Towards Deep Secure Tele-Surgery

Pedram Fekri[1], **Peyman Setoodeh**[1], **Fariba Khosravian**[2], **A.A. Safavi**[1] **and Mehrdad H. Zadeh**[3]
[1] School of Electrical and Computer Engineering, Shiraz University, Shiraz, Iran
[2] Tech Training Zone, LLC, Grand Blanc, MI, USA
[3] Electrical & Computer Engineering Department, Kettering University, Flint, MI, USA

Abstract - *This paper reports the latest results of our study on developing a new approach to secure tele-surgery systems as human-in-the-loop systems, using deep learning. In this approach, surgical behavior of expert surgeons are modeled and used to discriminate between valid commands generated by a remote surgeon and commands generated by a potential intruder. In tele-surgery, a remote surgeon and a surgical robot interact with each other through a network on the Internet or satellite. Surgical commands are transmitted to a robot manipulator and the robot transmits the feedback arising from executed commands to the surgeon. The threat of data manipulation and modification that streaming through this network undoubtedly is one of the most important security challenges. In this study, we propose a solution based on machine learning algorithms to detect manipulated or wrong commands transmitted by a potential remote user during a specific tele-operated surgical procedure. The proposed method protects the teleoperation surgical system from being hacked by attackers. We use a surgical simulation environment to simulate and collect essential data for training and evaluating the model in a supervised manner. The performance of system is tested in real-time to evaluate it during actual surgeries. Experimental results show that the trained model is able to detect and prohibit the execution of the manipulated command by the robot.*

Keywords: Haptic, Tele-operation, Deep Learning, LSTM, Recurrent Neural Networks, Security.

1 Introduction

Teleoperation surgical system is a subcategory of telemedicine and provides facilities of interaction between human operators and robots. Teleoperation surgical robotics as an application of teleoperation has attracted a lot of attention in the community. The system eliminates distance limitation in the medical surgeries. In fact, the surgeon performs surgical procedures without attending the surgical room, instead, transmits commands to surgical robots utilizing a robot manipulator device. The surgical robot performs operation based on received commands and sends information feedback to the robot manipulator device. The surgeon senses the robot feedback via the robot manipulator device. The system uses a network with various media such as satellite, ad hoc wireless or Internet, to make a connection between surgeon and robot. This system can be used in case of occurrence of an unforeseen problem, disaster or any hardship occasion. Feasibility and applicability of tele-surgical system has been exhibited and proven [1] [2]. Varieties of surgical issues such as Laparoscopy surgery utilize these systems [3]. Recent works are partially focused on designing surgical teleoperation system in the case of devising accurate and fast transmission method and vanishing network latency [1] [2]. Developing a simulated environment interacting with robot manipulator devices to approach human-robot interaction or medical resident training is another case of study [4].

When data, which contains master and slave messages is transmitted over a network, especially, if the teleoperation system is used in a battlefield or a disaster area, potentially it has the risk to be manipulated by a middle man. This is vital to guarantee the security of message transferred over the network because modification or hijacking of these messages may lead to irreparable wounds for patients. The important problem that takes place in cyber-security category is divided into three subcategories as follows [2]:

- Intention modification: an attacker aims to modify surgeon (master) commands toward the robot (slave) while data packets are transferred over the network and surgeon has no access to them. It is obvious that intention modification may cause wounds due to incorrect received commands and robot unusual movements.

- Intention manipulation: an attacker aims to modify transmitted feedback messages toward the surgeon based on the results of the executed commands. The feedback messages may contain haptic feedback signals or video streams. In this type of data manipulation, surgeon may be deceived and become bewildered based on these incorrect feedback messages.

- Hijacking: an attacker bans all access control of a surgeon and performs his/her own commands.

In [5], authors exerted a network protocol based on authentication and authorization to secure the connection between master and slave devices. In [6], a method was proposed based on Kalman Filter to detect system attacks. In [7], authors defined security problem as a discrete-time linear dynamical system that supervises data packet transmission and tries to find optimal solution. Another network secure communication protocol was introduced in [8] for application of military tele-surgical robot. An information coding method was devised in [9] to establish a secure wireless connection between master and slave based on encrypting messages by

key. As discussed, most of related work serve the teleoperation security by using different network protocols and data encryption approaches.

In this work, we focus on proposing a security solution based on machine learning algorithms to solve intention manipulation problem in tele-surgical procedures. We assume an expert will generate valid commands and a novice will generate invalid commands to transmit toward the surgical robot. Both the expert and the novice act as two roles of system. In contrast to other works, to make a secure teleoperation surgery, our proposed solution attempts to model the valid behavior of surgeon for detecting the invalid commands. The surgeon behavior emerges from robot manipulator device signals instead of data based on visual gesture.

Accordingly, we define a binary classification problem regarding these system roles and the goal of our system is to model the surgical behavior of both expert and novice while operating in a simulation environment with a deep neural network in a supervised manner.

We utilize an orthopedical tele-surgical drilling simulator to gather data for creating a dataset in order to train the model. We extract features of the signal emerging from the simulator while expert surgeons operate using the simulation environment. In addition, these experts pretend to operate as novice surgeons for gathering the data associated to the novice class. The dataset contains more than 30000 records that each sample is represented in a 35-dimension feature space. We train a deep recurrent neural network with this dataset and evaluate the performance of the model in real-time to detect whether the surgeon is an expert or not.

The main contributions of our proposed solution are summarized as follows:

- Our solution provides an observant system, which controls transmitted messages between robot manipulator device and surgical robot for detecting and prohibiting any unusual commands regardless of any network protocol or information coding.

- The system is able to distinguish a manipulated command from a valid command as well as to detect probable expert mistake commands during surgical operations.

- The system uses a dataset, which has been collected using an orthopedical telesurgical drilling simulator.

The rest of paper is organized as follows: the general explanation of proposed method is presented in section II. Section III contains data preparation and deep learning part with theoretical discussions. Section IV provides computer experiments. The paper concludes in the final section.

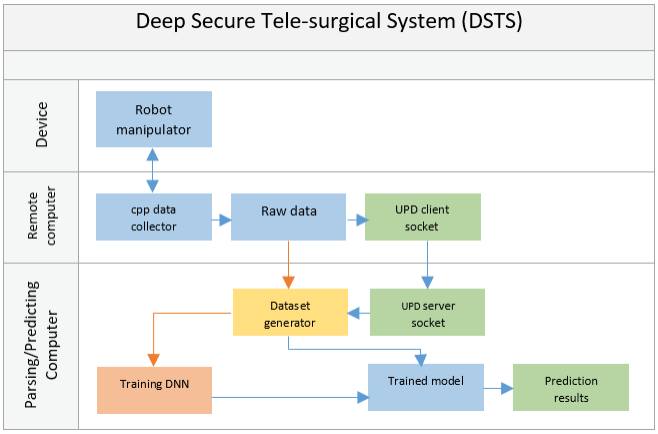

Fig. 1 This block diagram shows the secure tele-operation surgical system data flow. Dataset generator is used in both training (offline) and testing (online) phase

2 Deep secure tele-surgery system

Learning the valid surgical procedure commands is the proposed solution to make a secure connection between the robot and the robot manipulator. Deep secure tele-surgery system (DSTS) attempts to learn how the expert surgeon concludes a specific surgical task. Then, the trained DSTS is able to distinguish valid commands from invalids as the observant of network. The DSTS predicts the class label of surgeon at time t based on a previous certain time interval of data stream. The focus is on the orthopedical telesurgical drilling operation application to evaluate the performance of DSTS. Accordingly, this data which is captured from robot manipulator device, contains the features such as rotation, position, temperature, etc. The DSTS has been designed based on a deep recurrent neural network with LSTM architecture to learn the dynamic temporal of expert and novice surgeon behavior. The DNN is trained on the multiple completed task of surgical operation related to both novice and expert surgeon in the supervised manner. In summary, DSTS uses the data which has been sent from robot manipulator device to train the DNN. The expert and the novice surgeons generate this data while, completing a specific surgical task. The trained model predicts the class label of commands at time t in the real time (Figure 1).

3 Training and modeling

3.1 Data preparation

The general target of using Orthopaedic Surgical Drilling system is to simulate a telesurgical environment including a haptic device. The inputs of simulation system are patient specific CT data of femur bone and its segmentation, which is used for the virtual rendering of the bone volume. A segmentation method is employed to separate various layers of

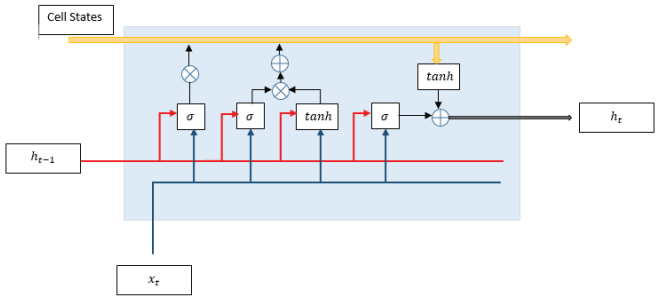

Fig. 2 The LSTM unit with forget gate, input gate, output gate and cell state.

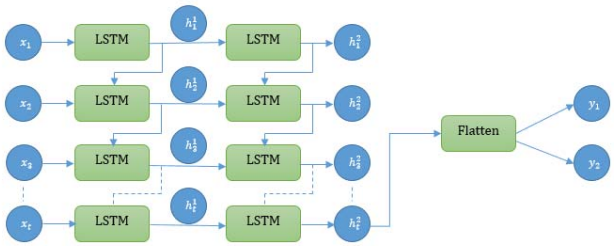

Fig. 3 An LSTM recurrent neural network with 2 hidden layers. Recurrent unit chain has been unrolled in a specific time instant t. The output of network has been received from the last unit in the second layer. The output implements a binary classifier.

the bone such as cortical bone, cancellous bone, and bone marrow to simulate their thickness and behaviors while interacting with a drill. This process is used to simulate the actual procedure in the operation room. On the other side, the surgeon interacts with the simulation system via a haptic device (Phantom Omni, Geomagic Touch, USA) as a robot manipulator device, a keyboard, and a computer mouse. Virtual drill can be manipulated to touch/drill the femur bone model through the stylus of the haptic device.

The four main steps to develop the simulation are described as follows. First, CT data of a patient, who suffers from femoral head necrosis are used to build a model for the simulation system. The most common modalities, which provide 3D medical images, are CT and MRI (Magnetic Resonance Imaging). There is a difference between these two methods: the MRI exceeds most in soft tissue while CT is more applicable for bone pathology diagnosis. However, the bone density and strength information that can be extracted from both methods is solitary extractable from the CT data [10]. A set of femur bone CT images were used for visual and haptic modeling. Intensity values on the CT images disclose the attenuation coefficient of the tissue.

Second, a voxel-based approach is developed to model the stiffness of the bone. A volume rendering method has been developed with respect to bone drilling application. Whenever the hard bone tissue is concerned, where drilling and tissue removal are the main operations, volume rendering has been preferred since it stores mechanical information of bone depth [11] [12] [13] [14]. To achieve a reasonable algorithmic complexity, voxel removal was modeled in the method with respect to the fact that every voxel has its own density value. The process of drilling on a set of voxels causes their density to be reduced by a certain rate and a voxel will be removed when its density becomes zero. Another technique was also developed to produce a more realistic model. The top view of the CT data was segmented to distinguish the bone from tissue and remove the tissue from the images.

Third, approaching of user-defined generation X-ray views is presented. In a real surgery of osteonecrosis in operation room (OR), the surgeon requires to stop drilling and change the C-arm position for taking X-rays from different points of views. This assures them that the drill traverses the correct path within the bone. This simulation is able to depict the perspective 3D model of the bone similar to the three X-ray views of the bone: the front, side, and top views.

The features of the developed graphical user interface are presented in the fourth and final step. The simulation can show the current drill temperature. There is some factors that have influence on the bone temperature, which are drilling speed, drilling time, or the applied force [15]. According to the experimental data presented in the literature, the temperature has the highest impact [15].

We employed seven surgical residents to perform drilling procedures using Touch 3d Stylus haptic device, which had been connected to simulation system via a network. We defined the pre-planned path, in which the residents had to pass through all the bone layers to get to the target point. Every participant had five minutes to get familiar with the simulator and then carried out the task two times, as an expert and pretending to be a novice. In the process of data collection, we collected the positions and angles of the robot manipulator device in x, y, and z axes and collected Theta (Eulers Angle), force exerted on the simulated bone and the simulated temperature of the drill. The data was collected with the frequency of 10 Hz to make a dataset with 30,000 samples.

3.2 Deep learning

As mentioned in the previous section, the data has been gathered with the frequency of 10Hz while surgeon operates the specific task of drilling with haptic device and simulation system. It is clear that we are dealing with a time-varying dataset. In fact, the behavior during the time should be modeled to discriminate a novice surgeon from an expert one. The system detects the class label of surgeon at each time t, based on a certain time interval of data stream. In order to create an appropriate model, a recurrent neural network has been employed instead of a feed forward one. The system models the surgeons behavior with a configuration of deep recurrent neural network based on the LSTM architect [16].
Recurrent neural networks can process the dynamic temporal behavior of data by their internal states. The LSTM unit (Figure 2) was proposed to solve the vanishing gradient problem in the basic RNN such as Vanilla RNN [17]. Similar to other recurrent

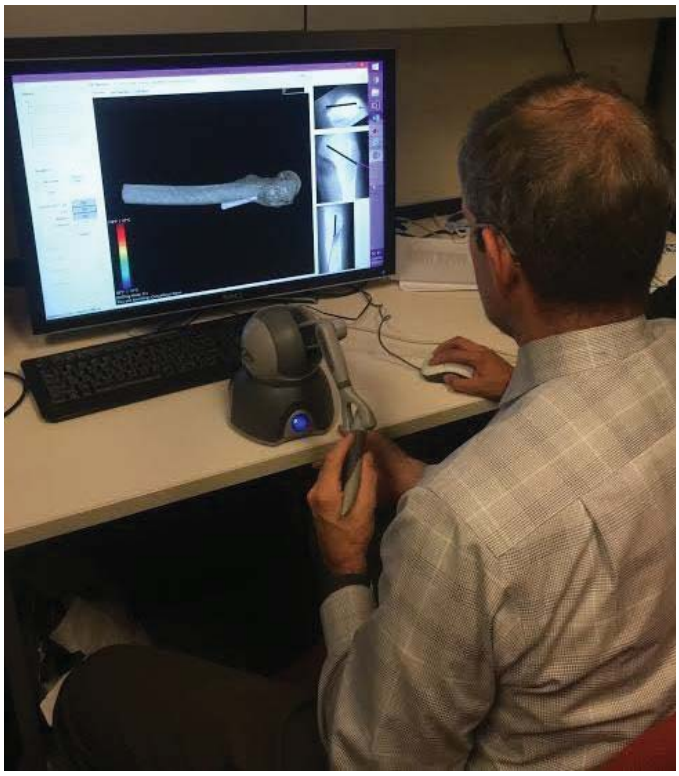

Fig. 4 The setup was used for collecting data during the haptic-enabled virtual drilling task.

neural networks, the LSTM unit has a loop that connects previous information to the current task at any time instant t. LSTM unit has four parts known as network layers. Cell state C_t preserves past information at time t. This information will be updated by time evolution. Forget gate exerts input x_t and previous output h_{t-1} to decide which data must be removed:

$$f_t = \sigma(W_f x_t + U_f h_{t-1} + b_f) \quad (1)$$

where σ is a sigmoid activation function, U_f and W_f are weight matrices and b_f is the bias vector. To update internal memory with new essential information, input gate i_t decides which value must be updated. Also, a hyperbolic tangent layer $\tilde{C}_t$ chooses new values with cooperation of input gate as follows:

$$i_t = \sigma(W_i x_t + U_i h_{t-1} + b_i) \quad (2)$$

$$\widetilde{C}_t = tanh(W_{\tilde{c}} x_t + U_{\tilde{c}} h_{t-1} + b_{\tilde{c}}) \quad (3)$$

Now, LSTM internal memory C_t is ready to get new updates:

$$C_t = f_t * C_{t-1} + i_t * \widetilde{C}_t \quad (4)$$

where $*$ denotes the element-wise multiplication. Finally, LSTM unit utilizes updated memory C_t and previous output via output gate o_t to produce the output h_t as follows:

$$o_t = \sigma(W_o x_t + U_o h_{t-1} + b_o) \quad (5)$$

$$h_t = o_t * \tanh(C_t) \quad (6)$$

where in all of the above equations, input $x_t \in R^n$, weight matrices $W \in R^{h \times n}$ and $U \in R^{h \times h}$, and biases $b \in R^h$. n is the size of input vector of each LSTM unit and h is the size of internal memory or cell state, which is defined by the designer. The unit chain connectivity should be unrolled according to length of past time interval in order to distinguish the surgeon class label at time t as shown in Figure 3.

We assume that the LSTM unit output h_t depends on $\{x_{t-100}, x_{t-9}, \dots x_{t-1}\}$. Then, the loop of RNN is unrolled during 100 latest inputs. In other words, the prediction at time t relies on 10 previous seconds of surgeon behavior while working with robot manipulator device in the simulation system. In fact, the unrolled units are system time steps. It is notable that all weight matrices and bias vectors are shared between unrolled units in each layer. These units create the first layer of the neural network. The outputs of each unit in the first layer is fed to the second layer of neural network. The LSTM DNN parameters are defined as follows:

$$W^l = \begin{bmatrix} W_f \\ W_i \\ W_{\tilde{c}} \\ W_o \end{bmatrix}, U^l = \begin{bmatrix} U_f \\ U_i \\ U_{\tilde{c}} \\ U_o \end{bmatrix}, b^l = \begin{bmatrix} b_f \\ b_i \\ b_{\tilde{c}} \\ b_o \end{bmatrix}, \quad (7)$$

where l is the number of layers in the deep NN. The size of network output must be equal to the number of the expected class labels. The class labels represented by one-hot vector as follows:

$$expert\ class = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, novice\ class = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad (8)$$

A transition layer is defined to transfer the output of LSTM neural network to the class label space:

$$a = W_a h_t^l + b_a \quad (9)$$

In fact, the output at last time step in the last layer is transferred to the class label space via a linear transition function. The objective function of DNN, which attempts to learn the expected input class label in a supervised manner, is defined as:

$$minimize\ obj(a,y) = -y.\log\left(\frac{1}{1+e^{-a}}\right) - (1 - y).\log\left(\frac{e^{-x}}{1+e^{-x}}\right) \quad (10)$$

where, y is the input class label. Different optimizer algorithms such as ADAM optimizer can optimize the above loss function [18].

4 Experiment

A full task of drilling operation must be prepared to train the deep LSTM neural network. In other words, DNN learns the behavior of surgeons during multiple complete drilling tasks operated by different surgeons as the training samples. The dataset needs some modification to prepare data, which is fed to DNN. The system considers 10 seconds of previous input stream for learning surgeon class labels. As discussed in the previous section, data has been received with frequency of 10 Hz from robot manipulator device while a volunteer completing a specific drilling task. Hence, r_i is defined as the ith record of prepared dataset, which is sorted by time. $r_{1:100}$ is the records related to 10 seconds of data in the dataset, where $r_i \in R^{35}$. Accordingly, the new dataset contains records as follows:

$$nd = \{rn_1 = r_{1:ts}, rn_2 = r_{2:ts+1}, \dots, rn_i = r_{i:ts+i-1}\} \quad (11)$$

where, $rn_i \in R^{ts\times n}$, $ts = time\ steps = 100$ and $i = ld - ts + 1$ (ld is the length of the previous dataset). The LSTM deep neural network is unrolled to 100 time steps as shown in Figure 3. The DNN was trained on the data batches of 4 completed drilling tasks belonged to expert and another 4 drilling tasks belonged to the novice class. All data was converted to the new dataset with 100 time steps ($rn_i \in R^{100\times 35}$). Each batch contained 50 records of data. The procedures of system are described as follows: The raw data was caught from C++ haptic device program. The raw data includes $X, Y\ and\ Z$ position and rotation of haptic device. The data is sent to the python program via a UDP client-server socket network. The data was converted to the new dataset described above. The converted data belonged to training dataset was utilized to train deep recurrent neural network. The prediction of trained model on the converted test data was sent to a monitoring computer via UDP client-server network. A python program parses the classification result and changes the color of monitor to red or green based on predicted class labels (Figure 1). The performance of system was evaluated by 2 unseen drilling tasks belong to both novice and expert classes. The system predicted the class label of data stream using 10 previous seconds of data stream in every one second. The results reported in the Table 1 obtained from the average of more than three times of system run.

Table.1 *the result computed from average more than 3 time run.*

Time steps	*layer*	*Memory dim*	*Train sample*	*Test sample*	*batches*	*accuracy*
200	1	128	16268	2388	100	78%
100	2	128	16868	2588	100	82%
100	1	64	16868	2588	100	87%

It is worth noting that all machine learning algorithms were implemented in Python using TensorFlow. All experiments were conducted on a Windows machine with Intel Core-i7 on 8GB RAM [19].

5 Conclusion

In this study, we report the latest results on the development of a deep recurrent neural network based on the LSTM architecture for surgeon classification in a potential tele-operated surgical procedure. We have focused on modeling the behavior of surgeon during the bone layer drilling procedure for a predefined path. The neural network was trained on many tasks of drilling procedure completed by both expert and novice surgeons. The trained neural network successfully predicted the correct class label with 70 – 92 percent of accuracy. This system can help to detect unusual behaviors, attacks, or mistakes during tele-surgical operation without using any network protocols. We hope to improve the performance of system by collecting more data from more expert surgeons.

ACKNOWLEDGMENT

The authors would like to thank orthopedic surgery residents at McLaren Hospital, Flint, MI, USA.

6 References

[1] R. M. Satava, "How the Future of Surgery is Changing: Robotics, Telesurgery, Surgical Simulators and Other Advanced Technologies:," *Jurnalul de Chirurgie,* vol. 5, no. 4, pp. 311-325, 2009.

[2] T. Bonaci, J. Herron, T. Yusuf, J. Yan, T.Kohno and H.J. Chizeck, "To Make a Robot Secure: An Experimental Analysis of Cyber Security Threats Against Teleoperated Surgical Robotics∗," *arXiv:1504.04339,* Apr 2015.

[3] J. Marescaux, J. Leroy, F. Rubino, M.Smith, M. Vix, M.Simone and D. Mutter, "Transcontinental Robot-Assisted Remote Telesurgery: Feasibility and Potential Applications," *ANNALS OF SURGERY,* vol. 235, p. 487–492, 2002.

[4] E. Biglari, et al, "Haptics-Enabled Surgical Training System with Guidance Using Deep Learning," in *Universal Access in Human-Computer Interaction. Access to Learning, Health and Well-Being. UAHCI,*

Lecture Notes in Computer Science, vol 9177. Springer, Cham, 2015.

[5] G. S. Lee and B. Thuraisingham, "Cyberphysical systems security applied to telesurgical robotics," *Computer Standards & Interfaces,* vol. 34, no. 1, pp. 225-229, 2012.

[6] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *47th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, Monticello, IL, USA, 2009.

[7] S. Amin, A. A. Cárdenas and S.S. Sastry, "Safe and Secure Networked Control Systems under Denial-of-Service Attacks," in *Hybrid Systems: Computation and Control. HSCC 2009. Lecture Notes in Computer Science, vol 5469. Springer*, Berlin, Heidelberg, 2009.

[8] K. Coble, W. Wang, B. Chu and Z. Li, "Secure software attestation for military telesurgical robot systems," in *MILCOM 2010 MILITARY COMMUNICATIONS CONFERENCE*, San Jose, CA, USA, 2010.

[9] M. E. Tozal and et al, "Adaptive Information Coding for Secure and Reliable Wireless Telesurgery Communications," *Mobile Networks and Applications,* vol. 18, no. 5, p. 697–711, 2013.

[10] J. C. Teo, K. M. Si-Hoe, J. E. Keh, and S. H. Teoh, "Relationship between ct intensity, micro-architecture and mechanical properties of porcine vertebral cancellous bone," *Clinical biomechanics,* vol. 21, no. 3, p. 235–244, 2006.

[11] R. E. Sofronia, A. Davidescu, and G. G. Savii,, "Towards a virtual reality simulator for orthognathic basic skils," *Applied Mechanics and Materials,* vol. 162, p. 352–357, 2012.

[12] T. N. Bogoni and M. S. Pinho, "Haptic technique for simulating multiple density materials and material removal," in *21st International Conference in Central Europe on Computer Graphics, Visualization and Computer Vision in cooperation with EUROGRAPHICS Association, p. 151-160*, 2013.

[13] Y. Liu and S. D. Laycock, "A haptic system for drilling into volume data with polygonal tools," in *Theory and Practice of Computer Graphics*, W. T. a. J. Collomosse, Ed., The Eurographics Association, 2009, p. 9–16.

[14] D. Morris, C. Sewell, N. Blevins, F. Barbagli, and K. Salisbury, "A collaborative virtual environment for the simulation of temporal bone surgery," in *Medical Image Computing and Computer-Assisted Intervention MICCAI . Lecture Notes in Computer Science, vol 3217*, Berlin, Heidelberg, 2004.

[15] R. K. Pandey and S. Panda, "Drilling of bone: A comprehensive review," *Journal of clinical orthopaedics and trauma,* vol. 4, no. 1, p. 15–30, 2013.

[16] S. Hochreiter and J. Schmidhuber, "Long Short-term Memory," *Neural Computation,* pp. 1735-80, 1997.

[17] S. Hochreiter, Y. Bengio, P. Frasconi and JSchmidhuber, "Gradient Flow in Recurrent Nets: the Difficulty of Learning Long-Term Dependencies," 2001.

[18] D.P. Kingma, J. Ba, "Adam: A Method for Stochastic Optimization," *arXiv:1412.6980,* 2014.

[19] M. Abadi, P. Barham, J. Chen, Z. Chen, A. Davis, J. Dean, M. Devin, S. Ghemawat, G. Irving, M. Isard, M. Kudlur, J. Levenberg, R. Monga, S. Moore, D. G. Murray, B. Steiner, P. Tucker, "TensorFlow: A system for large-scale machine learning," 2016 .