Privacy Algorithm for Cylindrical Holographic Weapons Surveillance System

Paul E. Keller, Douglas L. McMakin, David M. Sheen, A. David McKinnon, Jay W. Summet
Pacific Northwest National Laboratory, P.O. Box 999, Richland, WA 99352, USA
{paul.keller, doug.mcmakin, david.sheen, david.mckinnon}@pnl.gov, jay@summet.com

A novel personnel surveillance system has been developed to detect and identify threatening objects, which are undetectable by metal detectors, concealed on the human body. This new system can detect threats, which are fabricated with plastic, liquid, metal, or ceramic. It uses millimeter-wave array technology and a cylindrical holographic imaging algorithm to provide full-body, 360-degree coverage of a person in near real-time. This system is ideally suited for mass transportation centers such as airport checkpoints that require high throughput rates and full coverage.

Research and development efforts are underway to produce a privacy algorithm that removes the human features from the images while identifying the potential threats. This algorithm locates and segments the threats and places them on a wire-frame humanoid representation. The research areas for this algorithm development include artificial neural networks, image processing, edge detection, and dielectric measurements. This system is operational and results from this test and the privacy algorithm will be discussed in this paper.

INTRODUCTION

The technology employed in the cylindrical holographic image system (CHIS) includes a millimeter-wave (MM-wave) transceiver and array, high-speed digital signal processing computer, cylindrical scanner, and a cylindrical holographic imaging algorithm [1,2]. Because millimeter waves are, unlike x-rays, non-ionizing and therefore pose minimal health risks, they are ideally suited for surveillance of people. The array illuminates the person under surveillance with very low power millimeter waves, which readily penetrate clothing barriers and reflect off the body and concealed threats. These reflected signals are collected by the array and sent to a high-speed imaging computer where they are formed into very high-resolution radar images by the cylindrical holographic imaging software [3,4]. After the cylindrical holographic images are formed, they are sent to a video monitor where the system operator can detect and identify the concealed threats. Although this security system can detect and identify non-conventional concealed threats, it also displays human physical features in the imagery. This has delayed the full testing and implementation of this new scanning technology into airport checkpoints.

There is a perceived public opinion that directly presenting the imagery data to the operator would be unacceptable because of personal privacy concerns. It is believed that public acceptance of this type of screening system would likely be greater if the imagery was presented to a computer pattern recognition or segmentation algorithm for threat detection and identification rather than to a human operator. In this scenario, the operator would be retained in the security activity to clear the alarms generated by the privacy algorithm from either false positives or real threats. In 1997, work was initiated on a privacy algorithm for the CHIS with the near-term goal of developing software techniques to automatically segment concealed threats and innocuous items from the imagery and place these objects on a generic facsimile of a human. The ultimate goal for the privacy algorithm is to eliminate from the imagery all human features that may be considered too intrusive. This paper details the initial privacy algorithm development and laboratory testing.

Several techniques were applied to partially automate the detection of weapons in the imagery obtained from the CHIS system. All of these techniques are based on segmenting suspicious areas of the images and placing them on a wire-frame or optical video image of the person being scanned. This would alleviate privacy concerns by precluding the showing of the body parts of the person being scanned; instead, showing only detected items. The three segmenting techniques discussed in this paper, along with the results from this work, are:

- automation by using 3-D image depth information to segment suspicious areas for placement on optical video image or wire-frame model;
- automation by using pattern/texture recognition or segmentation schemes of the cylinder and mannequin data; and
- automation by using dielectric measurements to segment suspicious areas.

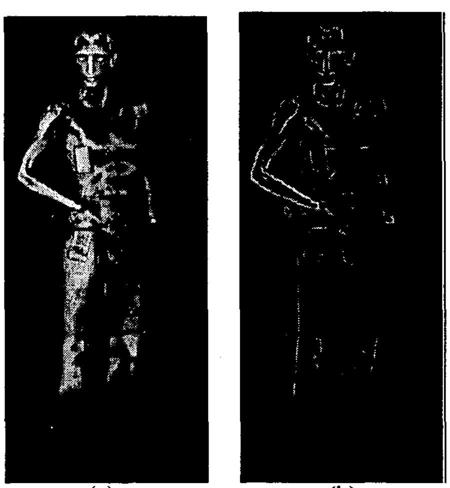
Additionally, this paper discusses work that was performed on the presentation techniques to the system operator that eliminate human features obtained in the MM-wave

0-7803-5247-5/99/$10.00 ©1999 IEEE

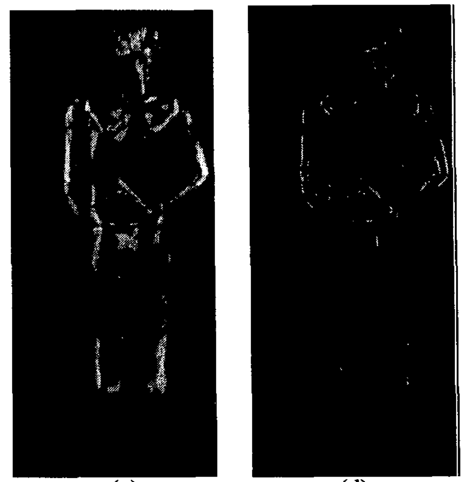
imagery. This paper also details preliminary test results from the application of pattern/texture recognition and segmentation schemes on data obtained from an operational test at the Seattle-Tacoma International Airport (Sea-Tac) in 1996 [5,6].

3-D IMAGE DEPTH INFORMATION TO SEGMENT SUSPICIOUS AREAS

A new three-dimensional (3-D) combined holographic algorithm has been developed. It uses cylindrical holographic imaging techniques similar to CHIS except that this new technique forms 3-D volumetric imagery that provides high-resolution depth information. Figures 1(a) and 1(c) show laboratory imaging results from this new technique. One reason for the success of this imaging technique is that the system uses a very wide-band transceiver to obtain very high depth resolution. With this reconstruction algorithm, edge and gradient detection algorithms can effectively be applied to the imagery to remove human features such as "skin" yet still retain the outline of the concealed objects. Figures 1(b) and 1(d) show the results of one edge detection algorithm applied to the 3-D combined holographic imagery. Figures 1(a) and 1(b) are pairs. In this imagery, innocuous items are concealed in a laboratory coat on the mannequin. These items are a cigarette pack concealed in a pocket near the chest and a hand calculator concealed in a pocket near the waist. As can be observed from the imagery in Figure 1(b) the "skin" is removed and the outline of the mannequin and concealed objects are still visible. Figures 1(c) and 1(d) are pairs. A Glock-17 handgun is concealed under the laboratory coat on the mannequin. Again, in Figure 1(d), the "skin" on the mannequin is removed and the outline of the concealed handgun remains clearly visible.



(a) (b)



(c) (d)

Figure 1. This figure illustrates the 3-D combined holographic image and morphological edge detection technique: (a) 3-D combined holographic image of mannequin with concealed cigarette pack and hand calculator, (b) morphological edge detection results, (c) 3-D combined holographic image of mannequin with concealed Glock-17 handgun, and (d) morphological edge detection result.

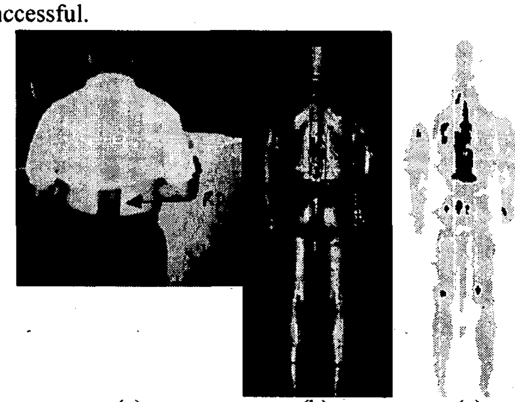
These edge and gradient detection algorithms are not yet fully implemented in software for automatically segmenting suspicious areas to place on either a wire-frame humanoid or optical video image. Software development with these techniques is ongoing and shows promise in simplifying the imagery and retaining shape information of the concealed objects. To fully realize these new techniques, the transceiver bandwidth must be increased and the 3-D combined holographic imaging algorithm should be implemented in the computer software.

PATTERN/TEXTURE RECOGNITION OR SEGMENTATION SCHEMES

Pattern or texture recognition schemes were explored in efforts to segment suspicious areas in the holographic images for subsequent placement on the wire-frame or video image of the person being scanned. Plastic, ceramic, and other dielectric items are partially transparent to the MM-wave illumination of the CHIS system. This often leads to a speckled texture on these items attributable to wave interference of the reflected and transmitted waves. This texture is substantially different from that of the human body's image and so may be used to segment dielectric items for subsequent removal and placement on the wire-frame or video image of the person being scanned. Therefore, texture may be used as a means of detecting concealed items in the holographic imagery.

To detect plastic texture in holographic imagery, a multi-layer perceptron artificial neural network (ANN) was developed and trained with the backpropagation of error algorithm [7] on images with plastic objects. Figure 2 shows the initial results from this work on the detection of RDX explosives that are concealed on a man. Figure 2(a) shows the optical image and Figure 2(b) shows the holographic image obtained with a rectilinear system at Ka band (27 – 33 GHz). Figure 2(c) shows the results of the ANN on the plastic explosive. As can be observed from the Figure 2(c), the plastic explosive is shown in red (dark gray in this paper), as are other areas that the ANN detected as plastic (false alarms). To reduce the number of false alarms found in the imagery, a frame to frame consistency-checking algorithm was developed.

Although the speckle detector can locate plastic objects by looking at texture in the image, a general-purpose man-made object detector would be useful for finding all threat objects. The first approach tried was to implement a Pulse-Coupled Neural Network (PCNN) [8]. A PCNN is a visual cortex model sometimes useful for object segmentation and edge detection. The initial implementation of the PCNN technique was not successful and additional development and understanding of the technique is required before it can be considered successful.



(a) (b) (c)

Figure 2. This figure shows the results of the ANN speckle detection algorithm for detecting RDX explosive: (a) optical image, (b) wide-band holographic image (27 – 33 GHz), and (c) ANN speckle detection results.

Man-made structures typically have higher spatial frequencies than natural objects such as the human body. With this knowledge, another man-made structure detection algorithm was initiated. This approach uses an artificial neural network trained on the spatial frequencies of image segments to identify possible areas on the image containing man-made structures. This work is ongoing and has not been fully proven.

DIELECTRIC MEASUREMENTS TO SEGMENT SUSPICIOUS AREAS

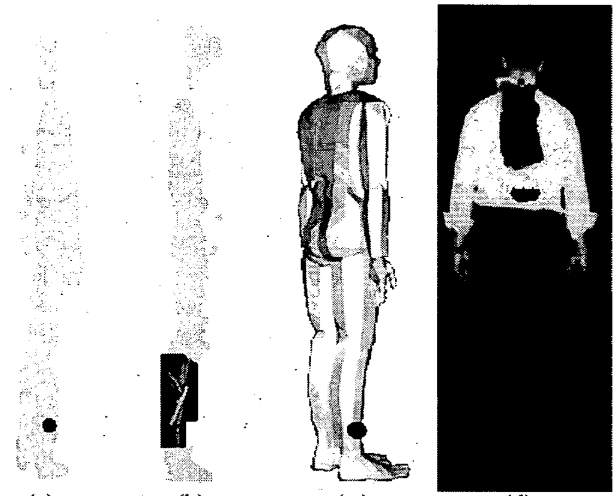
Dielectric measurement techniques were investigated with regard to the detection of concealed threats and anomalies and for the removal of the human body from the CHIS images. This was accomplished by performing dielectric and dissipation factor relative measurements of the person under surveillance. These relative measurements are performed by obtaining the amplitude and phase of the reflected signal in the antennas' field-of-view. These measured signals are similar to those obtained for the 3-D hologram. Although this technique would make CHIS a non-imaging system, the operator would be cued if there were anomalies hidden on the passenger. A wire mesh frame will be used to represent the passenger and anomalies will be located by CHIS and placed on the wire frame.

The results, however, show that this technique is highly unlikely to be successful because the contours of the human body affect the measurement results, producing a difficult inverse scatter problem.

SEGMENTATION AND DISPLAY TECHNIQUES

The summary of segmentation and display techniques for placing threats on the body is shown in Figure 3. Four potential techniques were explored and each one effectively removed privacy issues or human features from the MM-wave imagery. The first candidate display technique is shown in Figure 3(a). This technique thresholds the MM-wave image so that no detail of the person is in view. It displays the threat indication in red (black in this paper) on the silhouette. The second candidate, shown in Figure 3(b), is similar to the first except that a cutout view from the MM-wave images is displayed on the silhouette. The third candidate, shown in Figure 3(c), uses a 3-D-rendered generic human model generated from wire-frame polygons to match the various views of the millimeter wave movies. The threat is placed on the humanoid at the location where the privacy algorithm detects the threat in the MM-wave imagery. The fourth candidate is shown in Figure 3(d) and uses an optical image of the person and overlays the threat object from the privacy algorithm in red (black in this paper).

Because 360-degree, full body coverage of the person is advantageous for optimum threat detection, a 3D-facsimile of the human is necessary to show all sides of the person for accurate placement of the segmented concealed threat. A 3-D-rendering of a generic human model was generated from wire-frame polygons to match the 36 views in the snapshot millimeter-wave movies. Figure 4 illustrates a few frames from a 3-D-rendering of a generic human model movie indicating a flare gun on the lower leg. While this display technique is still under development, this work indicates the possibility of a generic human model replacing the outline of the individual in a future system.



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

Figure 3. This figure illustrates four proposed threat presentation and display techniques: (a) silhouette with threat indication, (b) silhouette with cutout view into threat area, (c) threat super-imposed on wire-frame rendered humanoid, and (d) threat super-imposed on optical image.

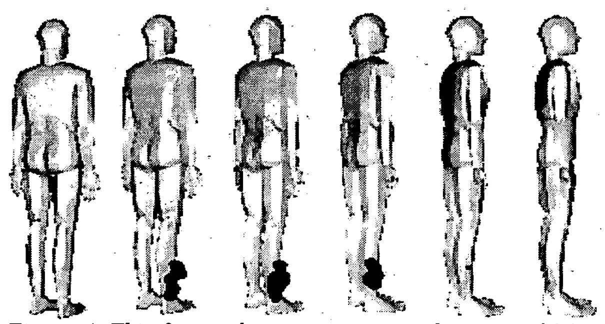


Figure 4. This figure shows a sequence of processed MM-wave frames indicating a potential threat object (flare gun) on the lower right leg.

PRELIMINARY PRIVACY ALGORITHM TESTING

Initial laboratory testing was performed on an ANN privacy algorithm that was trained to detect plastics in millimeter-wave holographic imagery. The ANN privacy algorithm utilizes texture pattern recognition techniques. In MM-wave holographic imagery, the texture of human skin is smooth and produces very little pixel-to-pixel variation. On the other hand, plastic materials typically have speckle texture patterns due to interference from the various returned coherent MM-waves which produces very rapid pixel-to-pixel variation in the image. By using these textural pattern attributes, an ANN was trained to detect speckle or rapid pixel-to-pixel variations.

The ANN privacy algorithm was trained and tested on the MM-wave database from the 1996 Sea-Tac airport screener test. The Sea-Tac movie test set contained 80 identical MM-wave movies at both Ka band (27 - 33 GHz) and Ku band (12 – 18 GHz). Forty of the movies contained no threat object and the other forty contained threat objects. Sixteen of the forty threat movies contained plastic threat objects (flare gun or simulated plastic explosives) and the other twenty-four contained non-plastic threats (guns and a knife). The Ka band and Ku band training movies were not identical, however. The Ka band had twenty-five training movies with nine containing plastic threats. The Ku band had twenty training movies with only five containing plastic threats. Of these five, only three could be used effectively to train the ANN, which affected the results from the ANN privacy algorithm Ku band test set.

The ANN speckle detection privacy algorithm was trained on the videos, which were used to train the checkpoint operators. The 1996 Sea-Tac airport test was conducted on two different frequency bands Ka (27 – 33 GHz) and Ku (12 – 18 GHz). The results from the 1996 Sea-Tac airport screener tests were compared to the speckle detection algorithm system. The results of the test on the Ka band videos with the human screeners and the ANN speckle detector at two sensitivities are shown in Figure 5. Although the probability of detection (P_d) is lower with the ANN, the probability of false alarm (P_{fa}) is lower as well for low sensitivity. For the high sensitivity case, the probability of detection has increased, but so has the probability of false alarms. Overall, these results show comparable performance of the ANN speckle detection algorithm to that of the human screeners for the detection of plastic threats.

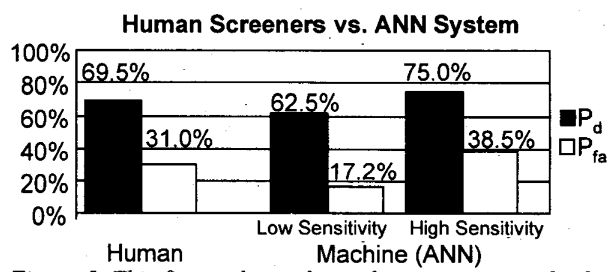


Figure 5. This figure shows the preliminary test results for human scanners and the ANN system at low and high sensitivities with Ka band videos. P_d is the probability of detection, and P_{fa} is the probability of a false alarm.

Figure 6 below shows results of a comparison of human screeners to the ANN speckle detection algorithms with Ku band (12 – 18 GHz) videos. The results in Figure 6 show that the Ku band ANN preformed with a poorer detection rate detecting fewer concealed plastic threats than the screeners did when trained with the original training set. This can be attributed to the fact that there were a lower number of plastic explosive training videos for the Ku band than for the Ka band. To improve the training video set, five videos with plastic explosives from the set which were shown to the screeners were randomly chosen and used to train the ANN. After training, a modified test was run and the results were similar to the human screener results. The results of this modified test are also shown in Figure 6.

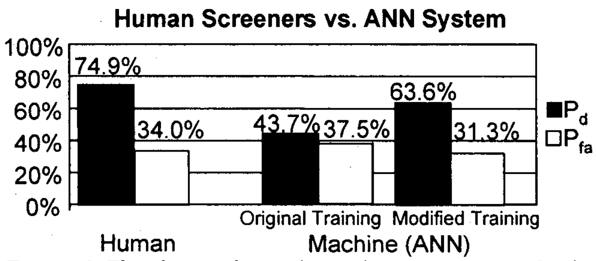


Figure 6. This figure shows the preliminary test results for human scanners and the ANN system developed with the original training set and a modified training set with Ku band videos.

DISCUSSION

While still in development, the research reported in this paper illustrates several technologies potentially important in the final implementation of an automated privacy algorithm for the millimeter-wave weapons screening system.

The 3-D image depth information shows potential for finding concealed objects through the use of gradients and edge detection methods. The dielectric measurement method can detect threats and anomalies by themselves, but is highly unlikely to be successful because the contours of the human body affect the measurement results, producing a difficult inverse scatter problem. The artificial neural network speckle detection algorithm is showing comparable results to human screeners for the detection of plastic threat objects and will likely show up in the final system. Finally, the various approaches outlined here must be automated and integrated into a single software package for the scanner.

Information about artificial neural network developments at Pacific Northwest National Laboratory is available on the World Wide Web at:

http://www.emsl.pnl.gov:2080/proj/neuron/neural/

ACKNOWLEDGEMENTS

The authors gratefully acknowledge the full support of this work by the U.S. Federal Aviation Administration under a Related Services Agreement with the U.S. Department of Energy. Pacific Northwest National Laboratory is a multiprogram national laboratory operated by Battelle Memorial Institute for the U.S. Department of Energy under Contract DE-AC06-76RLO 1830.

REFERENCES

1. D.M. Sheen, D.L. McMakin, H.D. Collins, T.E. Hall, and R.H. Severtsen, "Concealed explosive detection on personnel using a wideband holographic millimeter-wave imaging system," *AEROSENSE Aerospace/Defense Sensing and Controls*, Orlando, FL, USA, *Proceedings of the SPIE*, Vol. 2755, 1996.
2. D.L. McMakin, D.M. Sheen, H.D. Collins, T.E. Hall, and R.H. Severtsen, "Wideband, millimeter-wave, holographic weapons surveillance systems," *EUROPTO Symposium on Law Enforcement Technologies: Identification Technologies and Traffic Safety*, Munich, Germany, June 1995.
3. D.M. Sheen, D.L. McMakin, and T.E. Hall "Cylindrical millimeter-wave imaging technique for concealed weapon detection," *26th AIPR Workshop Exploiting New Image Sources and Sensors*, Washington, DC, USA, *Proceedings of the SPIE*, Vol. 3240, Oct. 1997.
4. D.L. McMakin, D.M. Sheen, T.E. Hall, and R.H. Severtsen, "Cylindrical holographic radar camera," *The International Symposium on Enabling Technologies for Law Enforcement and Security*, Boston, MA, USA, *Proceedings of the SPIE*, Vol. 3575, Nov. 1998.
5. D.L. McMakin, M.F. Bryan, A. Schur, and W.M. Harris, "Millimeter-wave Holographic Weapons Surveillance System (MMW-HWSS) Test and Evaluation Plan (TEP)," *DOT/FAA/AR-96/39*, Jan. 1996.
6. D.L. McMakin, G.F. Piepel, A. Schur, D.T. Donohoo, and W.M. Harris, "Millimeter-wave Holographic Weapons Surveillance System (MMW-HWSS) Test and Evaluation Report (TER)," *DOT/FAA/AR-96/40*, Oct. 1996.
7. D.E. Rumelhart, G.E. Hinton and R.J. Williams, "Learning internal representations by error propagation," *Parallel Distributed Processing: Explorations in the Microstructures of Cognition. Vol. 1: Foundations*, D.E. Rumelhart, J.L. McClelland, (ed.s), pp. 318-362, MIT Press, Cambridge, MA, USA, 1986.
8. T. Linblad and J.M. Kinser, *Image Processing using Pulse-Coupled Neural Networks*, Springer, London, UK, pp. 101-130, 1998.