REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
04-05-2019	Final Report	1-May-2016 - 31-Jan-2017

4. TITLE AND SUBTITLE
Final Report: Robust 3D Surveillance

5a. CONTRACT NUMBER
W911NF-16-1-0163

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
611102

6. AUTHORS

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
University of Texas at Dallas
800 West Campbell Road, AD15

Richardson, TX 75080 -3021

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS (ES)
U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSOR/MONITOR'S ACRONYM(S)
ARO

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
67369-CS.1

12. DISTRIBUTION AVAILIBILITY STATEMENT
Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Balakrishnan Prabhakaran
UU	UU	UU	UU		19b. TELEPHONE NUMBER 972-883-4680

RPPR Final Report
as of 06-May-2019

Agency Code:

Proposal Number: 67369CS **Agreement Number: W911NF-16-1-0163**
INVESTIGATOR(S):

Name: Balakrishnan Prabhakaran
Email: praba@utdallas.edu
Phone Number: 9728834680
Principal: Y

Organization: **University of Texas at Dallas**
Address: 800 West Campbell Road, AD15, Richardson, TX 750803021
Country: USA
DUNS Number: 800188161 EIN: 751305566
Report Date: 30-Apr-2017 Date Received: 04-May-2019
Final Report for Period Beginning 01-May-2016 and Ending 31-Jan-2017
Title: Robust 3D Surveillance
Begin Performance Period: 01-May-2016 **End Performance Period:** 31-Jan-2017
Report Term: 0-Other
Submitted By: Balakrishnan Prabhakaran Email: praba@utdallas.edu
Phone: (972) 883-4680
Distribution Statement: 1-Approved for public release; distribution is unlimited.

STEM Degrees: **STEM Participants:**

Major Goals: 1. Robustness of 3D data sensed by LiDAR (Light Detection and Ranging) cameras.
LiDAR cameras have longer range for sensing and provide data for applications in multiple fields such as self-driving cars, geography mapping (that can be used for surveillance as well). We will carry out anti-forensic and forensic studies on LiDAR data using the STIR funding. The preliminary results from this study will help us address the concern expressed by the reviewer (for the earlier proposal's focus on using only Microsoft's Kinect data).

2. Real-time Performance of Multi-camera 3D Meshing
We will also employ the STIR funding to get preliminary results on real-time performance of 3D reconstruction approaches. As mentioned earlier, we have been able to achieve real-time performance by working in the depth image domain, and mapping it back to the 3D. We will continue with our efforts and get additional preliminary results to show the feasibility for handling multiple camera data.

Accomplishments: 1. For RGB-D cameras, we first presented a real-time anti-forensic 3D object stream manipulation framework to capture and manipulate live RBG-D data streams to create realistic images/videos showing individuals performing activities they did not actually do. The framework uses computer vision and graphics methods to render photo-realistic animations of live mesh models captured using the camera. Next, we conducted a visual inspection of the manipulated RGB-D streams (just like security personnel would do) by users who are computer vision and graphics scientists. The study shows that it was significantly difficult to distin- guish between the real or reconstructed rendering of such 3D video sequences, thus clearly showing the potential security risk involved. Finally, we investigated the efficacy of forensic approaches for detecting such manipulations.

2. We investigated and identified three possible attacks on the LiDAR data. We also proposed two novel forensic approaches as a countermeasure for such attacks and study their effectiveness. The first forensic approach utilizes the density consistency check while the second method leverages the occlusion effect for revealing the forgery. Experimental results demonstrated the effectiveness of the proposed forgery attacks and raise the awareness against unauthenticated use of LiDAR data. The performance analyses of the proposed forensic approaches indicated that the proposed methods are very efficient and provide the detection accuracy of more than 95% for certain kinds of forgery at- tacks. While the forensic approach is unable to handle all forgery attacks, the study motivates to explore more sophisticated forensic methods for LiDAR data.

Training Opportunities: Nothing to Report

RPPR Final Report
as of 06-May-2019

Results Dissemination: 1. “Evaluating the Efficacy of RGB-D Cameras For Surveillance”, S. Raghuraman, K. Bahirat, B. Prabhakaran, Proceedings of IEEE International Conference on Multimedia & Expo (ICME 2015), Torino, Italy, June 29 – July 3, 2015.

2. “A Study on LiDAR Data Forensics”, K. Bahirat and B. Prabhakaran, Proceedings of the IEEE International Conference on Multimedia and Expo (ICME'17), Hong Kong, July 2017.

Honors and Awards: Nothing to Report

Protocol Activity Status:

Technology Transfer: Nothing to Report

PARTICIPANTS:

Participant Type: Graduate Student (research assistant)
Participant: Kanchan Bahirat
Person Months Worked: 9.00 **Funding Support:**
Project Contribution:
International Collaboration:
International Travel:
National Academy Member: N
Other Collaborators:

Participant Type: Graduate Student (research assistant)
Participant: Suraj Raghuraman
Person Months Worked: 9.00 **Funding Support:**
Project Contribution:
International Collaboration:
International Travel:
National Academy Member: N
Other Collaborators:

A STUDY ON LIDAR DATA FORENSICS

Kanchan Bahirat, Balakrishnan Prabhakaran

The University of Texas at Dallas
Kanchan.Bahirat@utdallas.edu, bprabhakaran@utdallas.edu

ABSTRACT

3D LiDAR (Light Imaging Detection and Ranging) data has recently been used in a wide range of applications such as vehicle automation and crime scene reconstruction. Decision making in such applications is highly dependent on LiDAR data. Thus, it becomes crucial to authenticate the data before using it. Though authentication of 2D digital images and video has been widely studied, the area of 3D data forensic is relatively unexplored. In this paper, we investigate and identify three possible attacks on the LiDAR data. We also propose two novel forensic approaches as a countermeasure for such attacks and study their effectiveness. The first forensic approach utilises the density consistency check while the second method leverages the occlusion effect for revealing the forgery. Experimental results demonstrate the effectiveness of the proposed forgery attacks and raise the awareness against unauthenticated use of LiDAR data. The performance analyses of the proposed forensic approaches indicate that the proposed methods are very efficient and provide the detection accuracy of more than 95% for certain kinds of forgery attacks. While the forensic approach is unable to handle all forgery attacks, the study motivates to explore more sophisticated forensic methods for LiDAR data.

Index Terms— 3D surveillance, 3D Forensic, LiDAR

1. INTRODUCTION

With recent advances in the depth sensing technology, it has become possible to quickly generate a complete 3D reconstruction of an object or an entire scene. Various depth sensors such as LiDAR are widely available in the market which can be used to scan indoor and outdoor scenes. Due to low cost, millimeter precision and ease of operation, the 3D scanned data obtained using the LiDAR sensors finds application in diverse areas [1, 2]. Benedek [1] demonstrates the capability of rotating multi-beam LiDAR as a future surveillance camera for a real-time 3D people surveillance. Various studies performed [2] encourage to use LiDAR data for damage detection in case of large deformed structures such as bridges, roofs. 3D laser scanning has become a powerful tool to collect the crime scene and civil accident data and bring it to the courtroom for legal investigation or insurance settlement

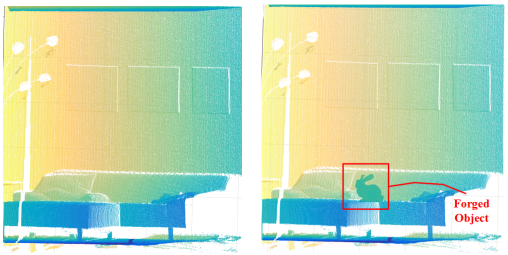


Fig. 1: Original LiDAR scan (left) and forged LiDAR scan (right)

[3, 4]. This technology allows for a collection of 3D data of the scene where the civil or criminal incident took place and to create the same scene graphically in a courtroom. Further, LiDAR has been successfully employed in autonomous automated vehicles such as Google Driverless Car [5], for detecting obstacles and re-planning the mission/path accordingly.

In this context, the genuineness of the 3D LiDAR data is a critical factor which further motivates to determine the possibility of forgery attacks on it. Any attack that manipulates the LiDAR data can be very harmful in the above applications. For example, in the case of autonomous automated vehicles, a false indication of an obstacle can cause a wrong driving decision and can potentially lead to an accident. Hence, it is important to address following two questions:

- Is the LiDAR data vulnerable to forgery attacks?
- Is it possible to detect such forgery attacks on the LiDAR data if there exists any?

In this paper, we address these questions as follows:

- We identify three possible approaches for attacks on the LiDAR data that do not need additional commodity hardware. Experimental results show the successful *blinding* due to proposed attacks. Figure 1[1] shows original and forged LiDAR data.
- We also present two novel algorithms for detecting such forgeries in LiDAR data and provide a detailed performance analysis of the proposed algorithms in case of different types of attacks.

Principal Contributions: This paper provides a detailed study of possible forgery attacks on LiDAR data. It outlines two novel forensic approaches for LiDAR data (As per our knowledge, this is the first attempt to address LiDAR forensics). Though the forensic algorithms are effective for

[1]Note, all the images in this paper are better visualized in color.

978-1-5090-6067-2/17/$31.00

specific types of forgeries, a forensic approach handling the wide spectrum of forgeries is necessitated. This work creates awareness about avoiding the blind usage of LiDAR data in critical applications and motivates to explore forensic of LiDAR data as an emerging research area.

Related Work: Forgery detection in images/videos has been a very well researched area. Two excellent surveys [6, 7] provide a list of current state-of-the-art methods in image/video forensics and highlight their features. On the other hand, forensics for 3D data is a relatively less explored area. As per our knowledge, no forensic method has been proposed to detect forgery in 3D data except the method proposed in [8]. Raghuraman et al. [8] propose a framework to capture and manipulate the live RGB-D data stream to create an illusion of an individual performing activities which they did not actually do. Authors also suggest a noise analysis based forgery detection for depth images which is incapable of detecting forgeries in all cases and unsuitable for LiDAR data.

In literature [9, 10], a verity of methods based on digital watermarking are explored. Most of these methods can be broadly classified as: *robust* and *fragile methods*. *Robust methods* [9] are constructed with the aim of providing ownership protection and distribution channel tracking. While *fragile methods* such as [11] are designed for authentication applications. As these methods require the connectivity information, they are not suitable for LiDAR data.

The resilience of a LiDAR against attacks has been studied concerning the security analysis of an automotive system [12, 13]. Petit et.al. suggest a use of a smart surface which is absorbent or reflective to manipulate the data sensed by the LiDAR in [13]. Relaying and spoofing attacks on LiDAR sensor with the aim of generating fake echoes and fake objects have been proposed in [12]. In 'relaying' attack, the original signal sent from the LiDAR is relayed from the other position to create fake echoes with additional two transceivers. A 'spoofing' attack is made by sending a counterfeit pulse during a listening interval of 1.44 microseconds of LiDAR to create an illusion of point being further away. Most of the work aim at studying possible attacks on the LiDAR sensor and hence require additional hardware. We differentiate from the previous work by developing *attacks on the 3D LiDAR data* that do not need extra commodity hardware.

2. ANTI-FORENSIC FRAMEWORK

To evaluate the vulnerability of the LiDAR data, we propose a novel anti-forensic framework that utilises basic computer graphic techniques to create forged LiDAR data. Adopting the attacker model used in [12], we assume that the attacker has limited resources regarding the type of LiDAR sensors, processing power and has the intention to disrupt the data unnoticeably. The proposed anti-forensic framework is designed to create three types of attacks on the LiDAR data. Figure 2 shows the pipeline for different types of attacks.

Additive Approaches: In additive approaches, an object

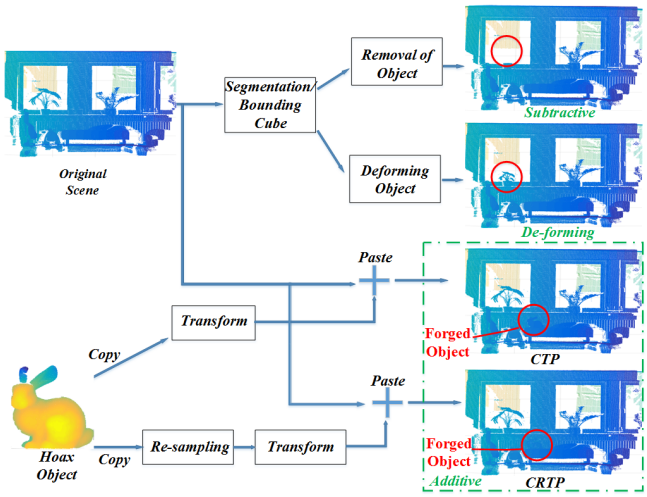


Fig. 2: Pipeline for different types of attacks on 3D LiDAR data

is added and placed in the original scene such that viewer or automotive system perceives the object being actually present in the scene. Taking inspiration from the copy-paste forgery in digital images [6], we designed two additive attacks:

Copy-Transform-Paste (CTP): Similar to the copy-paste forgery attacks on images, to add a hoax object in a scene, one can copy the set of points corresponding to the object and add it to the list of points corresponding to the scene. But this naive approach may not create an impactful illusion due to:

- Due to the limited resource availability to the attacker, we can assume, that the attacker may have a different sensor than the one used for scanning the scene. As two different sensors may utilize different metric for measurement, a range of coordinate values of hoax object may be significantly different than that of the scene.
- 3D coordinates of object points are defined with respect to it's local coordinate system which may be different from that of sensor used for scanning the scene.
- The orientation of the object's local coordinate system may differ from its orientation in the target scene.

To handle the issues as mentioned earlier, we incorporate an additional step of *'Transform'* before pasting the points of a forged object into the scene. It consists of following steps:

Scaling: Scaling helps to resolve the disparity in metrics used by different sensors for measurement. The scaling factor can be computed based on the knowledge of metrics employed by sensors or based on the range of values for the coordinate of points representing the scene and object.

Translation and Rotation: Object's points are first required to be translated into the local coordinate system of the scene followed by a translation needed to place it in the correct position in the scene. The cumulative amount of required translation t can be computed as $t = P_{object} - (o_{scene} - o_{object})$, where o_{scene} and o_{object} are centroids of the scene and the object respectively and P_{object} is the position of the object in the scene. Further, to correctly orient the object in the scene, each point of the object is multiplied by the rotation

matrix. Note that, rotation required is decided by the attacker based on how the object is supposed to be placed.

Copy-Re-sample-Transform-Paste (CRTP): The second attack is designed based on the fact that two sensors may have different resolution as per the underneath hardware. In CRTP forgery, we included additional *'Re-sampling'* step before the *'Transform'* step. In this step, the forged object is *'re-sampled'* (downsampled or upsampled) to match the resolution of the sensor used to scan the scene. Downsampling can be achieved by employing any of the point cloud sampling methods such as uniform sampling. Upsampling can be accomplished by performing interpolation of the current samples. Next, we defined the minimum inter-point distance (MID) which is the minimum Euclidean distance between the point and it's nearest neighbor. The factor of re-sampling is defined as:$\gamma = \frac{MID_o}{MID_s}$, where MID_o and MID_s are MID between object points and scene points respectively. The *'Re-sampling'* eliminates the inconsistency occurring in sampling density due to insertion of a hoax object.

Subtractive Approaches In subtractive forgery, to conceal the presence of an object in the original scene, the set of points representing the object are removed from LiDAR data. Due to the unstructured nature of LiDAR data, identifying points belonging to an object is a nontrivial task. Identification of the objects can be made manually by selecting a bounding cube around it with the help of visualisation toolkit or by performing a point cloud segmentation using the method such as [14]. Segmentation provides the labelling for each object in the scene. Hence, points having the same label can be eliminated from the original scene to perform subtractive forgeries. On the other hand, given the spread of a bounding cube, an algorithm determines the set of points inside the bounding cube and removes them. It should be noted that the segmentation will significantly increase the complexity of attack regarding the time and efforts needed.

Deforming Approaches In deforming approaches, the point representing the portion of the object are displaced from their original position. This type of forgery can be used to create a fake dent on the object's surface. The identification of the object to be deformed can be performed using either manual selection of bounding cube or the point cloud segmentation. As deforming attacks mainly target the data used in the visualization based applications and complexity involved in achieving realistic forgery make this attack more intricate.

System Overview The proposed system allows user to select the type of attack. If the additive attack is selected, the user needs to provide a 3D model of the hoax object, position and orientation of the object in the scene. Based on the required position and orientation, the parameters needed for *'Transform'* step such as rotation matrix and translation vectors are computed only once. Further, if a user selects to re-sample the data, the factor of re-sampling is obtained as suggested previously. For subtractive and deforming attacks, the user needs to provide a bounding box indicating the targeted area and deformation scale. For example, the user can decide to remove any object at the distance d in front of the car with length l, width w, and height h. Using these input parameters, the system can generate a selected attack.

3. FORENSIC EVALUATION

The detailed analysis of the possible attacks on LiDAR data motivates to design an algorithm to validate LiDAR data. We now describe two preliminary forensic algorithms for additive attacks. Due to the page limit, we restrict ourselves to forensic evaluation of additive attacks only.

Density Variation Based Forensic Algorithm I: As the resolution varies across sensors, the discrete point clouds of an object obtained using different sensors will have different sampling densities. Further, due to perspective projection based design of depth sensors, the sampling density of an object also depends on its distance from the sensor. For example, objects near the sensor will have a higher sampling density compare to objects away from the sensor. Moreover, the objects at the same distance from the sensors must have approximately similar sampling density.

Algorithm 1 *IsDensityConsistent*

for each point $p \in P$ **do**
  Compute nearest neighbor p'
  Compute $min_d(p) = d(p, p')$
end for
Sort points in the increasing order of z values.
Quantize z values to set of discrete levels Z
for each discrete level $z_1 \in Z$ **do**
  Consider set of point Q at distance z_1
  Compute $MIN_{ipd}(z_1) = mean(min_d(p))$ for all $p \in Q$
end for
Compute Moving average of the signal $MIN_{ipd}(z)$
if sudden rise or the fall in the averaged $MIN_{ipd}(z)$ **then**
  Declare "Forgery Detected"
end if

Assuming that the additive attack is created using different sensors with different resolution, the forged object will have a different sampling density compare to another object in the scene at the same distance from a sensor. Hence, for the unaltered data, if we compute an MID (Minimum Inter-point Distance) at different values of z (the distance from the sensor), it will increase as we move away from the sensor. On the other hand, if suddenly there is a continual rise or drop in MID for the range of depth values, then we can consider it as a forged data. Figure 5 a illustrates the sudden variation in the MID in the case of forged scene. It can be seen that inter-point distance corresponding to bunny is very high compared to other parts of the scene. Based on these observations, we formulate the algorithm *IsDensityConsistent* (I) that checks the consistency of sampling density. Here, P is the point cloud of original scene, $d(p, p')$ is Euclidean distance

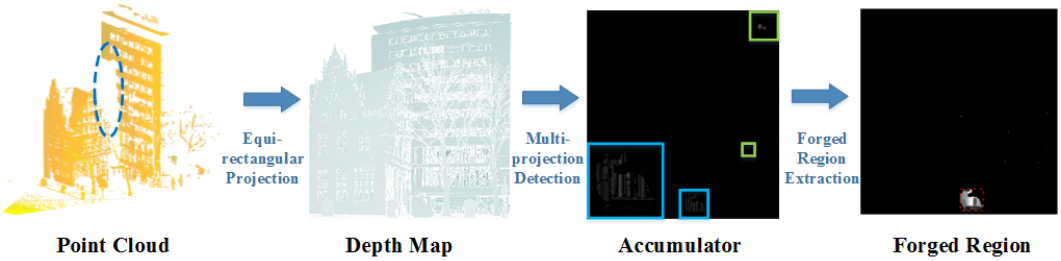


Fig. 3: Pipeline of *IsOcclusionConsistent* (forensic algorithm II). In this example, the input is the forged point cloud obtained by adding Stanford Bunny scan into the LiDAR scanned outdoor scene.

between p and p' and z represents Z-coordinate of p.

Multi-projection Based Forensic Algorithm II: Generally, due to the occlusion effect, objects which are behind another object may not be entirely or partially visible to the sensor. It can be observed from Figure 3 that the portion of the taller building is occluded by the front building and no points are measured by the LiDAR sensor in the occluded region. On the contrary, when the hoax object is inserted into the scene with additive attacks, the forged data will not exhibit such occlusion effect. Hence, points behind the hoax object still exist causing inconsistency in the occlusion effect.

Inspired by this idea, we propose a multi-projection based forensic algorithm, *IsOcclusionConsistent* (II) that determines the validity of the 3D LiDAR data by checking congruity in the occlusion effect. Figure 3 illustrates the pipeline of the proposed forensic algorithm II that includes:

Equi-rectangular Projection: For the unaltered LiDAR data, when all 3D points are projected on the 2D image plane, each point will be mapped to a distinct image pixel based on the selected image resolution. On the other hand, when a hoax object is inserted into the scene, there might be multiple points getting mapped to a single image pixel. We leverage this fact to determine any inconsistency in the occlusion effect by checking if there is a point behind the current point.

To obtain the projection of the scanned 3D data on a 2D image plane, we first convert each 3D point (x, y, z) in the Cartesian co-ordinate system to the corresponding (r, θ, ϕ) in the cylindrical co-ordinate system. Next, we apply a equirectangular projection [15] that relate the 2D image coordinates (i, j) linearly to θ and ϕ i.e. $i = \theta$ and $j = \phi$. The resolution of the image is determined by the vertical and horizontal angle resolution of the LiDAR sensor. Figure 3 shows the depth map generated using the equi-rectangular projection.

Multi-projection Detection: To determine if multiple points are getting mapped to a single image pixel, we maintain a 2D 'Accumulator'. If the 2D projection of the current point p is already occupied by another point q, we compute the distance between these point along the projection line as $|r_p - r_q|$ and store it in the 'Accumulator' at their common 2D projection (i, j). The accumulator populated using the proposed multi-projection detection is shown in the Figure 3. It can be seen that the bunny shape region has higher accumulation density. Therefore, the existence of multiple points behind the bunny in the scanned data evidences the forgery.

Forged Region Extraction: Though, the 'Accumulator' captures inconsistency in the occlusion effect, it also consists of few artifacts due to a slight mismatch between the image resolution, the resolution of the LiDAR sensor and the resolution of the forged object. The top, right box in the accumulator shown in Figure 3 describes such noisy points. While, bottom-left box shows the sparse bunny image. If we estimate connected components in the accumulator, the results may not accurately represent the forged region. To annihilate above mentioned issues, we apply post-processing to 'Accumulator' that includes morphological closing and median filtering followed by connected component estimation. The presence of a connected component with the area greater than the empirically defined threshold A_{th} is considered as a forgery.

4. EXPERIMENTAL RESULTS

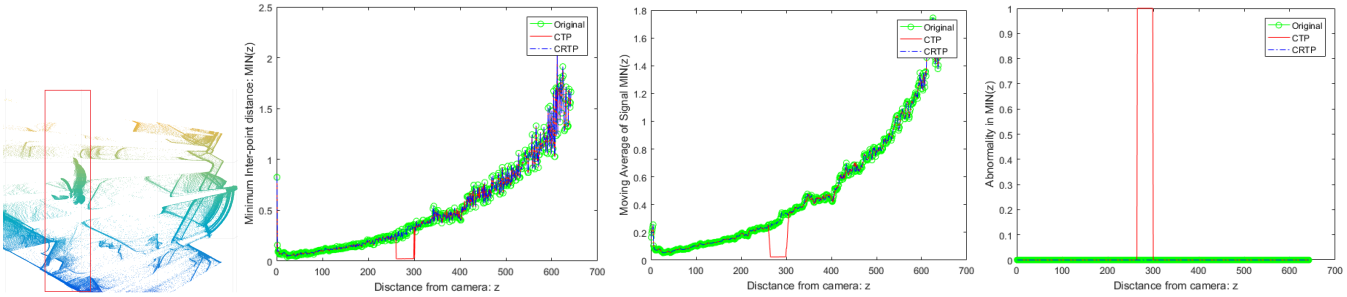
In this section, we demonstrate the effectiveness and efficiency of the proposed attacks and the proposed forensic evaluation algorithm. All attacks and algorithms are implemented in MATLAB and experiments are run on a CPU with Intel (R) Core (TM) i7-5820K with 3.30GHz speed and 32GB RAM.

We utilized LiDAR scans provided at Robotic 3D repository [16] along with Bunny and Dragon models from the Stanford Dataset as hoax objects. Robotic 3D repository includes indoor and outdoor scenes which are scanned using Riegl VS-400 and Optris PI IR camera. For our experiments, we considered indoor scenes which are taken at a residential house in Germany and outdoor scenes which are taken at downtown Bremen. From this dataset, we randomly selected 44 scenes which consist of 27 outdoor scenes and 17 indoor scenes. We createed 42 CTP type forgeries by adding Bunny and Dragon models in 13 different outdoor scenes and 8 indoor scenes each. Next, we create 24 CRTP types of forgeries by inserting re-sampled Bunny and Dragon models in 7 outdoor scenes and 5 indoor scenes. We also create 10 subtractive and deforming forgeries by identifying the object using MATLAB visualization tool. Figures 4 and 6 show visualizations of CTP, CRTP type forgeries and subtractive, deforming forgeries respectively for different scenes. This exercise demonstrates that the LiDAR data can be easily manipulated to deceive algorithms. All types of forgery attacks on different datasets are provided in the ***supplementary material***.

Next, we apply forensic algorithms *IsDensityConsistent* (I) and *IsOcclusionConsistent* (II) to 44 original scans and 66 forged scans. For algorithm *IsOcclusionConsistent*, we used

(a) (b) (c) (d) (e)

Fig. 4: For LiDAR scan of the indoor scene 1 a) Original, b) CTP forged data, and c) CRTP forged data; Indoor scene 2 d) Original, and e) subtractive forgery.



(a) (b) (c) (d)

Fig. 5: Illustration of variation in sampling density based on distance from sensor a) top view of forged scene; b) $MIN_{ipd}(z)$, c) Moving average of signal $MIN_{ipd}(z)$, and d) Abnormalities/sudden changes in signal $MIN_{ipd}(z)$.

0.06 resolution factor for both θ and ϕ based on angle resolution of Riegl VS-400 and $A_{th} = 20$. As the forensic algorithms are designed focusing on additive attacks, we evaluate their performance on CTP and CRTP type forgeries only. Tables 1, 2 enlist the performance of the proposed forensic algorithms on the above mentioned dataset. It can be seen that the algorithm *IsDensityConsistent* works well for the CTP type forgeries, but most of the CRTP type of forgeries remain undetected. It can be observed from Figure 5 that, the MID increases as the distance from the sensor increases for original data. But the insertion of the high-density hoax object in the scene causes a sudden, persistent drop in it. Whereas re-sampling the hoax object to match the sampling density in the original scene before inserting it into the scene does not alter the MID distance and hence, remains undetected. On the other hand, the algorithm *IsOcclusionConsistent* performs well for both CTP and CRTP types of forgeries. As the algorithm *IsOcclusionConsistent* is independent of density, it even detects CRTP types forgeries with significantly high accuracy.

5. DISCUSSION

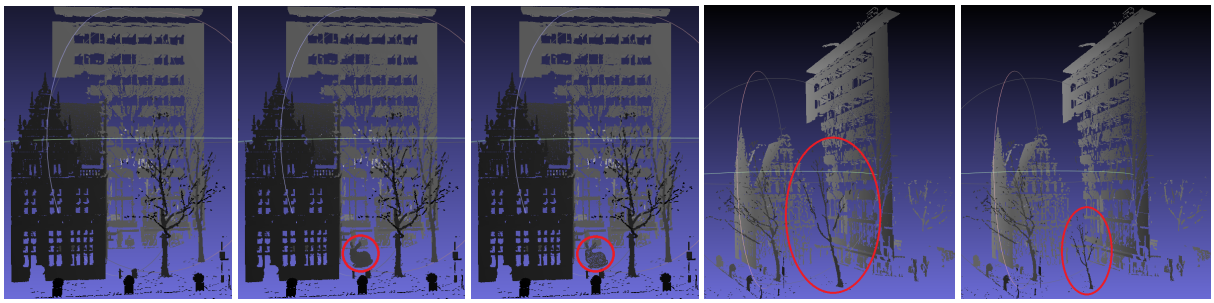
Some observations made during the study include:

Implementation Complexity: The complexity of the attack highly depends on whether the data is utilized by an algorithm or a human user. For example, for an automotive vehicle, a mere presence of hoax object alters the decision of algorithm. Hence, we mainly considered attacks on the LiDAR data that is used by algorithms. Among the attacks outlined here, additive attacks are easy to implement as they only require the forged object and it's desired placement in the scene. On the other hand, subtractive and deforming attacks need an additional understanding of the scene. Though, point cloud segmentation can be used to identify the object of interest, it increases the complexity of the attack significantly. However, given the required parameters, all types of forgeries can be created approximately in less than *50 milliseconds*.

Effectiveness of Attacks: When data is visualized by a human user, a more rigorous user study is needed to evaluate the effectiveness of attacks. As we only focus on applications that utilize raw LiDAR data, the effectiveness of attack is determined solely based on the possibility to perform it.

Limitations of the Forensic Approach: The proposed algorithm *IsDensityConsistent* is effective in the case of CTP type of forgeries whereas the algorithm *IsOcclusionConsistent* is efficient for both CTP and CRTP types of forgeries obtained using a single scan. But, if the LiDAR data is obtained by fusing multiple scans, these approaches may not be useful for detecting forgery in such cases. More sophisticated forensic methods need to be investigated to detect the extensive set of forgeries including subtractive and deforming forgeries.

Conclusions: An experimental study done in this paper opens up a new research area of forensic for LiDAR data. We have analyzed and identified possible attacks on the LiDAR data, which do not need additional hardware. Given the parameters for the modifications, these attacks can be carried out in real-time. We have also proposed two novel forensic approaches based on minimum inter-point distance and occlusion consistency for detecting additive forgery attacks. The analysis raises awareness to address possible threats to LiDAR data and to develop sophisticated forensic approaches for LiDAR data. Proposed attacks and forensic algorithm are also applicable to 3D point cloud data generated using other depth sensors as well. In future, we plan to exploit intrinsic properties of LiDAR data such as perspective projection to



(a) (b) (c) (d) (e)

Fig. 6: For LiDAR scan of the outdoor scene 1 a) Original, b) CTP forged data, and c) CRTP forged data; Side view of d) Original, and e) Deforming Forgery.

Outdoor Scenes	# of Scenes	Detected as Original		Detected as Forged	
		I	**II**	**I**	**II**
Original	27	25	26	2	1
CTP	26	1	0	25	26
CRTP	14	13	1	1	13
Indoor Scenes	# of Scenes	Detected as Original		Detected as Forged	
		I	**II**	**I**	**II**
Original	17	16	16	1	1
CTP	16	0	0	16	16
CRTP	10	9	0	1	10

Table 1: Performance of *IsDensityConsistent* and *IsOcclusionConsistent* on the experimental dataset

	Original		CTP		CRTP		Overall	
	I	**II**	**I**	**II**	**I**	**II**	**I**	**II**
Accuracy (in %)	93.18	95.45	97.62	100.00	8.33	95.83	76.36	97.27

Table 2: Classification accuracies of *IsDensityConsistent* and *IsOcclusionConsistent* on the experimental dataset

build a generic forensic algorithm to validate LiDAR data.

6. REFERENCES

[1] Csaba B., "3d people surveillance on range data sequences of a rotating lidar," *Pattern Recognition Letters*, vol. 50, pp. 149 – 158, 2014.

[2] "Automated tornado damage assessment and wind speed estimation based on terrestrial laser scanning," *Journal of Computing in Civil Engineering*, vol. 29, no. 3, pp. 04014051, 2015.

[3] Che-Yen W., Hsuan-Hsiao C., Chao-Kuo L., and Wen-Chao Y., "A study of applying light detection and ranging (lidar) to crime scene documentation," *Forensic Science Journal*, vol. 12, pp. 31–46, 2013.

[4] P. Francis, "At the scene of the crime," `http://www.pobonline.com/articles/92344-at-the-scene-of-the-crime`, September 3, 2006.

[5] E. Guizzo, "How Google's Self-Driving Car Works," Online, Oct. 2011.

[6] H. Farid, "Image forgery detection," *Signal Processing Magazine, IEEE*, vol. 26, no. 2, pp. 16–25, March 2009.

[7] S. Milani, M. Fontani, P. Bestagini, M. Barni, A. Piva, M. Tagliasacchi, and S. Tubaro, "An overview on video forensics," *APSIPA Transactions on Signal and Information Processing*, vol. 1, 2012.

[8] S. Raghuraman, K. Bahirat, and B. Prabhakaran, "Evaluating the efficacy of rgb-d cameras for surveillance.," in *ICME*. 2015, pp. 1–6, IEEE.

[9] K. Qi, X. Dong-qing, and Z. Da-fang, "A robust watermarking scheme for 3d point cloud models using self-similarity partition," in *Wireless Communications, Networking and Information Security 2010*, pp. 287–291.

[10] N Medimegh, S Belaid, and N Werghi, "A survey of the 3d triangular mesh watermarking techniques," *Int J Multimed*, vol. 1, no. 1, 2015.

[11] B. Yeo and M. Yeung, "Watermarking 3d objects for verification," *Computer Graphics and Applications, IEEE*, vol. 19, no. 1, pp. 36–45, 1999.

[12] J. Petit, B. Stottelaar, M. Feiri, and F. Kargl, "Remote attacks on automated vehicles sensors: Experiments on camera and lidar," in *Black Hat Europe*, 11/2015 2015.

[13] J. Petit and S. Shladover, "Potential cyberattacks on automated vehicles," *Intelligent Transportation Systems, IEEE Transactions on*, vol. 16, pp. 546–556, 2015.

[14] B. Zheng, Y. Zhao, Joey C. Yu, K. Ikeuchi, and S. Zhu, "Beyond point clouds: Scene understanding by reasoning geometry and physics," in *The IEEE Conference on Computer Vision and Pattern Recognition*, June 2013.

[15] H. Houshiar, J. Elseberg, D. Borrmann, and A. Nüchter, "A study of projections for key point based registration of panoramic terrestrial 3d laser scan," *Geo-spatial Information Science*, vol. 18, no. 1, pp. 11–31, 2015.

[16] A. Nüchter and K. Lingemann, "Robotic 3d scan repository," `http://kos.informatik.uni-osnabrueck.de/3Dscans`, 2010.