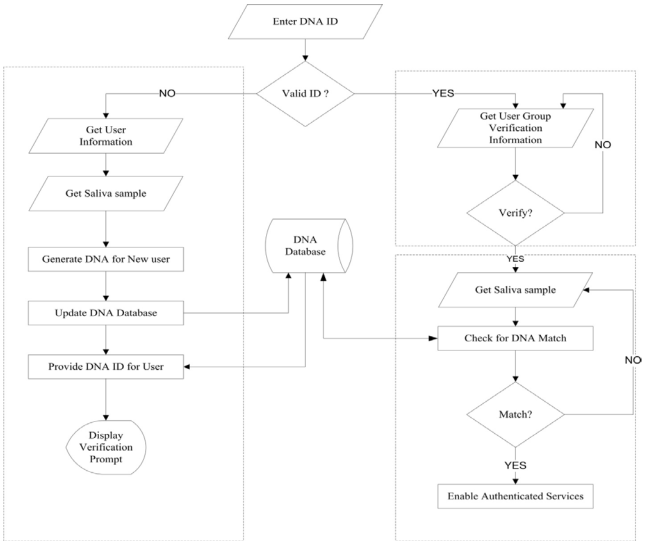

Figure 2. Flowchart of (D-SSS) A DNA based saliva security system.

DNA is a water loving substance (Hydrophilic) it can be obtained as a solid substance by adding ethanol, since it will not dissolve in it. DNA spooling is done to get the

Table 3. Salivary biomarkers with their possibilities for use

Saliva/ Oral Fluid Biomarkers	Possibilities for use
DNA	Standard genotyping, Bacterial infection, Diagnosing carcinomas of head and neck Forensics, Security and authentication
RNA	Viral/bacterial identification, Carcinomas of the head and neck
Proteins	Diagnosing periodontitis, Diagnosing carcinomas of the head and neck Detecting dental cavities
Immunoglobulins	Diagnosing viruses (HIV, hepatitis B and C)
Metabolites	Diagnosing periodontitis
Drugs & their metabolites	Monitoring drug abuse, Detecting of drugs in the body
Viruses and bacteria	Epstein-Barr virus reactivation (mononucleosis)
Cellular material	Diagnosing carcinomas of the head and neck

DNA strands out the solution, and these strands obtained after swirling in water. Table 3 shows the salivary biomakers with their possibilities for use.

6. How Saliva used in System Security

This section of D-SSS approach focuses on the value of saliva in enhancing security mechanism by specifying how the information is registered in the database and processed. Figure 2 shows the flowchart of (D-SSS) A DNA based Saliva Security System.

A new user has to register with the database by providing required details along with sample saliva through the device.

The devices store the user information along with the extracted DNA from the user sample in the database and provide DNA id for the user.

The devices prompt the user to verify the new DNA id thus, validates the user and the information submitted by the user.

The existing user provides the DNA id, which in turn is verified by the device and prompts the user to provide the user group id or information.

This information is used to check the user of a particular group and his usage authentication limits.

Now the user is requested to submit the saliva sample to the device.

The device performs the extraction process to identify the DNA and blood group etc.

Along with the unique DNA pattern and the user information like id and group, information authenticates a user as who he claims he is.

7. Conclusion

From the existing Biometric authentication methods, DNA is one of the best methods due to its high accuracy and allows both identification and verification. Our proposed scheme explains that DNA extracted from Saliva can be used in real life system security and could give more secure authentication to protect the system against security threats. DNA obtained from Saliva provides not only high-level authentication but also user-friendliness. The proposed work enables the authentication process in an efficient manner and as well as in a feasible way.

8. Acknowledgement

The work is supported with the project of "An insight study on Visual Secret Sharing scheme: Design and development of optimal strategies to reconstruct the secret image using Visual Cryptography in Healthcare applications" by SRM University, under Research Projects Engineering and Technology.

9. References

1. Authentication of forensic DNA samples [Internet]. [Cited 2009 Jun 16]. Available from: http://www.

benlaguer.org/documents/Frumkin_2009_Forensic-Science-International-Genetics.pdf.

2. Computer Security SS3: Biometric Authentication [Internet]. [Cited 2004]. Available from: http://www.cs.bham.ac.uk/~mdr/teaching/modules03/security/students/SS3/handout/.
3. Bubeck U, Sanchez D. Biometric authentication-technology and evaluation. San Diego State University. Term Project CS574, Spring; 2003.
4. Tan SC, Yiap BC. DNA, RNA, and protein extraction: The past and the present. Journal of Biomedicine and Biotechnology. 2009 Nov; 2009:1–10.
5. Saliva [Internet]. [Cited 2016 Aug 05]. Available from: https://en.wikipedia.org/wiki/Saliva.
6. Mun H-J, Li Y-Z, Jin K. Method of secure App user authentication from auto-login in the mobile device. Indian Journal of Science and Technology. 2016 Jun; 9(24):1–5.
7. Bhattacharyya D, Ranjan R, Alisherov AF, Choi M. Biometric authentication: A review. International Journal of u- and e- Service, Science and Technology. 2009 Sep; 2(3):13–28.
8. DNA Extraction from Marlene Schoeneck [Internet]. [Cited 2015 Apr 08]. Available from: https://plus.google.com/wm/2/se/1/106869062506793009451/posts/Pfp3JQSLY2Z.
9. Arita M, Kobayashi S. DNA sequence design using templates. New Generation Computers. 2002 Sep; 20(3):263–77.
10. Security system using biometric technology: Design and implementation of Voice Recognition System (VRS) [Internet]. [Cited 2008 May 13]. Available from: http://ieeexplore.ieee.org/document/4580735/.