Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 00 (2019) 000–000

Procedia Computer Science

www.elsevier.com/locate/procedia

International Conference on Computational Intelligence and Data Science (ICCIDS 2019)

Securing Medical data by Hidden Biometry and Steganography concepts

Malathi.P[1], Gireesh Kumar.T[2], Vaikunth Raghavan[3], Prithvi.V[4], Supraja R Nair[5], Uha Sai Lakshmi[6]

[1] *Department of Computer Science and Engineering, Amrita School of Engineering, Coimbatore, Amrita Vishwa Vidyapeetham, India*
[2] *TIFAC CORE in Cyber Security, Amrita School of Engineering, Coimbatore, Amrita Vishwa Vidyapeetham, India*
[3] *Department of Computer Science and Engineering, Amrita School of Engineering, Coimbatore, Amrita Vishwa Vidyapeetham, India*
[4] *Department of Computer Science and Engineering, Amrita School of Engineering, Coimbatore, Amrita Vishwa Vidyapeetham, India*
[5] *Department of Computer Science and Engineering, Amrita School of Engineering, Coimbatore, Amrita Vishwa Vidyapeetham, India*
[6] *Department of Computer Science and Engineering, Amrita School of Engineering, Coimbatore, Amrita Vishwa Vidyapeetham, India*

Abstract: Biometrics are means of identification but are prone to forgery. For this hidden biometrics like retina, veins, brain were introduced. It has the characteristic of being inconspicuous to outside world without scanning devices. Brain Biometrics is a novel field but a lot of work has been done to use brain's electrical activity as biometric verification. This paper focuses on securing the features extracted from the features of a brain biometric system with the help of concepts of steganography and image processing. Steganography conceals the confidential information within mediums or covers such as image, video, audio, DNA, etc. Steganography methods are adopted to hide the features of the brain inside a DNA cover, addressed as mask for implementing. The paper also aims to maintain the integrity of the features throughout the process as the performance of the biometric system is dependent on it.

Keywords: Biometrics, Brain biometrics, DNA Steganography, Hidden Biometrics, Steganography

1. Introduction

The term Biometrics was coined from the two Greek words bios=”life” and metron = “measure”. Human characteristics and traits can be measured and stored digitally in the form of biometrics. These can be used for access control on uniquely identifying an individual from a large groups that is under surveillance. This is feasible due to the distinctive, measurable characteristics that are present in the human biometrics naturally. Due to natures variability inherited in these parts of the body they are utilized as unique identifiers to describe individuals as a label. Physiological biometrics like fingerprint, face recognition, DNA, hand geometry, iris, and retina are utilize the uniqueness in shape to distinguish.

Humans differ from each other in actions and behaviour because of brain. Humans actually identity is cerebrum) that is unique to every individual is used. An extraction of features of this region to authenticate a person is the main motive of brain biometrics, which is a sub-field of hidden biometrics. But the trivial part that goes unnoticed is the securement of the features extracted from these scans. Any small feature of this cortical region, if changed or tampered can cause a chaos on verification of an individual.

Steganography provides a scheme to mask confidential information within a cover like image, DNA, audio, etc. The confidential information is hidden and secured from unauthorized users by means of using various algorithms to conceal. Based on the masking

*p_malathy@cb.amrita.edu , t_gireeshkumar@cb.amrita.edu, cb.en.u4cse15452@cb.students.amrita.edu , cb.en.u4cse15436@cb.students.amrita.edu, cb.en.u4cse15449@cb.students.amrita.edu, cb.en.u4cse15451@cb.students.amrita.edu

mediums used, it is classified as image steganography, DNA steganography, audio steganography, video steganography, etc. The image steganography has a lot of algorithms to conceal the data inside the image with various security features. As the embedding capacity of the image is low, it cannot mask a huge data inside it. To overcome this drawback of embedding capacity, DNA based steganography was introduced. The DNA sequences are an enormous dataset and have a high embedding capacity. The confidential information is obscured inside the DNA sequence using techniques like DNA insertion, substitution and complementary algorithm. Of the three techniques, the DNA insertion algorithm has the lowest cracking probability.

In this paper, the concepts of Digital Image Processing and Steganography are utilized to secure the brain feature used by the biometric system.

2. Related work

[1] Brain biometrics is a developing field over the last few years. Brain biometric provides security using the medical features of brain from onbiosignals, MRI and X-Ray images. These were initially used for the purpose of medical assessment of brains, here we use them for identification. [2] Use of onbiosignals such as ECG, EEG and EMG and MRI and X-Ray images are used to perform robust biometrics under the domain of hidden biometry. Geometrical features of brain like shape can be used to find inter variability of brain shape and used to identify the individuals. A work most similar to ours is the use of MRI images for identification. Extraction of brain surfaces from 3D level segmentation approach and geometrical descriptors from a 3D brain volume. [6] Wang's information hiding using DNA steganography used vigenere cipher scheme to secure confidential data and converted the ciphered text to binary and which is then hidden inside DNA sequence using DNA encoding algorithm. [7] Jiao's paper proposed a way to hide data inside a living organisms DNA through encryption. The message is converted to binary and made of DNA bases of codons (35 codons have been used in this paper). Encryption techniques like RSA, AES are used that enable mutation in DNA sequences silently. Similarly a decryption process is developed to retrieve the encoded information. [8] Mohammad developed a data concealment technique for cloud environments. In his paper he uses DNA complementary algorithm to encrypt his data and the upload it to the cloud. Any client accessing the cloud downloads the faked DNA sequences and reverses the complementary algorithm to get the data. [9] Peterson's paper gave a way embed data within DNA sets by using DNA substitution technique. The paper uses 64 symbols for encoding like S=AGC and counter the problem of attackers seeking repetitive letters or patterns using it. [10] Shiu proposed three methods of DNA hiding namely insertion, complementary and substitution. These methods hide a secret message within DNA sequences. Insertion hides the binary form of message among the binary form of DNA sequences and secures them. The paper also uses a substitution principle and also complementary pair generation using complementary rules and implements the other two methods. The cracking probability of all the three proposed methods, capacity, bits per nucleotide (BPN) values and payload are used as performance comparators. [11] Rishi Agarwal proposed a dictionary based substitution method. The algorithm uses codons for data hiding in DNA set. The lengths of codons in binary format are calculated and are appended with zeros if the length is not a multiple of six. This binary code of six bits is converted using the corresponding codons into DNA and sent to the receiver who reverses this process to decode the information. This improvised algorithm has a lower cracking probability than DNA insertion method.

3. Proposed algorithm

3.1 Problem definition

The problem aims to formulate a pragmatic and feasible solution to embed and hide features retrieved out of MRI scans into a DNA cover where they would seem inconspicuous and remain safe.

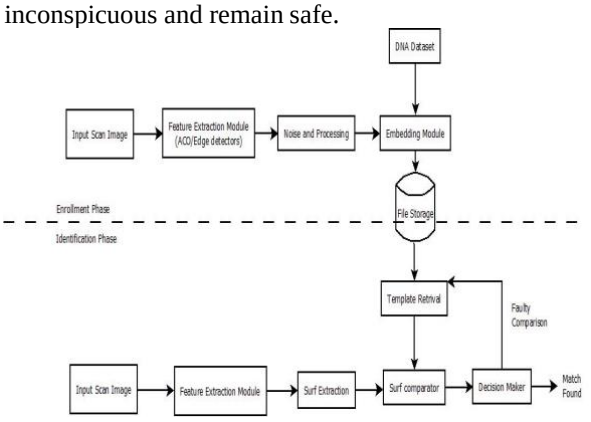

Figure.1 Overall System Architecture

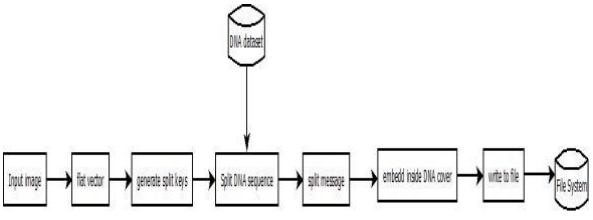

Figure.2 Basic Embedding Architecture

3.2 Encryption Phase

The sliced MRI region is taken from the feature extraction stages of the biometric system. The edges of

the image is extracted using the edge detection methods to get the required edges of the cortical region. This edge is then processed to get the clear. This image is then hidden inside a DNA cover addressed as mask using the insertion algorithm. The keys that have been generated for this entire process are saved and secured in a file using cryptographic methods. The masked output is now saved as the template in the biometric system database.

3.2.1 Steps for encryption

Step 1. Extract the edges for the input MRI image slice (addressed as 'i')

Step 2. Convert "i" to a flat single row binary sequence "I" of size "S"

Step 3. Randomly generate a binary sequence "r" whose elements sum up to "S"

Step 4. Split the sequence "I" as M= {Ir1, Ir2, Ir3…Irm}, i.e. split I into m elements depending on the values of array elements of "r".

Step 5. Convert the binary values in M to the DNA acids based on the dictionary rule adopted.

Step 6. Randomly generated number "K", which is less than size of M.

Step 7. Split the DNA sequence by K value.

Step 8. Using insertion algorithm, insert the values in M onto the DNA sequence which has been split into K divisions and generate "Y".

Step 9. Write the masked DNA "Y" onto a text file.

Step 10. Write "r" and "K" onto another file and encrypt the file using AES method.

3.3 Decryption and Identification Phase

The templates are retrieved along with their respective key files. Firstly the keys are decrypted and retrieved and with it, the cortical edges are obtained back from the mask by using the algorithm defined to reverse the insertion process. To validate the current extracted feature and the recovered templates, the SURF (speed up robust feature) are deployed and the match is verified. If found to be matching, the biometric system authenticates the enroller as identified or else moves on to look for another matching template in the database.

3.3.1 Steps for decryption

Step 1. Read the keys required to decrypt and store it into the variables "K" and "r", to skip DNA characters and number of message bits to be read.

Step 2. From Y skip K characters and read till the number of characters specified by the ri^{th} element and add it to the sequence M. Repeat this step until Y has been completely read by using the decryption logic of insertion algorithm.

Step 3. Convert the contents of M back to its binary format using the dictionary rule used as "I".

Steps for Identification

Step 1. Consider the current enrolled image as "E".

Step 2. From the database, extract and decrypt a stored template as "I".

Step 3. Obtain the surf points for both E and I and compare them.

Step 4. If they are a genuine match, identify them as valid, or else repeat the steps 1 to 3 for another template taken from the system.

4. Results and Discussion

By this research, we introduced a novel method to secure brain prints from MRI scans that act as biometric signature for brain biometric systems. Brain folds have intricacies that allow low inter variabilities. Features were extracted through edge detection. As result, we developed a steganography method to protect the prints. These results provide a promising solution to overcome spoofing issues that hinder the biometric model

The MATLAB R014b has been used for stimulation and implementation of the proposed algorithm because of its native support for image processing. The algorithm takes the input images generated by the mapping of curvilinear slices (that include the cerebral cortex) as 2D images from the 3D MRI brain scan models. The standard images from Omega database have been taken to design the system.

The images obtained through the encryption and decryption process depict a sample of output that is likely to be obtained in the case of a genuine and imposter match scenario. By analyzing the surf point matches in both the images, we can easily categorize and validate a person's identity.

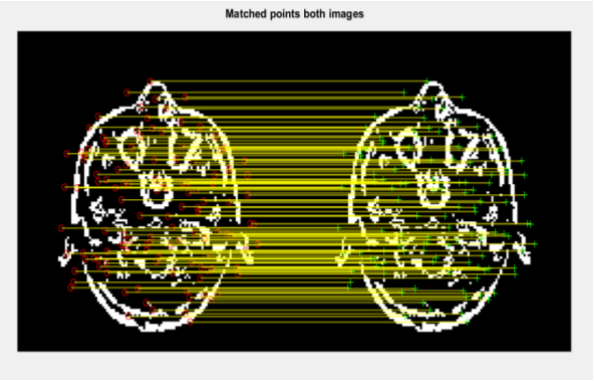

Figure.3 Genuine match example

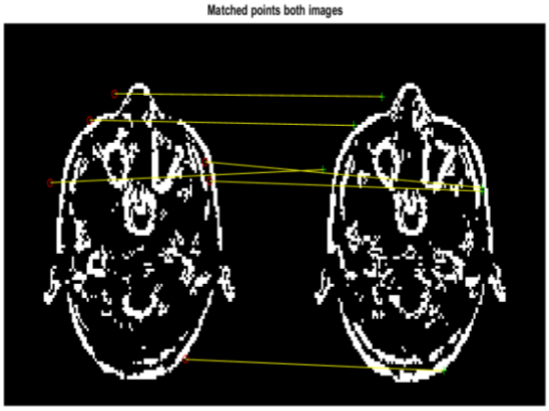

Figure.4 Imposter match example

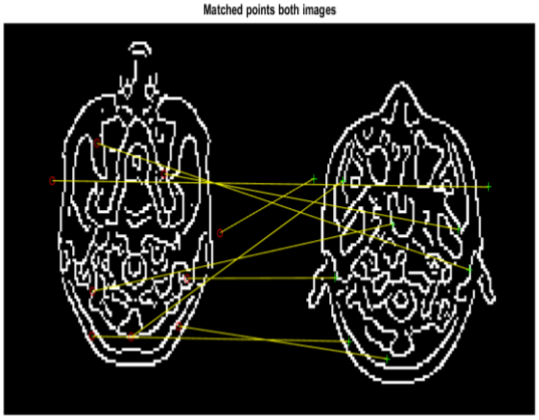

Figure.7 Imposter match example

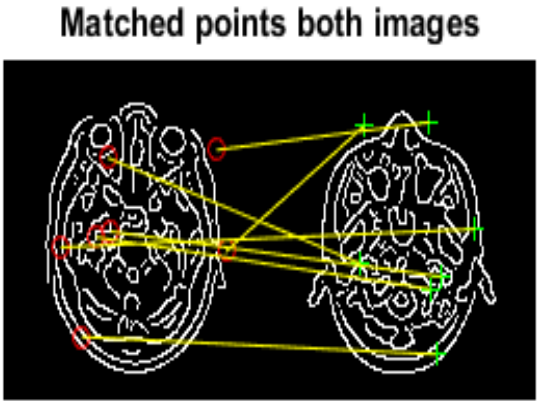

Figure.5 Imposter match example

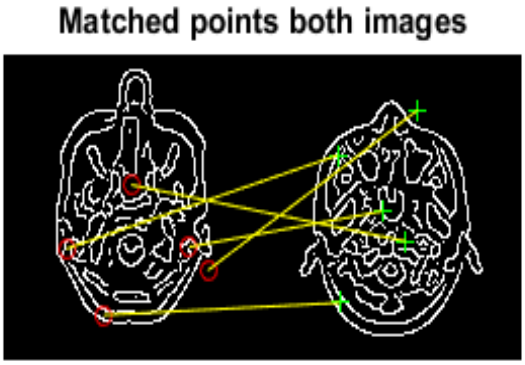

Figure.8 Imposter match example

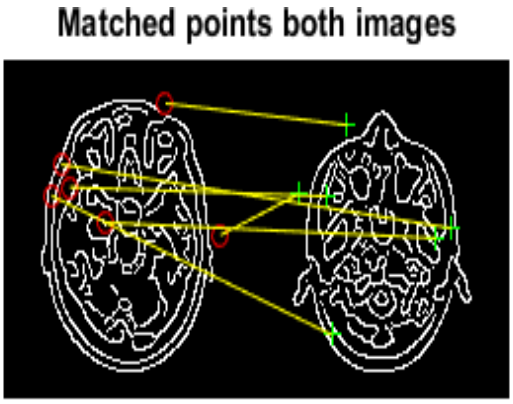

Figure.6 Imposter match example

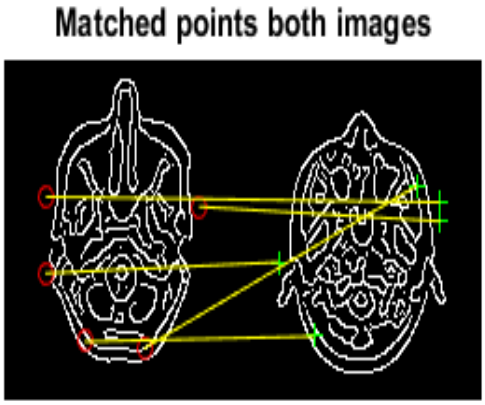

Figure.9 Imposter match example

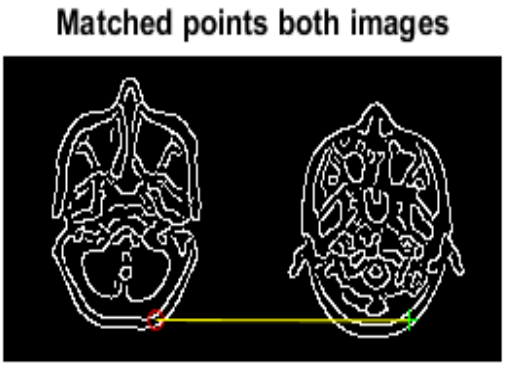

Figure.10 Imposter match example

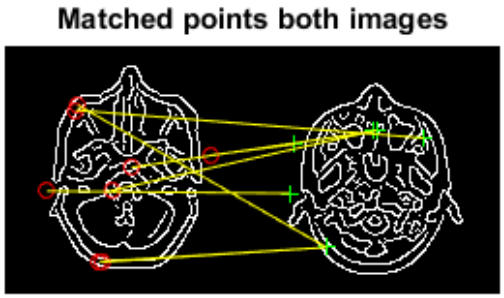

Figure.11 Imposter match example

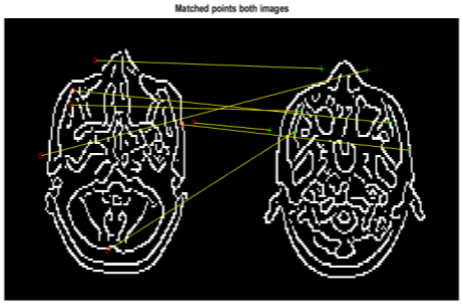

Figure.12 Imposter match example

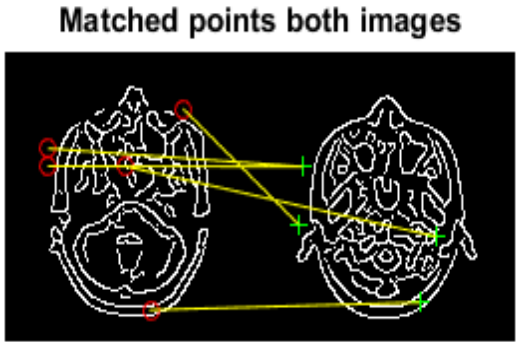

Figure.13 Imposter match example

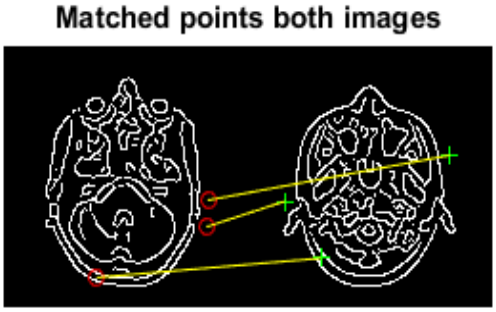

Figure.14 Imposter match example

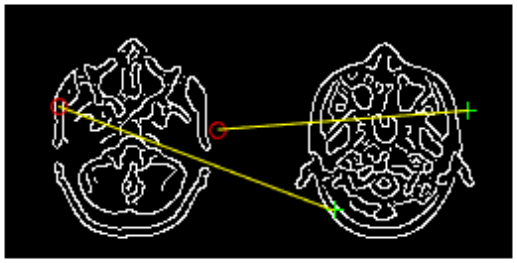

Figure.15 Imposter match example

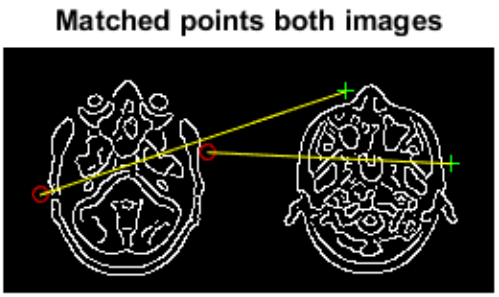

Figure.16 Imposter match example

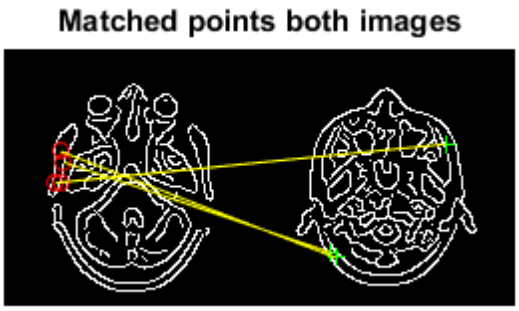

Figure.17 Imposter match example

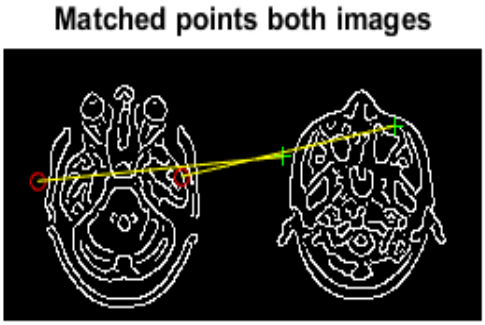

Figure.18 Imposter match example

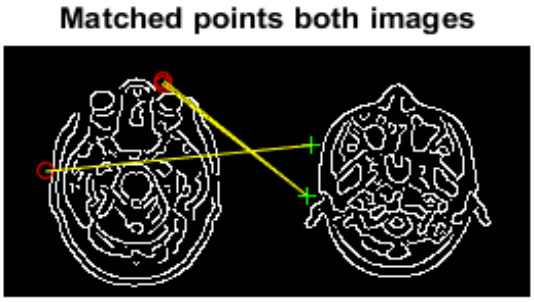

Figure.19 Imposter match example

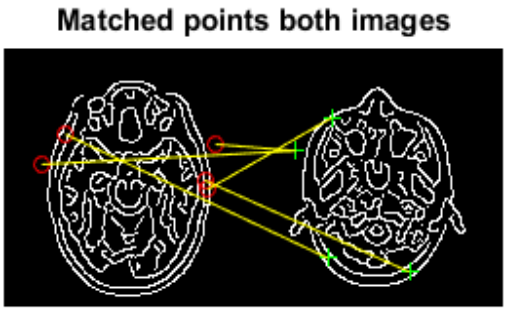

Figure.20 Imposter match example

5. Conclusion

The work presented in this paper is a novel technique to use the medical physical features extracted from the brain images which can uniquely identify the subjects and at the same time safeguard the traits extracted to validate the individual. The proposed system is the first system to extract as well as secure the brain biometry through encrypted processes. The inconspicuous nature of the secured data enhances its utility to be deployed for high security purposes. The algorithm is easily deployable with any medical imaging machine with slight modifications in software. With the advances in the brain scanning and imaging methods we expect that the brain biometric will become a trait in biometric verification technology for its high security.

References

[1] Maheshwari, S. & Choudhary, P. (2016). Hidden Biometric Security Implementation through Human Brain's Artificial Macro Structure. Procedia Computer Science, 78, 625-631.

[2] Aloui, K., Nait-Ali, A., & Naceur, M. S. (2018). Using brain prints as new biometric feature for human recognition. *Pattern Recognition Letters*, *113*, 38-45.

[3] Reshmi, K. C., Muhammed, P. I., Priya, V. V., & Akhila, V. A. (2016). A novel approach to brain biometric user recognition. *Procedia Technology*, *25*, 240-247.

[4] Yin, J. H. J., Fen, G. M., Mughal, F., & Iranmanesh, V. (2015, December). Internet of Things: Securing data using image steganography. In *2015 3rd International Conference on Artificial Intelligence, Modelling and Simulation (AIMS)* (pp. 310-314). IEEE.

[5] Khalifa, A. (2013, November). LSBase: A key encapsulation scheme to improve hybrid crypto-systems using DNA steganography. In *2013 8th International Conference on Computer Engineering & Systems (ICCES)* (pp. 105-110). IEEE.

[6] Wang, Z., Zhao, X., Wang, H., & Cui, G. (2013, May). Information hiding based on DNA steganography. In *2013 IEEE 4th International Conference on Software Engineering and Service Science* (pp. 946-949). IEEE.

[7] Jiao, S. H., & Goutte, R. (2009). Hiding data in DNA of living organisms. *Natural Science*, *1*(03), 181.

[8] Abbasy, M. R., & Shanmugam, B. (2011, July). Enabling data hiding for resource sharing in cloud computing environments based on DNA sequences. In *2011 IEEE World Congress on Services* (pp. 385-390). IEEE.

[9] Shiu, H. J., Ng, K. L., Fang, J. F., Lee, R. C., & Huang, C. H. (2010). Data hiding methods based upon DNA sequences. *Information Sciences*, *180*(11), 2196-2208.

[10] Shiu, H. J., Ng, K. L., Fang, J. F., Lee, R. C., & Huang, C. H. (2010). Data hiding methods based upon DNA sequences. *Information Sciences*, *180*(11), 2196-2208.

[11] Agrawal, R., Srivastava, M., & Sharma, A. (2014, December). Data hiding using dictionary based substitution method in DNA sequences. In *2014 9th International Conference on Industrial and Information Systems (ICIIS)* (pp. 1-6). IEEE.

[12] Vinodhini, R. E., & Malathi, P. (2018). DNA based image steganography. In *Computational Vision and Bio Inspired Computing* (pp. 819-829). Springer, Cham.

[13] Vinodhini, R. E., Malathi, P., & Kumar, T. G. (2017, January). A survey on DNA and image steganography. In *2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS)* (pp. 1-7). IEEE.

[14] Malathi, P., Manoaj, M., Manoj, R., Raghavan, V., & Vinodhini, R. E. (2017). Highly Improved DNA Based Steganography. *Procedia Computer Science*, *115*, 651-659.

Draft Changes

All the reviewer comments were addressed, and the following changes were made:

Conclusion

Before Change:

The work presented in this paper is a novel technique to use the medical physical features extracted from the brain images which can uniquely identify the subjects. The proposed system is mainly targeting high security. The algorithm is easily deployable with any medical imaging machine with slight modifications in software. Every time person has to get under medical imaging scan to get the brain image acquired. This may be cumbersome but due to advance in the brain scanning and imaging methods we expect that the brain biometric will become a trait in biometric verification technology for its high security.

A**fter Change:**

The work presented in this paper is a novel technique to use the medical physical features extracted from the brain images which can uniquely identify the subjects and at the same time safeguard the traits extracted to validate the individual. The proposed system is the first system to extract as well as secure the brain biometry through encrypted processes. The inconspicuous nature of the secured data enhances its utility to be deployed for high security purposes. The algorithm is easily deployable with any medical imaging machine with slight modifications in software. With the advances in the brain scanning and imaging methods we expect that the brain biometric will become a trait in biometric verification technology for its high security.

References

Before Change:

[1] Hidden biometry security implementation through human brain's Artificial Macro Structure
[2] Using brain prints as new biometric feature for human recognition, Kamel Aloui, Amine Nait-Ali, Mohamed Saber Naceur
[3] A Novel Approach to Brain Biometric User Recognition, Reshmi K.C., Ihsana Muhammed P., Priya V.V., Akhila V.A.
[4] Internet of Things: Securing Data using Image Steganography, Joanne Hwan Jie Yin, Gan May Fen, Fiza Mughal, Vahab Iranmanesh
[5] 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; 105-110.
[6] Wang Z, Zhao X, Wang H, Cui G. Information hiding based on DNA steganography. In 4th IEEE International Conference on Software Engineering and Service Science (ICSESS) 2013; 946-949.
[7] Jiao SH, Goutte R. Hiding data in DNA of living organisms. Natural Science 2009; 1(03):181.
[8] Abbasy MR, Shanmugam B. Enabling data hiding for resource sharing in cloud computing environments based on DNA sequences. In IEEE World Congress on Services (SERVICES), 2011; 385-390.
[9] Peterson I. Hiding in DNA. Proceedings of Muse. 2001:22.
[10] Shiu HJ, Ng KL, Fang JF, Lee RC, Huang CH. Data hiding methods based upon DNA sequences. Information Sciences 2010; 180(11):2196-208.
[11] Agrawal R, Srivastava M, Sharma A. Data hiding using dictionary based substitution method in DNA sequences. In 9th International Conference on Industrial and Information Systems (ICIIS), IEEE, 2014; 1-6

After Changes:

[1] Maheshwari, S., & Choudhary, P. (2016). Hidden Biometric Security Implementation through Human Brain's Artificial Macro Structure. *Procedia Computer Science*, *78*, 625-631.
[2] Aloui, K., Nait-Ali, A., & Naceur, M. S. (2018). Using brain prints as new biometric feature for human recognition. *Pattern Recognition Letters*, *113*, 38-45.
[3] Reshmi, K. C., Muhammed, P. I., Priya, V. V., & Akhila, V. A. (2016). A novel approach to brain biometric user recognition. *Procedia Technology*, *25*, 240-247.
[4] Yin, J. H. J., Fen, G. M., Mughal, F., & Iranmanesh, V. (2015, December). Internet of

Things: Securing data using image steganography. In *2015 3rd International Conference on Artificial Intelligence, Modelling and Simulation (AIMS)* (pp. 310-314). IEEE.

[5] Khalifa, A. (2013, November). LSBase: A key encapsulation scheme to improve hybrid crypto-systems using DNA steganography. In *2013 8th International Conference on Computer Engineering & Systems (ICCES)* (pp. 105-110). IEEE.

[6] Wang, Z., Zhao, X., Wang, H., & Cui, G. (2013, May). Information hiding based on DNA steganography. In *2013 IEEE 4th International Conference on Software Engineering and Service Science* (pp. 946-949). IEEE.

[7] Jiao, S. H., & Goutte, R. (2009). Hiding data in DNA of living organisms. *Natural Science*, *1*(03), 181.

[8] Abbasy, M. R., & Shanmugam, B. (2011, July). Enabling data hiding for resource sharing in cloud computing environments based on DNA sequences. In *2011 IEEE World Congress on Services* (pp. 385-390). IEEE.

[9] Shiu, H. J., Ng, K. L., Fang, J. F., Lee, R. C., & Huang, C. H. (2010). Data hiding methods based upon DNA sequences. *Information Sciences*, *180*(11), 2196-2208.

[10] Shiu, H. J., Ng, K. L., Fang, J. F., Lee, R. C., & Huang, C. H. (2010). Data hiding methods based upon DNA sequences. *Information Sciences*, *180*(11), 2196-2208.

[11] Agrawal, R., Srivastava, M., & Sharma, A. (2014, December). Data hiding using dictionary based substitution method in DNA sequences. In *2014 9th International Conference on Industrial and Information Systems (ICIIS)* (pp. 1-6). IEEE.

[12] Vinodhini, R. E., & Malathi, P. (2018). DNA based image steganography. In *Computational Vision and Bio Inspired Computing* (pp. 819-829). Springer, Cham.

[13] Vinodhini, R. E., Malathi, P., & Kumar, T. G. (2017, January). A survey on DNA and image steganography. In *2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS)* (pp. 1-7). IEEE.

[14] Malathi, P., Manoaj, M., Manoj, R., Raghavan, V., & Vinodhini, R. E. (2017). Highly Improved DNA Based Steganography. *Procedia Computer Science*, *115*, 651-659.

Other Changes made in the draft:

1) Format changed according to manuscript template guidelines.
2) Comparative analysis of this system cannot be made at this point as there are no such systems that extract brain biometrics and secure them at the same time as elucidated in the paper. This is a novel approach.
3) Images of higher quality cannot be obtained as the size restrictions imposed on the source data itself. The dataset is made of 128*128 pixels and the image is directly processed without altering its size. Thus the maximum quality which had been obtained is added to the results of this study.