Terrometer for Reflectionist artistic in(ter)vention: A handheld measuring instrument for measuring local terror levels

AUTHOR AUTHOR AUTHOR

***Abstract*—This paper presents the "terrometer" (terrorism meter) as a new artistic intervention, albeit in a more humourous rather than scholarly light.**

In the same way that unusual people (people of different skin colour, or people of different ethnic or physical appearance) are often singled out for suspicion, the terrometer creates a kind of reversalism of this scrutiny by purporting to look for unusual establishments. Instead of the usual Person of Interest, it purports to find "Buildings of Interest" or "Businesses of Interest".

The terrometer purports to measure unusualness or "weirdness" of places such as cities, streets, stairways, business establishments, and the like. What it actually measures — as a form of artistic intervention / inquiry / performance art — is aversion to measurement (e.g. the degree to which officials in those spaces object to the scrutiny purported by the terrometer).

The terrometer works by sensing this aversion to sousveillance (i.e. aversion to inverse surveillance) through sensing and classifying responses, gestures, movements, and the like, of people in those spaces. The apparatus comprises a hand-held camera and wearable computer system connected to a large d'Arsonval moving-coil meter movement that indicates the degree to which sensing (e.g. the very act of photography inherent in the computer vision system from which the terrometer is constructed) is contested by officials within the organization. Using a neural network and machine learning system, the terrometer classifies behaviour and indicates high "terrorism" levels in the presence of officials who objecting to its presence, and its scrutiny.

I. Introduction

This paper presents an artistic in(ter)vention that follows the traditions of organizations like Critical Arts Ensemble, The Santa Cruz Weapons Inspection Team, and other forms of "Citizen Inspections" for action, education, and social inquiry.

We build upon the sousveillance ("people watching people") notion of suspicion, with regards to terrorism in high-places, not just terrorism in low-places. We begin with an etymological look into the origins of the word "terrorism", and then, taken within its original context, as well as its current usage, show that terrorism, as broadly defined, has the potential to exist anywhere. We argue that our notions of suspicion should be pointed along ALL axes of evil, not just along **some axes**. Moreover, we argue that even if suspicion is directed along ALL axes, we still have not covered all of our bases, because this leaves the origin (of evil) unsuspected. Thus we must become a people watching all people, not just a people being watched by some people. It is this notion of everyone suspecting everyone else, rather than the masses being suspected by a select few, that gives rise to the invention of the **terrometer**. We present the invention of the terrometer, an instrument for measuring **terrosity levels**.

Fig. 1: Terrometer GOOD/BAD scale with needle at rest position wherein, lacking evidence of "GOOD", "BAD" is assumed.

The Emperor's New People

> "Some animals are more equal than others."
> – *the pigs in George Orwell's "Animal Farm"*

A. Etymology and first use of the word "terrorism"

Let us consider, for a moment, the etymology and first use of the word "terrorism". The ONLINE ETYMOLOGY DICTIONARY defines terrorism as follows:

> Terrorism is first attested 1795, "government intimidation during the Reign of Terror" (1793-July 1794) after the Fr. Revolution, from Fr. terrorisme. General sense of "systematic use of terror as a policy" is first recorded in Eng. 1798. Terrorize "coerce or deter by terror" first recorded 1823. [1] – earlier it was used of extremist revolutionaries in Russia (1866); and Jacobins during the French Revolution (1795) – from Fr. terroriste.

Note that Webster's includes terrorism as a mode of government:

Terrorism \Ter"ror*ism\, n. [Cf. F. terrorisme.] The act of terrorizing, or state of being terrorized; a mode of government by terror or intimidation.

–Jefferson.

(Webster's Revised Unabridged Dictionary (1913) [2]).

B. Committee Of Public Safety (C.O.P.S.)

While investigating the etymology and origins of terrorism, one will find that the first use of the word "terrorism" is to describe government action against its own citizens [3]:

> It [The Reign of Terror] was established by the government on Sept. 5, 1793, to take harsh measures against those suspected of being enemies... Controlled by the radical Committee of Public Safety... Terror eliminated enemies... A law passed in June 1794 that suspended a suspect's right to public trial or legal defense... About 300,000 suspects were arrested during the period; about 17,000 were executed, and many others died in prison.
>
> *–Britannica Encyclopedia*

C.O.P.S. was established for investigating acts of Treason and was a successor to the Legislative Assembly's 'Committee of Surveillance' which was responsible for the conduct of Terror, working with other branches of the government, to maintain enforcement of state security [4], [5], [6].

C. The enemy within

From the aforementioned origins of terrorism, it should be self evident that terrorism is not limited to the acts of a lone miscreant. The potential for terror exist everywhere, from "the THEM" to "the US". They might be terrorists and we might be terrorists. And we, jointly, and severally might be terrorists, i.e. we ourselves might be terrorists, and we, collectively (i.e. our governments) might also be terrorists. It has been said that:

> In the world we live in, you can't trust anybody. Even Presidents and First Ladys are making crime![7]

At protests against police brutality, people hold up signs or wear T-shirts stating, "Danger, Police in Area." (a quote perhaps attributable to artist Dread Scott).

Some have even gone so far as to say that any form of law enforcement is terrorism, and even that any form of enFORCEement in general is terrorism, i.e. that soldiers and police are terrorits.

While this view may seem extreme, it is kind of ironic that, according to the original first use of the word "terrorist", a suicide bomber would be a terrorist, if and only if his or her actions were sponsored by a government, and that if a police officer is paid for by a government, then he or she would fit the original definition of "terrorist" more closely than an independent criminal.

D. Locking only SOME of the doors

The potential for terrorism could come from any direction, i.e. from above or from below, and from left or from right. It might come from the Axes of Evil, or it might come from the Origin of Evil. (The point at which axes meet is called the "origin".)

Thus the **war on SOME drugs** or merely **locking SOME of the doors** is not sufficient to protect us from terrorism.

Imagine, for example, if you only locked the passenger side door of your car, but left the driver's side unlocked. Would it not make more sense to lock ALL the doors? Yet when we suspect each other ("people watching people") without suspecting the Emperor (or Empress), we leave ourselves open to the possibility that the Emperor might himself be a terrorist.

Terrorism is driving the future: it's time to see who's steering...

It seems that Today's homeland (in)security strategy is to lockdown only the passenger-side door, but leave the driver's side door unlocked. Why lock only the basement door when you leave the upstairs door unlocked?

Our Poetic License Server has expired, and we're outsourcing and outforcing our guns to our governments. With no guns ourselves, as we drill for ARMageddon, we don't Drill the Whole, we leave a hole in the drill. It is like having a fire drill in only some places but not others. Why not leave nothing undrilled? In addition to bioterror attack drills in which volunteers wear swimsuits under their clothes and are herded through showers, we should also drill for when goverment becomes opressive. Don't drill the passenger side only; don't drill only your right arm and let the rest of your body atrophy.

The first thing the terrorists will try to do is take control of our airports with their gunmen.

Gunmen: a gunman is a man with a gun.

Is a policeman with a gun, also a man with a gun (i.e. a gunman)?

Do we drill in case the wealthy landowner is a terrorist, or do we only do drills to prepare us for dirty bomb attacks by misfit miscreants? If the Enemy is Within, the enemy is drilled into us (bored into us). We've been reamed, tapped, and screwed.

In the past we were told "don't trust your neighbours", and now we're told that we should watch our neighbours. We're told that we should be a "people watching people", and that we should report suspicious activity to the authorities.

Turn in your neighbour but trust the police.

A terrorists cell or resistance cell is the opposite of Bentham's Panopticon (i.e. intercell trust, extracell mistrust).

The fact of the matter is, we never do drills or exercises to prevent insider terrorism. The traditional drill is to suspect a neighbour, i.e. another citizen, and never do we train on how to prevent takeover by the Emperor himself. What we need is a form of scrutiny that's blind to heirarchy, i.e. we need a system that suspects authority as much as it suspects individuals. The aphorism "question authority" becomes "suspect authority".

E. *We must all join in total war on terror*

Combatting terrorism:

Terrorism is now so pervasive that we must all enlist in total war against it. We're of the same religion, homeland security, so we must shoot first and shoot later, detect, document and eradicate all possible terrorist activity.

It is self evident that the only way to completely rid humanity of the possibility of terrorism is to eliminate humanity itself. However, since total human genocide is largely considered an undesirable solution, the next best solution is total activity awareness: People Watching People.

Since terrorism is clandestine by it's nature, anyone could be a terrorist or pre-terrorist sympathizer. Some terrorists, such as suicide bombers, are found to have come from the unwashed masses. Others, such as Maximilien Robespierre, author of the French Reign of Terror, have been found at the highest levels of government. No quality such as race, religion, age, gender or nationality can convey an imprimatur against guilt of terrorist persuation. Everyone from paupers to presidents are potential terrorist threats.

Therefore we must augment the existing and effective governmental tactic of suspecting and photographing everyone with a more grass-roots, pragmatic tactic of photographing one another. We must photograph one another since any of us may be terrorists. By documenting everyone and everything in this way, we can significantly reduce the possibility of terrorists in our midst going undetected. Furthermore, when alone, we must document ourselves since we may unknowingly begin terrorist thinking patterns at any time. Documenting our own private actions would therefore be our first line of defense against terrorism.

The current practice of monitoring merely **some** people is like the **war on some drugs** or the security of locking merely **some** doors. This practice is absured and obviously ineffective. We need to lockdown all the doors. We need a complete lockup, lockdown, washup, washdown, stripdown and documentation campaign for everyone. Without total war on terrorism, we are doomed to be slaves to terror without any hope of liberation.

To manage this total war on terrorism, we must establish a Committee Of Public Safety (C.O.P.S.), similar to the Commitee of Public Safety of the Council of the City of New York for post-September 11th security in New York City. COPS would oversee the Department of Homeland Security. In addition to it's oversight responsibilities, COPS would administer concomitant websites such as, cops.gov, for gathering daily documentation from citizens, and, turnin.gov, for citizens to report other citizens as suspected terrorists.

It may be noted that in order to safeguard ourselves from terrorism, we must all become like benevelent information terrorists to one another. This **ben** evelent information terrorism, (like Benthamism), is a kinder, gentler terrorism preventing malovelent terrorism by entirely supplanting it. Benthemism keeps us aware that we are all watching one another for the common good. In this way, just as one fights fire with fire, we can defeat negative terrorism with positive terrorism, the latter canceling out the former.

II. The Terrometer: An instrument for the measurement, capture, and reportage of terron counts in the range from one microterron to one Gigaterron

Accordingly, we designed and built an instrument that we call the **terrometer** (pronounced "traumeter"). The terrometer measures threat level. Unlike a divining rod, or the dowser that finds oil, or witches, the terrometer can be used to accurately and reliably locate terrorism.

Additionally, we propose a unit of measure that quantifies terrosity levels. We call the unit the **terron**. Our first prototype terrometer is accurate over a range from one microterron to one gigaterron, and provides a quick threat assessment.

Our first prototype had a logarthmic terrosity scale divided into seven color-coded regions:

1) Undetectable = White; Less than one microterron.
   No action required.
2) Low = Green; between one microterron and one milliterron.
   Refine and exercise appropriate preplanned Protective Measures; Ensure personnel receive proper training on the Homeland Security Advisory System and specific preplanned department or agency Protective Measures; and Institutionalize a process to assure that all facilities and regulated sectors are regularly assessed for vulnerabilities to terrorist attacks.
3) Guarded = Blue; between one milliterron and one terron.
   Check communications with designated emergency response or command locations; Review and update emergency response procedures.
4) Elevated = Yellow; between one terron and one Kiloterron.
   Increase surveillance of critical locations; Coordinate emergency plans as appropriate. Assess characteristics of the threat.
5) High = Orange; between one Kiloterron and one Megaterron.
   Coordinate security efforts with Federal, State, and local law enforcement, or National Guard. Take additional precautions at public events. Prepare to execute contingency procedures.
6) Severe = Red; between one Megaterron and one Gigaterron.
   Increase or redirecting personnel to address critical emergency needs; Assign emergency response personnel and pre-positioning and mobilizing specially trained teams or resources. Monitor, redirect, or constraining transportation systems. Close public and government facilities.
7) Hopeless = Black; greater than one Gigaterron.
   Armageddon has ensued. No action is possible because most of the world's population is dead. Your terrometer is likely damaged due to excess terrocity levels.

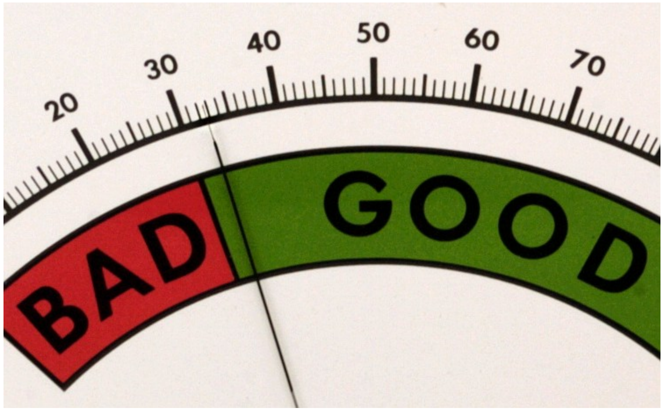

Fig. 3: Terrometer scale indicating "GOOD".

This seven color system was found to be too confusing to many of our terrometer users, and we therefore abandoned this design. Moreover, by having high terrometer readings on the right hand side, and lower values on the left (like a voltmeter), we found that the reverse association was often made, i.e. because people are used to the idea that good is to the right and evil is to the left. For example, a reading of 4.7 Kiloterrons would appear further on the right, than, for example, a reading of 3.3 microterrons, which would appear toward the left hand side of the scale.

A. Human Factors considerations in an improved terrometer design

Our next approach was to design a terrometer having a reversed scale reading in "INVERSE LOGARITHMIC TERRONS". And instead of the seven color system, we adopted a simpler, more familiar two color system: RED for EVIL (which we later changed to "BAD"), and GREEN for GOOD, as shown in the figure 2:

With the reversed scale, EVIL (BAD) is on the left, and GOOD is on the right, which is the way that most prospective customers seemed to like to have the scale arranged. That "EVIL" is a loaded word, we decided to use "BAD" and "GOOD", so that a user could determine whether or not it was safe to, for example, enter or exit through a doorway into a dark and potentially evil corridor.

With a reading of GOOD, as shown in figure 3: all that is required is a simple **lockup**, whereas with a reading in the RED (BAD), a full **lockdown**, and lockin (locking everyone in the building) for mass casualty decon, would be initiated.

III. Terrometer principle of operation

The key discovery leading to our invention of the terrometer was a simple observation that persons with dark and evil thoughts (i.e. those with terrorist thoughts) are more easily startled by a flash of light than those who are pure of thought. In particular, the terrometer measures the response, in the environment, to a stimulus that comprises a flash of light. The terrometer comprises a hand grip, with trigger, having a "hot shoe" mount for a standard photographic flash, such as a Nikon SB800, or the like. The photonic burst of energy from the terrometer, which it uses as the stimulus upon which to base its measurement, may be thought of as an antiterron ("terroff"). ("Terroff" is a portmanteau for Turning Terrons OFF.)

When launching an antiterron, more terrons migrate toward the locale. Much as electrons travel along the path of least resistance, terrons contaminate/propagate along the path of least resistance. Therefore, there is both safety and risk in the measurment of terron proliferation. Terrons are "other" (self is safe).

Our various terrometers come with a standard photographic "1/4, 20" (1/4 inch, 20 threads per inch) mount, so that dozens of terrometers can be affixed to a long bar, to make an antiterron pushbroom, for doing a clean sweep. From mineswepping to cell sweeping, (high density of terron cells), terrometers can thus work together in unison.

It was found that terrons self organize into sparsely connected autonomous cells (terrcells). Mature terrcells (terron cells) have a structure identical to the molecular structure of many bioterror agents.

Terrorism is neither a particle nor a wave, but it exhibits both particle and wavelike properties. We often have "waves" of terrorism (terrorism comes in waves), and terrorist "cells" (discrete particle-like entities). While cells are countable (i.e. "things"), waves are uncountable (i.e. "stuff"), and Terrons are neither things nor stuff (neither digital nor analog), but exist everywhere in both the digital and analog world. We cannot quarantine terrons to one or the other world, as they flow fluidly across digital/analog boundaries.

Victims of severe terron contamination can be guided (much as photons, by bending their paths), by means of specialy designed terrorist decontamination hospitals (TD Hospitals), into T-cell (terron afflicted cells), known as Correctional Facilities. We are also currently working on an Anti-Terrorism, video game, based on this paper, where each team, with a terrometer calibrated for their team, attempts to root out evil (where evil is defined as being a member of the opposite team).

IV. Some empirical observations on terrons

Terrons are formed in the brain, of certain afflicted individuals (victims of evil influence). On startup, the terrometer begins at "EVIL" ("BAD") until proven good. In fact, when the batteries of the terrometer run out, the needle of it's moving coil meter movement (d'Arsonval movement) falls to the leftmost (worst) end of the scale to indicate BAD, as a safety feature in keeping with our societal norm of "guilty until proven innocent" (EVIL until proven GOOD).

This is no safetycharm of some Church Of Anti Terror (COAT) of ARMS. This is a very accurate scientific instrument upon which prison sentences and executions can be reliably and accurately based!

As the needle leans more to the right, one can be sure that the situation is getting better.

With such a reliable and necessary instrument, it is suggested that nobody should be without a terrometer, in such

Fig. 2: Early prototype of terrometer in action: Measuring "terrosity" levels in a building's fire exit.

a dangerous world that we live. Everyone must aid in the detection and reporting of terrorism. Everyone has both a right and a responsibility to continuously monitor themselves and others for terron levels....

Terrometers work by measuring the Terron Transfer Function, which requires a stimulus and measured response. The stimulus comes from the excition ionizer, with a 300 to 480 volt potential, across cations and anions, in Xenon gas, to bring it into a plasma state. A suitable source is the Metz Mecablitz (330 volt system), or the Lumedyne product (480 volt system), but smaller units like the Nikon SB800 have been found to give satisfactory results at lower terron levels. Like RaDAR, the terrometer is an active measurement instrument, in that it sends out a signal and measures the response.

We could have prevented the Holocaust, had we had a terrometer, we could have aimed the terrometer at various SS men, and their nefarious essence would have would have been illuminated.

The terrometer captures the essence of a potentially evil soul. It can also save people before it's too late.

Moreover, the offset logarithmic scale reads only non negative results, i.e. inverse logarthmic terrosity levels not less than zero. This was necessary from a human factors point of view, otherwise negative values (i.e. if a DeciBel was used), would be confusing. In particular, it may be necessary to RECTIFY the behaviour of certain or all individuals. In this paper, "rectify" means prevention of negativity.

We cannot settle for a low cost terrometer, except for those who don't care too much about the safety of their families. Militerror grade terrometers are not suitable when a microterrometer is within our budgets. Militerron Police (MPs) are likely to only police when levels are above the milliterron level.

Terrorists are frightened of terrometers and will try to steal a terrometer.

The terrometer captures reflected light, and light is in fact related to good and evil (good and bad). The Devil is afraid of light, and God enLIGHTens, such that Terron level rises as dusk grows near: the threat level goes up every night, so we must all carry our terrometers at night.

The terrometer works together with a computer vision system to capture and measure the response. A typical computer vision camera when used with the terrometer has daylight, tungsten, flourescent settings, to adjust to suit individual lighting needs, but calibration of the terrometer itself is still necessary. If someone's wearing dark blue, or black, the instrument must be appropriately calibrated, plus three steps for dark blue, and plus four steps for black. This calibration is done using the thumbwheel that'ssculpted into the terrometer's ergonomic grip, as shown in figure 4:

V. "White Balance" and other concepts for fair and balanced operation of the terrometer

Almost all cameras have a "White Balance" feature. AWB (Automatic White Balance) is typical of low cost cameras suitable for use with the terrometer.

Fig. 4: The “white balance” thumb wheel on the terrometer.

The amount of light returned to the instrument may, of course, affect the reading, i.e. without compensating for the albedo of a person’s skin, an incorrect reading may be obtained. Calibration must always, of course, be done with an eye toward “zeroing” the terrometer as well as adjusting the above mentioned thumbwheel. Zeroing a d’Arsonval meter movement is well known in the art, and will not be elaborated upon here, except to show that such funcationality is present in the terrometer, as illustrated in figure 5:

If you go into a Black neighbourhood, you need to make sure you White balance the terrometer, otherwise you could get a(n) (t)erroneous (unbalanced) reading. White BALANCE is like the scales of justice: you need to white balance both the flash and the camera in order to get a FAIR AND BALANCED reading.

In particular, the terrometer must be set to proper ethnicity: black skin absorbs almost 3 f stops more light than white skin.

Terrons are related to photons, so, of course, the color spectrum comes into play. Anyone who objects to your use of a terrometer, is likely afflicted with high terrocity, and needs to

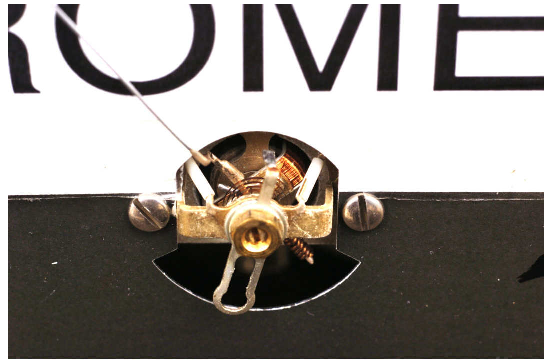

Fig. 5: Zeroing mechanism for the terrometer’s d’Arsonval meter movement

be reported (i.e. documented, which the terrometer, fortunately does as a side effect). High terrocity individuals need to be corrected (balanced), and reported to the C.O.P.S..

Prior to food purchase, you can use the terrometer to scan your food for terron levels. However, terrocity can only be measured in-situ, so, for example, once food is purchased, it’s terrocity level can no longer be measured. If there’s evil in the merchandise, the terrometer will move the terrons to the clerk, and posess the clerk. Take a terrometer into a liquor store, and you will notice that if there are grey-market bottles and such, (i.e. liquor with high methanol or other poison content), you will get a high terrosity reading from the vendor, or others working in the store. You cannot get a terron reading from inanimate objects, so it is essential that people are present in order to get a reading.

In particular, the whole science of terrometry is based on “people watching people”, not “people watching merchandise”.

If you take a terrometer to a pawnshop to measure potentially stolen merchandise, a high Terron reading indicates the presence of stolen merchandise. The terrometer will generally only give a high reading if the clerk knows the merchandise is stolen, but of course this is useful as culpability, else a false low reading may result. This culpability is related to the Entanglement theory of physics.

WARNING: Terrons may be hazardous to your health. If the terrosity level is greater than 1GT, evacuate the vicinity immediately.

VI. Measurement of terrosity

The cheapest and easiest way to measure reflected light is with a sensor array, such as CCD or CMOS.

Other than the computer programs that analyze the data to make the terron count, the terrometer is little more than a photographic flash light (to provide the excitation) and a camera (to measure the response). Thus, for example, if you point the terrometer at an officer of the law, if he’s a rogue police officer, he will of course get angry and try to take your camera, otherwise he’d have nothing to hide, because only criminals have something to hide. Only criminals have secrets.

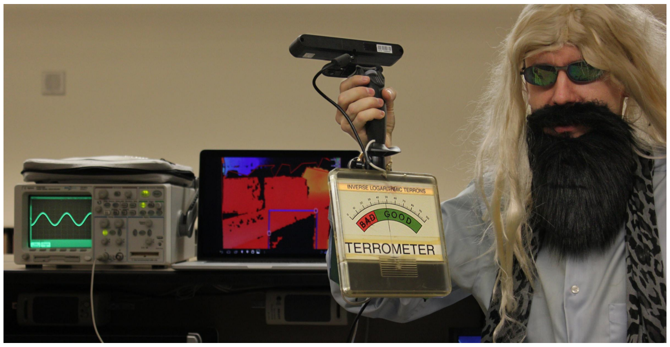

Fig. 6: Pierre Bataille with updated terrometer design using 3D Primesense camera and wearable computer: testing in lab.

Masked gunmen: a masked gunman is a terrorist (secrets). Historically only the bad guys wore masks, but now military do, so that they have also entered into the realm of darkness, evil, and terror.

But with our "people watching people" citizenry, many of us will wear a gas mask, because our government has warned us of the possibility of a bioterror attack. As we cover up our dark skin so that justice is blind (safer in a gas mask), we'll give the terrometers that others measure us with, a fair and (white) balanced reading.

In summary: Authority is good. Cameras are good. Anti-terrorism is good. We must all remember to keep our batteries charged and our terrometers ready.

VII. Going Further, 3D terrometer

An improved terrometer was built using a 3D Primesense camera, and a neural network and machine learning algorithm to detect irregular or unusual readings, most commonly generated by suspicious officials, who themselves therefore became suspects. The terrometer was attributed to a modern-day Leonardo daVinci figure, named Pierre Bataille. This work was presented to various design schools by way of a submitted portfolio of work, including the terrometer, as an example of visionary work that is "not sufficiently mediocre".

In this application, we are interested in having the terrometer to recognize gestures as the result of terror, shown in Figure 11. For this purpose, we resort to hand gesture recognition, which consists of two main components:

1) Hand detection
2) Gesture recognition

Hand detection concerns about how to robustly determine the contour of the hand in an environment with complex background; while gesture recognition is concerned about correctly interpreting the meaning of a gesture.

To achieve hand detection, many researchers take advantage of controlled environments, such as constant lighting and static background [8], [9]. However, these methods are not reliable in real world environments with complex lighting and background changes. Other methods focus on tonal based features. Some focuses on the skin tone as a feature to perform segmentation [10]. These features are not reliable in certain

Fig. 7: Testing updated terrometer in stairwell.

Fig. 8: Testing updated terrometer on public roadway.

background or lighting condition, for example, similar colours between the background and human skin. In addition, some methods use specially coloured gloves or other sensing device such as the data glove to provide additional information for segmentation [11]. Understanding the problems of the methods discussed above, we explore an alternative method based on the depth information provided by an infrared range camera, such as a PrimeSense camera, to perform close range hand detection. Such a camera computes the depth map which contains information of an object's distance with respect to the camera. The depth map can be considered as an additional dimension of information for feature extraction and image segmentation [12], [13]. Most of the current approaches use only an infrared range camera from a third person perspective. The solution assumes there is no confusion between the hands depth information with other obstacles in the environment. Besides the infrared range camera, some approaches use a combination of a single color camera, a stereo color camera and a thermal camera to obtain additional information for image processing and denoising[14]. These methods achieve promising results in the static indoor setting.

A. Proposed Method

For a mobile or a wearable platform, we attempt to minimize the number of devices in the system and instead of performing gesture recognition using PrimeSense camera from a third person view, where the camera observes the users gestures on a steady platform [15], we propose to use the camera from the first person perspective, where it is mounted on the user's eye glasses and observe the world from the user's point of view [16]. Therefore, a wearable construct based on the PrimeSense camera is of interest, which has appeared in the use of the navigation helmet proposed by Steve et. al [16].

Similar to methods [15], [10], [12], [13], we achieve the gesture recognition in two stages:

1) segmentation; and then
2) classification.

The purpose of the segmentation stage is to first locate the hands of the official objecting to being sensed (typicaly officials come to investigate and are then measured for "terrosity levels").

The outstretched hand of the official, for example, creates a form of gesture which can be classified by the neural network and machine learning algorithms implemented in the terrometer. We apply the classfication algorithm to a segmented image to identify suspicious (e.g. "no photography" gestures that might indicate the official has something to hide.

B. Segmentation

In order for the system to classify gestures (actions of the subject in response to the terrometer), it needs to first locate the hands. Since the hands of the subject are of interest, we assume the hands appear as objects within close proximity to the camera. This information can be obtained from the range camera sensor, like the PrimeSense camera. The PrimeSense camera provides two types of images:

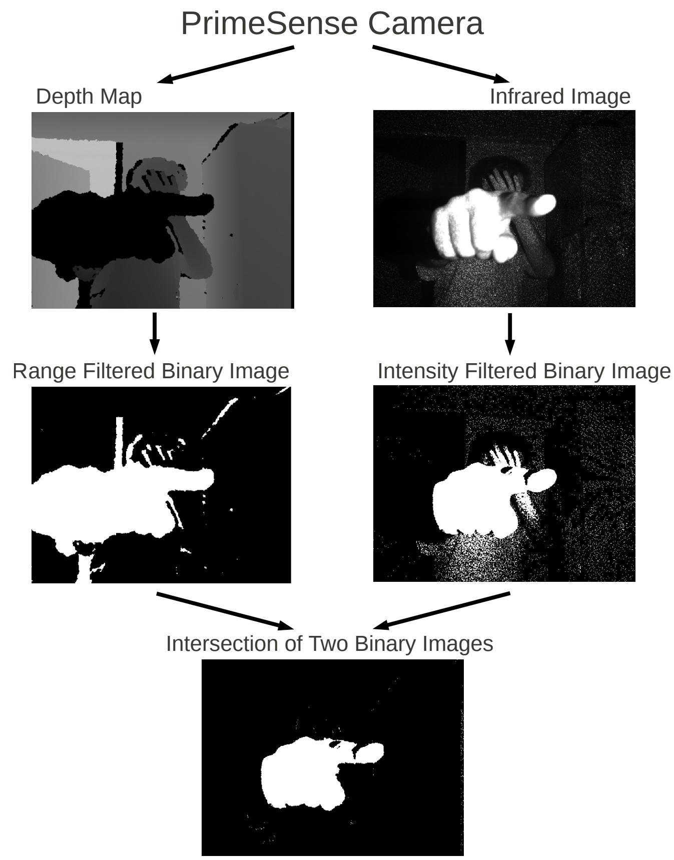

Fig. 9: Image segmentation example. The binary image on the left sets pixels to one if the depth map is unable to identify the subject's relative distance. The binary image on the right filters out the lower than threshold pixels by setting them to zero. The intersection of the two binary images becomes the image mask for gesture recognition. Notice that there is still noise present in the image mask. This noise is present when both binary images fail to filter out the out-of-range pixels. For example, a close distance bright light source is both unidentified in the depth map and is high in pixel values in the infrared image, causing unwanted interference. In subsequent models of the terrometer we overcome this problem by using 3D HDR (High Dynamic Range) sensing.

1) Infrared image
2) Computed depth map

The infrared image is a gray scale image that shows the level of infrared light sensed by the camera. The depth map is provided by the camera which approximates the distance of the objects in the scene. The two images are thresholded independently to filter out the pixels that do not meet the constraints. The results are two binary images that intersect to produce the final image mask, as shown in Figure 9. The image mask is a binary image for hand extraction.

Due to device limitations, the depth map can only return a finite range of distance values. This is a known hardware limitation. A depth map pixel is set to zero if the viewing object is either too close or too far from the camera. Additionally, the distance of any light source or reflective material in the scene that corrupts the projected pattern is unknown and set to zero. With the camera worn on the user's head, we

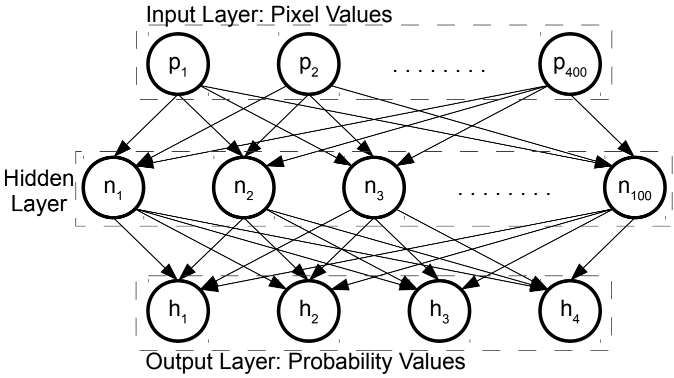

Fig. 10: The neural net implemented in the terrometer takes 400 pixels at the input layer; has 100 nodes in the hidden layer; and 4 output nodes. Each node represents the confidence of the input being a specific gesture.

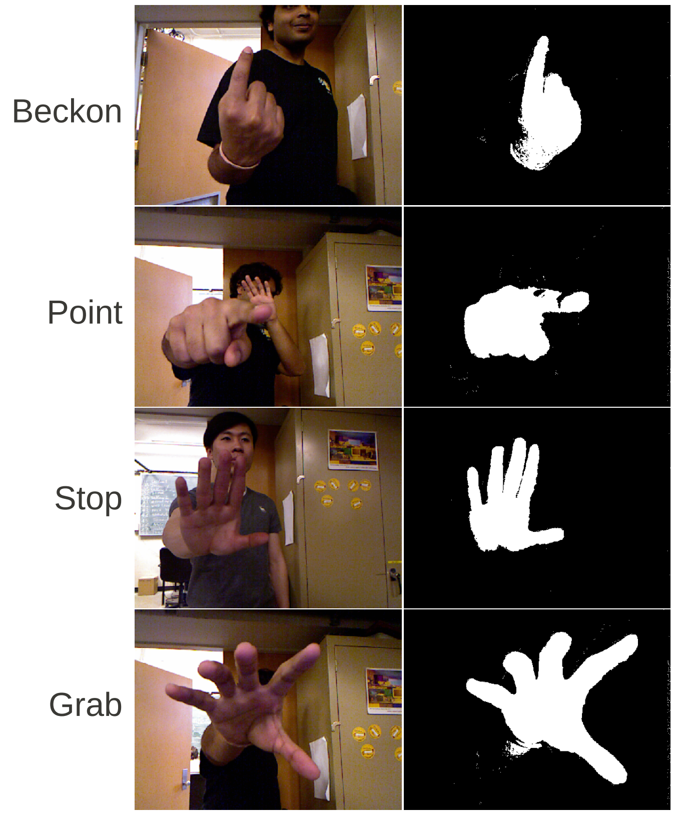

Fig. 11: Sample masked images of the four "photography disapproval gestures" trained into the neural net. During the classfication of the gesture, the system will recognize the two gestures: point-angled and point-up as finger pointing. This helps increase the flexibility of gesture recognition in identifying a series of "no photography" gestures as signs of disapproval (and therefore suspiciousness, i.e. "something to hide").

assume that the gestures appear within the distance range up to the fully stretched arm length away from the camera. This means that objects with depth values under certain threshold d_{th} are considered the candidates of the user's hand. However, this includes false candidates such as light sources, shadows, reflective objects, and distant objects. The resulting binary image sets the pixels under d_{th} to one and others set to zero.

Since the PrimeSense camera projects the patterns in the infrared spectrum, given the condition that no other infrared light source is present, the objects closer to the camera are relatively brighter than the objects from afar. We assume this property even with other light sources or highly reflective materials are present in the scene. With this assumption, a binary image based on the infrared image is created by thresholding the pixel values. Denote p_{th} as the pixel threshold, we set the pixels below p_{th} to zero and others to one.

The intersection of the two binary images is performed to generate the mask. The binary image of the infrared image filters out the distant objects that would appear as candidates in the binary image of the depth map while the binary image of the depth map filters out the pixel intensities greater than p_{th} that are too far from the camera, as shown in Figure 9.

To extract the hands from the image mask, we resort to fitting bounding boxes on the extracted contours. Typically, the two hands are the largest objects in the image mask. Therefore, we apply this heuristics of finding only the objects that are bounded by the two largest boxes. The two largest objects become the candidates for gesture recognition.

C. Classification

We use a single layer neural network to achieve real time suspiciousness or gesture recognition. The extracted image mask of the hands or other objects is resized to a 20×20 image. This image is fed into the neural network, and the neural network outputs the probability of each gesture. Each pixel in this image patch is treated as an input unit as shown in Figure 10. Therefore, our input vectors to the neural network are always 400 to 1. For the hidden layer, we choose to only implement 100 hidden units. By choosing a small number for the hidden units, we are able to limit our total parameter size to 40400. We decided this number is an efficient use of memory for a real time recognition system. Finally, we have 4 output units since there are 4 different possible gestures we are interested in, as shown in Figure 11. Each of these output units is the probability of an unique gesture.

To train our neural network, we first need to define the cost function. This function is the log likelihood of logistic regression. To find the best possible parameters for the model, we suppose to find find the parameter which will maximize this function. However, due to our gradient descent setting, we decided to add a minus sign in front of it and make it a minimization problem. Therefore, we are trying to maximize the log likelihood function using minimization techniques. To prevent over fitting to the training data, we added a regularization term by adding the square of each parameter at the end of the cost function. These regularization terms will punish the cost function as the parameters become too big, which can result in a floating point overflow. The training cost function $J(\theta)$:

$$J(\theta) = l(\theta) + R(\theta, \lambda) \tag{1}$$

The term $l(\theta)$ is the logistic regression for minimization:

$$l(\theta) = -\frac{1}{s}\sum_{i=1}^{s}\sum_{j=1}^{c}[y_j^{(i)} log(h_\theta(x^{(i)}))_j + (1 - y_j^{(i)}) log(1 - (h_\theta(x^{(i)}))_j)] \quad (2)$$

for which s denotes the total number of training cases and c denotes the total number of output gestures. Since our objective of this function is to add up the cost from each of our training cases. Thus, we use i to denote the current training cases that are being used to calculate the cost. $h_\theta(x^{(i)})$ denotes the estimation resulted from the forward propagation. After calculating the the estimate from forward propagation, we use a logistic function to rescale that number between 0 and 1.

The term $R(\theta, \lambda)$ is the regularization term:

$$R(\theta, \lambda) = \frac{\lambda}{2s}[\sum_{i=1}^{n}\sum_{j=1}^{p}(\theta_{i,j}^{(1)})^2 + \sum_{i=1}^{c}\sum_{j=1}^{n}(\theta_{i,j}^{(2)})^2] \quad (3)$$

for which n denotes the total number of nodes in the hidden layer and p denotes the total number of nodes in the input layer, which is also the number of pixel we have in each of our training image patch.

D. Training

The training data were collected using the PrimeSense camera to record a sequence of the image masks of various hand gestures. In particular, we focus on the following gestures:

- the framing gestures (consists of both hands that form the corners in diagonal of each other)
- the finger pointing gesture.

1) Gesture Variation: One problem associated with gesture recognition is that the the orientation or form of a single gesture varies, with respect to the user and instance. Specifically, we consider two types of variations: the variations due to change in orientation [12], [13], [15] and variations due to different forms of gesture that represent the same action.

Figure 12 shows some gestures that have the same meanings. The differences of these forms of gestures are not mere geometric transformation from one to another. To adapt to the form variations, we first define a group of different gestures that mean the same action. Each gesture of the same group is trained separately.

In addition to the form variations, we also attempt to train for the variations in orientation. This allows recognition system to adapt to slight angle changes of the hand. The inclusion of the variations helps the training to account for the gesture differences, which avoids limited recognition of only a single instance of the gesture.

2) Data Collection: Collecting more training data is one of the most effective way to improve the performance of a learning algorithm. In our setting, collecting more training data simply means recording more gesture samples in our daily use of the device. Although we are achieving high accuracy

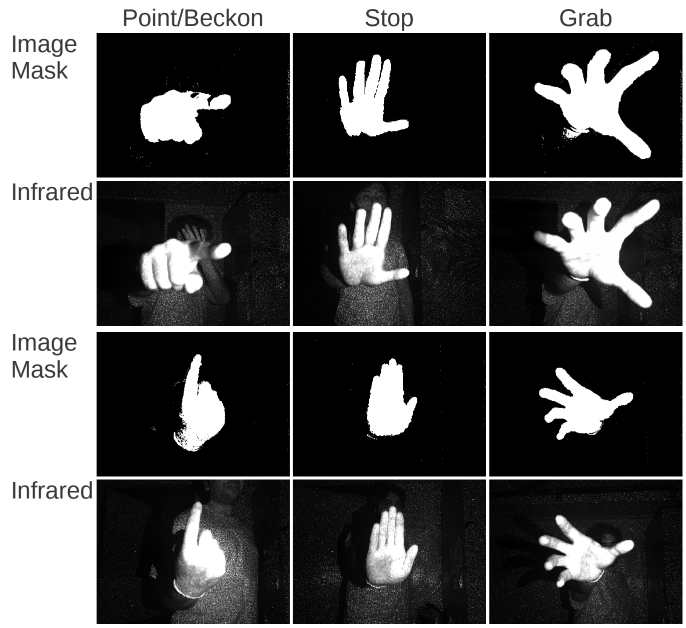

Fig. 12: Demonstration of the variations of gestures. The top two rows are one instance of the three different gestures: upper coner, lower corner and finger pointing. There are other possible gestures that represent the same action. The lower two rows are the examples of the alternative gesture of the top rows.

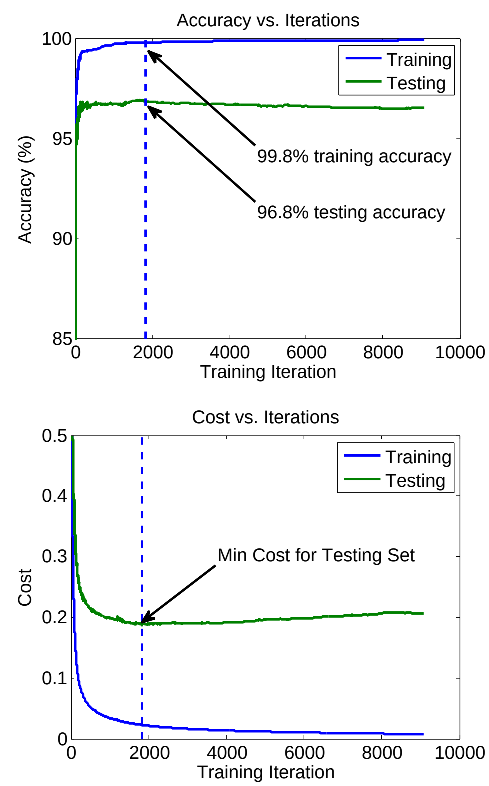

Fig. 13: A graph of the Cost function versus Training iteration. The graph shows the iteration at which to stop training the neural net - the minimum point of the testing cost. Beyond this iteration, more training causes an increase in the testing cost. At that iteration, the training set achieves a 99.8% accuracy and the testing set achieves 96.8% accuracy.

on our existing training data. We are constantly streaming our gestures and give label them with the correct label. This data collection approach will keep improving our learning algorithm the more we use it.

3) Early Stopping: In order to avoid over fitting to our training data. We separated 80% of our data as our training data and 20% of our data as test data. On every iteration of neural net training, we run forward propagation to get our gesture prediction accuracy and cost on both training and test set. We plot the cost on both training and test sets versus the number of training iterations as shown in Figure 13. As you can see in the Figure 13, at around iteration 2000, the cost of the test data starts to increase while the cost of the training data is still decreasing. This tells us that after approximately 2000 iterations, our neural net is being over trained to the training data, that is, if left to train forever, the neural network will only match items in the training data and reject everything else.

VIII. Implementation

In this project, our goal is to create and implement a believable "terrorism meter" that purports to detectu "unusualness", but that actually merely detects gestures of disapproval to being sensed (and therefore "terror" suspicion). This is done using gesture recognition. To achieve this, we utilize the ASUS Xtion sensor to observe the world and gestures from a first person view. The ASUS Xtion is a PrimeSense based range camera which provides depth maps and infrared images of the scene it is observing. This camera uses an infrared projector and infrared camera to determine an image depth map. The images are processed in real time with an ODROID-X, which is an Android-based mobile development platform with a 1.7GHz ARM Cortex-A9 Quad Core processor. Finally we display the result either on the d'Arsonval moving-coil meter movement, or on a separate Epson Moverio BT-100 worn by the user of the terrometer (or both). The Epson Moverio BT-100 is a transparent head mounted display that runs on Android 2.2. Based on the wearable computing principles discussed in [17], Epson's Moverio is a good candidate for mediated reality applications due to its transparent displays. The Moverio is capable of streaming from an external NTSC source and was therefore used as a display for the processed information from the range camera. In this project, we processed the range camera information with ODROID-X and added additional mediated reality information to the Moverio. The user will see a mediated reality, such as a mediated terrorism map, derived from the subject gesture interface that will interact with real world objects.

A. Performance

The training stage of our neural network achieved an accuracy of 99.8%. The cross-validation of the trained neural network achieved an accuracy of 96.8%. The performance in frames-per-second (FPS) on the ODROID-X is 20 FPS.

IX. Conclusion

Various embodiments of a device we call a terrometer have been designed, built, and tested. The first prototype of the terrometer functioned by creating a flash of light and measuring the response (e.g. of suspicous "camera-shy" individuals with "something to hide") to the flaosh of light. The response was measured using change detection programs that analyzed the output of a camera, to quantify the degree to which persons in view of the camera altered their behaviour (motion) in response to the flash. The optical flowfield differencing was displayed on a moving coil d'Arsonval movement, for easy viewing.

In the second embodiment, a 3D Primesense camera was built into the terrometer, and used with a machine learning system to quantify the "wierdness" or irregularity of spaces, and of the response to officials protecting or surveilling those spaces. The result of the neural-network-based learning algorithm was displayed on the moving coil d'Arsonval meter movement, and, in some cases, a head-mounted display as well.

Although clever subjects can "trick" the terrometer into low readings, by ignoring the flash, a side effect of widespread terrometery is likely to be the end of prohibitions on sousveillance, which could lead to a fair and balanced "people looking at people" world.

Acknowledgment

The Authors would like to thank Epson, ODROID and ASUS for their contributions to this project.

References

[1] O. E. Dictionary. [Online]. Available: http://www.etymonline.com/index.php?term=terrorism

[2] W. R. U. Dictionary. Webster's revised unabridged dictionary (1913 + 1928). [Online]. Available: http://machaut.uchicago.edu/?resource=Webster3=on

[3] B. Encyclopedia. Reign of terror (french history). [Online]. Available: http://www.britannica.com/EBchecked/topic/588360/Reign-of-Terror

[4] J.-B. Clery, "Journal of the Terror, Translation of Clery's Journal de ce qui s'est passe a la tour du Temple, and of Edgeworth de Firmont's Dernieres heures de Louis XVI." Littlehampton Book Services Ltd; New edition edition, 1974, ISBN 0460041541.

[5] D. Greer, *Incidence of the Terror During the French Revolution: A Statistical Interpretation*. Peter Smith Pub Inc., 1935, ISBN 978-0-8446-1211-9.

[6] D. Edelstein, *The Terror of Natural Right*. University of Chicago Press, 2009 ISBN 978-0-226-18438-8.

[7] S. Mann, "Shootingback," *the winners of the prix ars electronica 1997*, Sep 8-13 1997, http://www.rito.com/prix/winners.htm See also, http://wearcomp.org/shootingback.html.

[8] K. Imagawa, S. Lu, and S. Igi, "Color-based hands tracking system for sign language recognition," in *Automatic Face and Gesture Recognition, 1998. Proceedings. Third IEEE International Conference on*. IEEE, 1998, pp. 462–467.

[9] P. Hong, M. Turk, and T. Huang, "Gesture modeling and recognition using finite state machines," in *Automatic Face and Gesture Recognition, 2000. Proceedings. Fourth IEEE International Conference on*. IEEE, 2000, pp. 410–415.

[10] R. Kjeldsen and J. Kender, "Toward the use of gesture in traditional user interfaces," in *Automatic Face and Gesture Recognition, 1996., Proceedings of the Second International Conference on*. IEEE, 1996, pp. 151–156.

[11] D. Sturman and D. Zeltzer, "A survey of glove-based input," *Computer Graphics and Applications, IEEE*, vol. 14, no. 1, pp. 30–39, 1994.

[12] Z. Ren, J. Yuan, and Z. Zhang, “Robust hand gesture recognition based on finger-earth mover’s distance with a commodity depth camera,” in *Proceedings of the 19th ACM international conference on Multimedia*. ACM, 2011, pp. 1093–1096.

[13] D. Uebersax, J. Gall, M. Van den Bergh, and L. Van Gool, “Real-time sign language letter and word recognition from depth data,” in *Computer Vision Workshops (ICCV Workshops), 2011 IEEE International Conference on*. IEEE, 2011, pp. 383–390.

[14] J. Appenrodt, A. Al-Hamadi, and B. Michaelis, “Data gathering for gesture recognition systems based on single color-, stereo color-and thermal cameras,” *International Journal of Signal Processing, Image Processing and Pattern Recognition*, vol. 3, no. 1, pp. 37–50, 2010.

[15] Z. Li and R. Jarvis, “Real time hand gesture recognition using a range camera,” in *Australasian Conference on Robotics and Automation*, 2009, pp. 21–27.

[16] S. Mann, J. Huang, R. Janzen, R. Lo, V. Rampersad, A. Chen, and T. Doha, “Blind navigation with a wearable range camera and vibrotactile helmet,” in *Proceedings of the 19th ACM international conference on Multimedia*. ACM, 2011, pp. 1325–1328.

[17] S. Mann, “Wearable computing: Toward humanistic intelligence,” *Intelligent Systems, IEEE*, vol. 16, no. 3, pp. 10–15, 2001.