Different Attack Patterns for Deep Brain Implants By Using CNN

Gophika.T, Aarthi.R, Akash.R, Anish.V

Abstract: Deep Brain Stimulation (DBS) is a neuro surgical procedure that is a neuro stimulator (brain pacemaker) is placed which can send the electrical impulses, through implanted electrodes, to specific targets of brain for the treatment of neurological disorders such as Parkinson, movement disorder, epilepsy, and psychiatric disorders. The device must be fully secured since it directly affects the mental, emotional and physical state of human bodies which may lead to patient's death. The adversary can impair the motor functions, or modify the emotional pattern of patient by stimulating fake signals by Deep Brain Stimulators (DBSs). This project uses deep learning methodology to predict different attack stimulations in DBSs. This proposed work uses a long short-term memory, a type of Convolutional Neural Network (CNN) which is a class of deep neural network commonly applied for visual imaginary for forecasting and predicting rest tremor velocity (characteristic used to evaluate intensity of neurological disorder) which helps in diagnosing fake versus original stimulations. This methodology was used to detect different attack patterns efficiently.

Index Terms: Convolutional Neural Network, Deep Brain Stimulators, Deep Learning, Implantable Medical Devices, Machine Learning, Neural Network, Security.

1 INTRODUCTION

The sensory and neurological systems in human patients is pulled by using the electrical stimulation. Parkinson, movement disorder, epilepsy, and psychiatric disorders are treated by using Deep brain stimulation. It has shown that most of people are affected by movement disorders. It is estimated that over 1,80,000 individuals below 70years of age are affected by Parkinson diseases. There are other factors that also influence Parkinson diseases such as depression, stress, etc, more than 18 million people are affected due to depression and other mental problems. Despite of psychiatric problems, DBS is also used for treating hypertension, obesity and dietary issues. It is also proposed for treatment of neurological pains and headaches. Some of the frameworks that are utilized as a part of DBS are Medtronic65 and Advanced Neurological Frameworks. Stroke or also called as brain attack occurs when there is no proper blood flow or circulation to the brain. When the blood flow decreases the brain cells will die which results in lack of oxygen [15]. Strokes are classified into two types such as (i)Strokes that are caused by the blockage of blood flow and and (ii) Strokes thar are caused due to bleeding in the brain [24]. The most frequent cause of stroke is ischemic stroke that is caused due to blockage of blood vessel in the brain or neck region, which is responsible for more than 80 percent of strokes [28]. The three conditions of blockage of stem are:(i)Thrombosis are defined as clot formed within blood vessel in the neck or brain region (ii)Embolism which is defined as when the clot is moved from one part of the body to the another part such as from the heart to the brain and(iii) Stenosis is defined as abnormal narrowing of blood vessel or leading to the brain. The second type of stroke is Haemorrhagic stroke which are caused by the bleeding into the brain or the spaces that are surrounded to the brain region [32]. The two key factors that will lower the risk of death or disability from stroke are (i) control stroke's risk factors and (ii) known stroke's warning sign. The scientific research that conducted by the NINDS states the warning signs of strokes as sudden numbness, sudden confusion, sudden trouble in vision, trouble in walking and severe headache.

- *Aarthi. R is currently pursuing UG scholar in Electronics and Communications Engineering in Easwari Engineering College ,India.Email:aarthiramesh1505@gmail.com*
- *Akash. R is currently pursuing UG scholar in Electronics and Communications Engineering in Easwari Engineering College ,India .Email:akashrajendiran11@gmail.com*
- *Anish. V is currently pursuing UG scholar in Electronics and Communications Engineering in Easwari Engineering College ,India.Email :anish.sbioa@gmail.com*
- *Gophika. T, Assistant Professor, Department of Electronics and Communication Engineering in Easwari Engineering College, India. E-mail: gophi487@gmail.com*

Fig. 1. Deep Brain Stimulators

2 IMPLANTED MEDICAL DEVICES

Wireless Implanted Medical Devices (IMD) have the capability of transmitting the information without any wired connection. This may create a platform for attackers to steal the information with an intent of harming the patient [11].

This can be done by reprogramming the implanted medical devices. For example, a trespasser can learn all the private data by listening to IMD radio frequency without any effects [16]. It can access to the data of oscilloscope, programming radio and other medical devices. Another type of attack can be introduced by the trespasser where he has the ability to create radio transmissions to reply repeated operations [12],[13]. There are many types of solutions for addressing the security issues, but Bio-metric based approach has unique physiological characteristics and authentication for human body [18]. It is a secured and light weight system but it lacks in accommodating the bio-metric changes with respect to time [20],[21]. The distance between the IMD and the caregiver can be estimated by distance-based approaches by using the transmitted and the received data through piezoelectric elements [15]. This system fails science the patient and the attacker can make physical contact and it may lead to weak the authentication [41]. Therefore, key management protocol is used for providing authentication only to the authorized users using symmetric [15], physiological [25] signals for key generations. This paper classifies different attack patterns of DBS and provides efficient and fast model for improving security in DBS with deep learning strategy. Following objective are achieved:

1. A deep leering classifier to predict and consecutive brain stimulation pattern by designing and training Long short-term memory (LSTM)
2. Different types of attacks patterns are emulated and classified in deep brain implants. Prediction mechanism is developed by using different attack patterns and can be used by the attackers.

3 PROPOSED METHOD

3.1 Motivation

Applications of biological domain concepts such as body and brain operation to practical problems in other domain like security and other interruption problems are called Bio-inspired system. This have caught the attention of scientific community in many different fields like computer science, mechanical, agriculture, energy, etc. When compared to other fields Biological inspired approaches seems to be favourable and are considered stronger. In contrast to the existing models it is observed that it requires regular updating, replacement, nourishing, bio-inspired models that have the ability to maintain themselves and also that could adapt to the changing conditions. Therefore, scientists and engineer from many domains are participating in finding innovative design architecture to overcome from different challenges. In upcoming years, we may have machines that have the ability to repair themselves like how the skin heal themselves from the injury. We may expect more designs in future that are related to flexible, self-healing bio- inspired models.

3.2 Neural Network

Neural networks learning strategy, is inspired from biological neural networks (human brain). The biological neural network contains interconnected neurons used to commerce the messages from one another. The interconnections have weights that can be tuned with respect to experience, thus making neural networks for learning. The objective here is not to make practical models of the human brain, but rather to create robust and effective information structures that we can use to model difficult problems. Neural networks are classified into 6 types such as (i) Feedforward Neural Network (ii) Radial Basis Function Neural Network (iii) Kohonen Self Organizing Neural Network (iv) Recurrent Neural Network (RNN) (v) Convolutional Neural Network (CNN) (vi) Modular Neural Network. Recurrent Neural Network (RNN) is an Artificial Neural Networks where the connections are between the nodes i.e. from the directed graph down the temporal sequence. Various length sequence of inputs can be processed in RNN by using internal memory. This is used in unsegmented, hand recognition, speech recognition. The main disadvantage of Recurrent Neural Network (RNN) is that it is difficult to train, gradient vanishing and exploding problem and processing of very long sequence is not possible to overcome these problems Convolutional Neural Network (CNN) is introduced. When compared to other neural networks CNN have the ability to detect important features itself without the help of human supervision. It is suitable for images. CNN takes fixed size of input and provides fixed size of output.

3.3 Convolutional Neural Network

In machine learning, visual imagery is being successfully analyzed by using Convolutional Neural Network (CNN or ConvNet) which is a class of deep, feed-forward artificial neural networks. Shift Invariant or Space Invariant Artificial Neural Network (SIANN) are defined as minimal pre-processing requirement in CNNs to design a variety of multiplayer perceptions that are based on their shared-weights architecture and translation in variance characteristics. The connectivity pattern of the convolutional network between the neurons that resembles the animal visual cortex organization are the inspiration for the biological processes. It uses respective field which is defined as the individual cortical neurons respond to stimuli only in the restricted region of the visual field. The entire visual field is covered by the overlapping of the different neurons partially in respective fields. CNNs are used because that uses relatively little pre-processing when compared to other image pre-processing algorithms, that means the network learns traditional algorithms filters that were hand-engineered. The major advantage this algorithm is that the independence from prior knowledge and human effort in feature design. CNN consist of many layers like an input layer ,an output layer and many hidden layers. The hidden layers in CNN are convolutional layer, pooling layer, fully connected layer and normalized layer. Each layer perform different operation like convolutional layer will apply convolution operation to the input image and pass it to the next layer. The convolutional layer will reduce the image size by 5x5 for learnable 25 free parameters. Fully connected layer is used to connect every neuron in one layer to every neuron in another layer.

3.3 Designing and Training

The deep brain stimulators are type of wireless implantable medical device which is used to treat neurological disorders by stimulations inside the human brain . Many patients have progressively benefited through DBS but it includes several security implications. Security is most important because it can directly affect both the mental and physical orientation. Long Short-Term Memory is utilized in this project and a type of Convolutional Neural Network(CNN), to predictand forecast the pattern of DBS. To study the intensity of neurological disorders which is examined by Rest Tremor Velocity (RTV) . To design and train the Convolutional Neural Network(CNN) we examined RTV values.

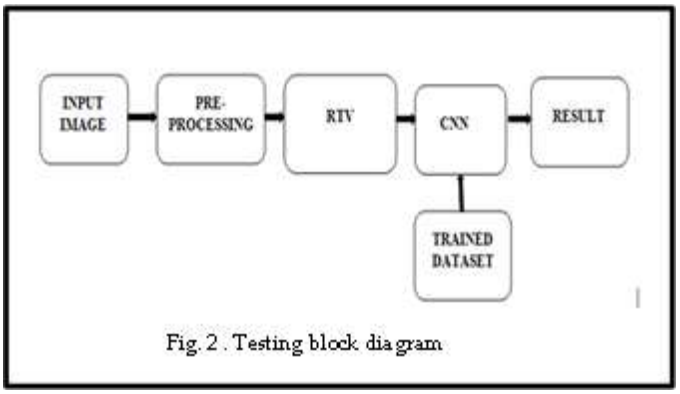

Fig. 2 . Testing block diagram

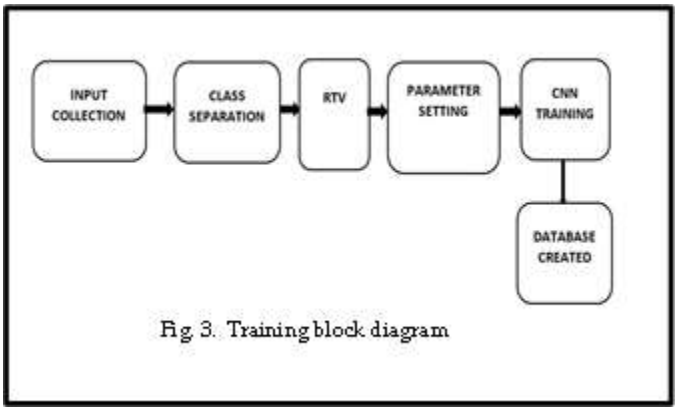

Fig. 3. Training block diagram

To emulate and classify different attack strategies various attack patterns were introduced in the DBS framework. The model was able to classify different attack patterns in the DBS with smaller loss values and minimal training time as the result. The proposed framework will be implemented on a real deep brain stimulator environment with real RTV measurement, in the near future. The performance of the framework in terms of accuracy and reliability can be evaluated , genuine and fake measurements will be classified and predicted at run time. The pre-processing time in CNN is less when comparing other image algorithms This independence is the major advantage from prior knowledge and human effort . In CNNS there is an input and an output layer, and multiple hidden layers that is, convolutional layers, pooling layers, fully connected layers and normalization layers . The process is described as convolution in neural networks. Mathematically it is a cross-correlation. In the matrix it only has significance for the indices, and thus which weights are placed at which index.

4 RESULTS AND DISCUSSION

Different attack patterns were detected by using Deep brain stimulators (DBS). The result obtained by this model shows that this model could detect different attack patterns with smaller lass value and minimal training time by using DBS. When compared to the discontinuous and arbitrary attack patterns (stuck-at and noise) and continuous and single pulse attack, the loss value is less in continuous and single pulse attack which are spike, outlier, incremental, chronic. The maximum loss value occurs in stuck-at and noise attack pattern since the patten is hard to be predicted more training time is required. A flag was raised when there is a difference in predicted RTV and true RTV and consecutive iterations was studied to predict emulated attack. Emulated attack strategies where classified in the deep brain stimulators and therefore a flag was raised in this model. By observing the parameters like signals amplitude, fluctuation amplitude, spectral concentration and median frequency LSTM were able to detect the abnormality in RTV which is calculated by observing next 10 times steps. The next epoch is predicted by using LSTM. For each step-in time for 700 steps the predicted RTV value and the true RTV value exceeds 50-times. The RTV should be predicted approximately zero even after the attack is introduced this is taken care by the LSTM in the system. For example, RTV could reach up to 50 in spike attack but the system predicts that RTV should not exceed zero based on the learning. RTV values come in range of 0 to 3 in stuck-at and incremental attack patterns since the pattern is hard to be predicted more training is required. When they exhibit difference in predicted and true RTV a flag was raised and emulated attack is predicted.

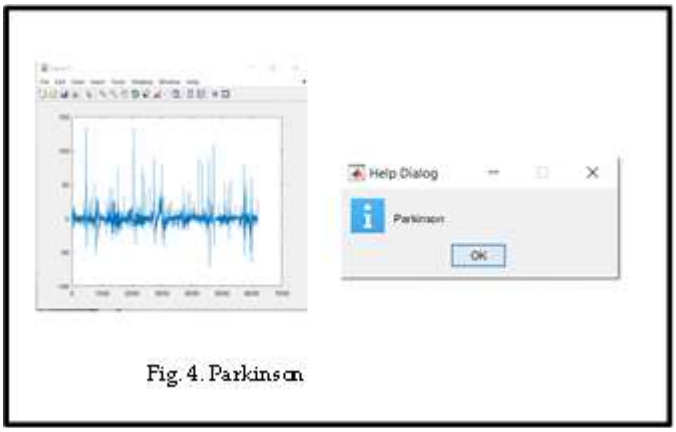

Fig. 4. Parkinson

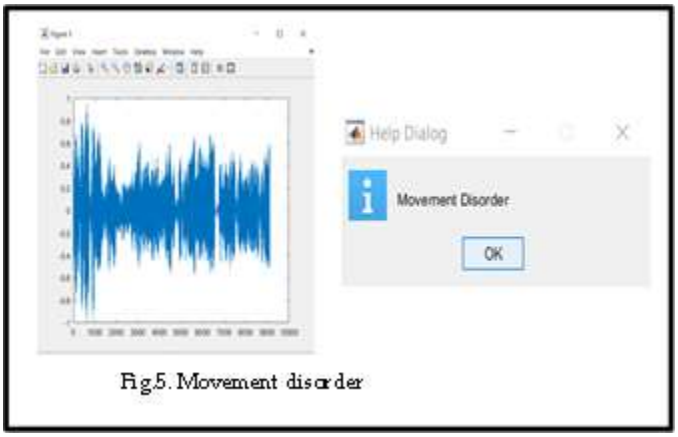

Fig.5. Movement disorder

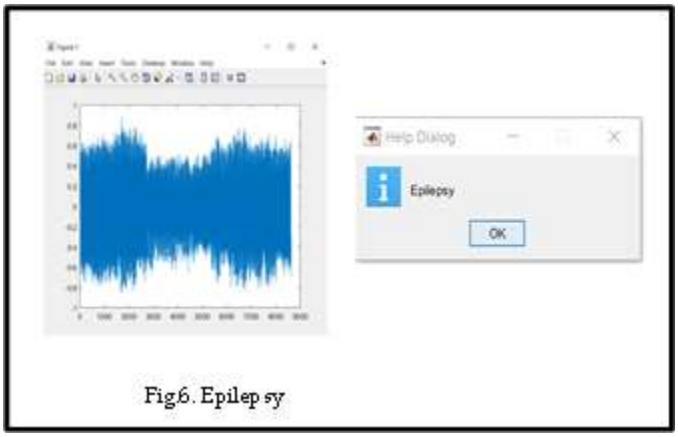

Fig6. Epilepsy

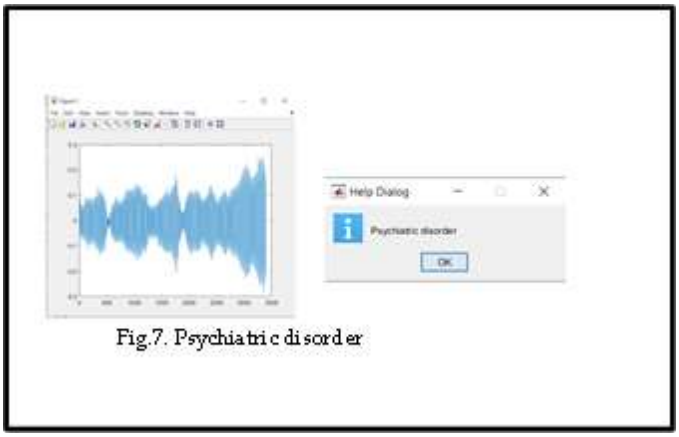

Fig.7. Psychiatric disorder

5 CONCLUSIONS

Neurosurgical procedure which involves placement of neuro stimulator that sends electrical pulses through implanted electrodes to specific part of the brain is known as Deep Brain stimulation. It is used for the treatment of neurological disorders such as Parkinson, movement disorder, epilepsy and psychiatric disorder. Since it affects the mental, emotional and physical state of human bodies which may lead to patient's death so it should be fully secured. The motor functions can be impaired by the adversary or emotional pattern of the patients by stimulating fake signals by DBSs. Deep learning adversary or emotional pattern of the patients by stimulating fake signals by DBSs. Deep learning methodology is used to predict different attack stimulations in DBSs. Long term memory is used in the proposed work and for forecasting and predicting rest tremor velocity which helps in diagnosing fake vs original stimulations by a type of Convolutional Neural Network (CNN). Different attack patterns can effectively detect by this method. This model effectively finds out the different attack patterns in the DBS with smaller loss values and minimal training time. It can be implemented on a real deep brain stimulator environment with real RTV measurements in near future. The performance of the frame work in terms of accuracy and reliability, genuine and fake measurements can be classified and can be predicted at run time.

REFERENCES

[1] Henna Rathore, Abdulla Khalid Al-Ali, Amr Mohamed, Xiaojiang Du2, Mohsen Guizani, "A Novel Deep Learning Strategy for Classifying Different Attack Patterns for Deep Brain Implants" in Proc. IEEE,2019.

[2] D. M. Long, ``Electrical stimulation of the nervous system for pain control,'' Electroencephalogram. Clin. Neurophysiology. Suppl., 1978.

[3] T. Parkinson, ``Appeal for deep brain stimulation, history of deep brain stimulation,'' Tech. Rep., Jun. 2018.

[4] J. Gardner, ``A history of deep brain stimulation: Technological innovation and the role of clinical assessment tools,'' Social Stud. Sci., 2013.

[5] J. M. Schwalb and C. Hamani, "The history and future of deep brain stimulation," Neurotherapeutics, 2018.

[6] Deep Brain Stimulators (DBS) Market Analysis by Application (Pain Management, Epilepsy, Essential Tremor, Obsessive Compulsive Disorder, Depression, Dystonia, Parkinsons Disease) And Segment Forecasts To 2020, Market Research Report, 2015.

[7] Deep Brain Stimulators Market Worth $1.6 Billion by 2020, Grand View Research, 2015.

[8] E. R. Dorsey et al., ``Projected number of people with Parkinson disease in the most populous nations, 2005 through 2030,'' Neurology, 2007.

[9] M. Leone et al., ``Deep brain stimulation and cluster headache,'' Neurological Sci., May 2005.

[10] M. B. Keller, ``Issues in treatment-resistant depression,'' J. Clin. Psychia-try, vol. 66, pp. 512, Jan. 2005.(2017).

[11] H. Rathore, ``Artificial neural network,'' in Mapping Biological Systems to Network Systems. Springer, 2016.

[12] Z. E. Ankarali, Q. H. Abbasi, A. F. Demir, E. Serpedin, K. Qaraqe, and H. Arslan, ``A comparative review on the wireless implantable medical devices privacy and security,'' in Proc. EAI 4th Int. Conf. Wireless Mobile Commun. Healthcare (Mobihealth), Nov. 2014.

[13] C. Li, A. Raghunathan, and N. K. Jha, ``Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system,'' in Proc. 13th IEEE Int. Conf. e-Health Netw. Appl. Services (Healthcom), Jun. 2011.

[14] N. Paul, T. Kohno, and D. C. Klonoff, ``A review of the security of insulin pump infusion systems,'' J. Diabetes Sci. Technol., 2011.

[15] D. Halperin et al., ``Pacemakers and implantable cardiac debrillators: Software radio attacks and zero-

power defenses," in Proc. IEEE Symp. Secur. Privacy, May 2008.
[16] W. Burleson, S. S. Clark, B. Ransford, and K. Fu, ``Design challenges for secure implantable medical devices," in Proc. 49th Annu. Design Autom. Conf., Jun. 2012.
[17] D. Halperin et al., "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses," in Proc. IEEE Symp. Secur. Privacy, May 2008.
[18] J. Radcliffe, "Hacking medical devices for fun and insulin: Breaking the human SCADA system," in Proc. Black Hat Conf. Presentation Slides, 2011.
[19] H. Rathore, A. Mohamed, A. Al-Ali, X. Du, and M. Guizani, "A review of security challenges, attacks and resolutions for wireless medical devices," in Proc. 13th Int. IEEE Wireless Commun. Mobile Comput. Conf. (IWCMC), Jun. 2017.
[20] H. Rathore et al., "Multi-layer security scheme for implantable medical devices," Neural Comput. Appl., Oct. 2018.
[21] H. Rathore, A. Al-Ali, A. Mohamed, X. Du, and M. Guizani, "DTW based authentication for wireless medical device security," in Proc. IEEE 14th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC), Jun. 2018.
[22] K. B. Rasmussen, C. Castelluccia, T. S. Heydt-Benjamin, and S. Capkun, "Proximity-based access control for implantable medical devices," in Proc. 16th ACM Conf. Comput. Commun. Secur., 2009.
[23] B.Kim ,J.Yu ,and H.Kim, "In-vivo NFC: Remote monitoring of implanted medical devices with improved privacy,"in Proc.10th ACM Conf. Embedded Netw. Sensor Syst., 2012.
[24] K. Singh and V. Muthuk kumarasamy, "Authenticated key establishment protocols for a home health care system," in Proc. 3rd Int. Conf. IEEE Intell. Sensors, Sensor Netw. Inf. (ISSNIP), Dec. 2007.
[25] G. Zheng, G. Fang, R. Shankaran, M. A. Orgun, and E. Dutkiewicz, "An ECG-based secret data sharing scheme supporting emergency treatment of implantable medical devices," in Proc. IEE, 2015
[26] E Int. Symp. Wireless Pers. Multimedia Commun. (WPMC), Sep. 2014.
[27] L. Pycroft et al., "Brainjacking: Implant security issues in invasive neuromodulation," World Neurosurgery, Aug. 2016.
[28] T. Denning, Y. Matsuoka, and T. Kohno, "Neurosecurity: Security and privacy for neural devices," Neurosurgical Focus, 2009.
[29] H. Rathore, "Bio-inspired approaches in various engineering domain," in Mapping Biological Systems to Network Systems. Springer, 2016.
[30] X. Hei, X. Du, S. Lin, I. Lee, and O. Sokolsky, "Patient infusion pattern based access control schemes for wireless insulin pump system," IEEE Trans. Parallel Distrib. Syst., Nov. 2015.
[31] H. Rathore, A. Al-Ali, A. Mohamed, X. Du, and M. Guizani, "DLRT: Deep learning approach for reliable diabetic treatment," in Proc. IEEE Globecom, Dec. 2017.
[32] H. Rathore, L. Wenzel, A. K. Al-Ali, A. Mohamed, X. Du, and M. Guizani, "Multi-layer perceptron model on chip for secure diabetic treatment," IEEE Access, 2018.
[33] X. Hei and X. Du, "Biometric-based two-level secure access control for implantable medical devices during emergencies," in Proc. IEEE INFOCOM, Apr. 2011.
[34] X. Du, Y. Xiao, M. Guizani, and H.-H. Chen, "An effective key management scheme for heterogeneous sensor networks," Ad Hoc Netw., 2007.
[35] X. Hei, X. Du, J. Wu, and F. Hu, "Defending resource depletion attacks on implantable medical devices," in Proc.IEEE GLOBE COM, Dec.2010.