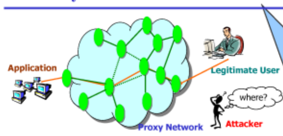
An Analysis of Location-Hiding Using Overlay Networks

Ju Wang and Andrew A. Chien
Department of Computer Science and Engineering, University of California San Diego

Overlay Network for Location-Hiding

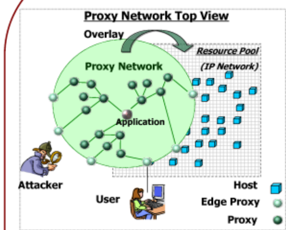


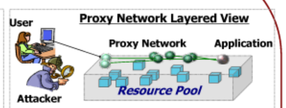
- Communication infrastructure to allow applications to communicate with users without disclosing IP addresses
- Protect applications from direct attacks

Problems

- Can proxy networks achieve location-hiding? If so, under what circumstances? (feasibility)
- How long will it take attackers to reveal application location? (metrics)
- How do properties of defense & proxy networks affect location-hiding? (parametric)
  - Resource recovery
  - Proxy network reconfiguration
  - Correlated host vulnerability

Generic Framework for Location-Hiding





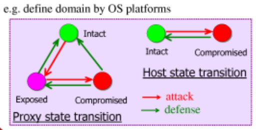
- Proxies: software components run on hosts
- Proxies adjacent: iff IP addresses mutually known
- Proxy Network Topology: adjacency structure
- Depth: min distance (hops) from edge proxies to app
- Edge proxies publish their IP addresses
- Users access applications via edge proxies

Attack Model

- Goal: reveal application location (IP address)
- Compromise hosts and reveal (expose) location of adjacent proxies
- Penetrate proxy network using exposed location information

Correlated Vulnerability

- Hosts w/ similar configurations grouped as domain
  - High correlation inside domain
  - Low correlation across domains
- e.g. define domain by OS platforms



Defense Model

- Goal: recover compromised hosts, invalidate information attackers have
- Resource recovery
  - Recover compromised hosts
  - Reactive recovery: detection-triggered
  - Proactive reset: periodic reload/security patch
- Proxy network reconfiguration
  - Invalidate information attackers have
  - e.g. proxy migration

Stochastic Model

Notation	Meaning	Examples*
λ_0	Rate of new vulnerability discovery	Bi-weekly
λ_v	Rate of compromise w/ known bugs	~minute
μ_s	Rate of proactive resets	λ_0-relative
ρ	True positive ratio of reactive	≥0.80
μ_d	Speed of reactive recovery	Real time
μ_r	Rate of proxy migration	10~100xλ_0

* Data shown in examples are inferred from Microsoft Security Bulletin critical vulnerability data, worm propagation speed, Lippmann et al Intrusion detection systems evaluation results, and our prototype proxy network evaluation results.

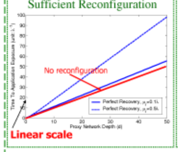
Feasibility of Location-Hiding

Uncorrelated Vulnerability

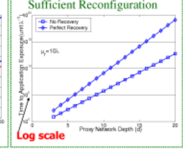
Theorem I Without proxy network reconfiguration, the expected time to application exposure $T \le dT_\lambda$ where T_λ is the expected time to compromise a host, d is proxy network depth.

Theorem II Consider a proxy network with random proxy migration rate μ_r ($\mu_r \ge 2\lambda$), the expected time to application exposure T grows exponentially with the proxy network depth d; specifically $\Theta((\frac{\mu_r}{2\lambda})^{d-2})T_\lambda \lesssim T \lesssim \Theta((\frac{\mu_r}{\lambda})^{d-1})T_\lambda$

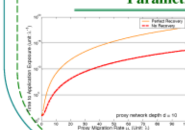
Location-Hiding Infeasible w/o Sufficient Reconfiguration



Location-Hiding Feasible with Sufficient Reconfiguration



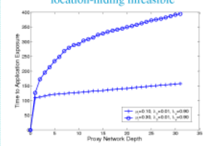
Parametric Study



- migration has qualitative impact
- migration rate + proxy network depth ➔ exponential improvement
- resource recovery limited impact

Correlated Vulnerability

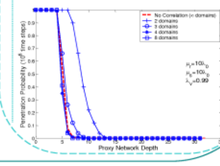
Correlated host vulnerabilities can make location-hiding infeasible



All hosts share similar vulnerabilities (single domain). Even with high migration rates, can't achieve location-hiding. λ_v the dominant attack rate, is much here than migration rate.

Exploiting limited host diversity & intelligent proxy placement achieves location-hiding

- Interleave proxies on different domains
- Proxies migrate inside domain



Summary

- Design of a generic framework and analytic model for proxy network approaches to location-hiding
- Using analytic modeling and simulation techniques, we characterize key properties of proxy network and find
  - Existing approaches employing static structure are vulnerable to host compromise attacks
  - Adding proactive defenses employing proxy network reconfiguration and migration makes location-hiding feasible, proxy network depth & reconfiguration rates are critical factors
  - Correlated host vulnerability can make location-hiding infeasible
  - By exploiting limited host diversity and intelligent construction of proxy network, negative impact of correlation can be mitigated and location-hiding can be achieved

Work in Progress

- Impact of overlay topology in location-hiding (SSRS'03)
  - Using a similar model, we characterize favorable and unfavorable topologies for location-hiding from a graph theoretic perspective
  - Found high connectivity, a merit in other context, may undermine location-hiding
  - Popular overlays, e.g. Chord, are unfavorable for location-hiding; low-dimensional CAN and binary de Bruijn graphs are favorable.
- Proxy Network DoS Resilience (empirical study)
  - Simulation testbed: large scale Internet simulator (MicroGrid)
  - Proxy network working prototype
  - Real DDoS attack tool (Trinoo) and real application (Apache)
  - Study impact of attack and effectiveness of proxy network (impact of proxy deployment as well)

This work is supported in part by the National Science Foundation under awards NSF EIA-99-75020 Grads and NSF Cooperative Agreement ANI-0225642 (OptIPuter), NSF CCR-0331645 (VGrADS), NSF NGS-0305390, and NSF Research Infrastructure Grant EIA-0303622. Support from Hewlett-Packard, BigBangwidth, Microsoft, and Intel is also gratefully acknowledged.

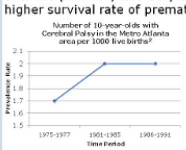
Using a Computer to Engage Children With Cerebral Palsy

Miyako Jones
Dr. Suleyman Uludag, faculty advisor

Department of Computer Science, Engineering, and Physics

1. INTRODUCTION

Cerebral palsy is a group of nonprogressive, incurable brain disorders that affect motor control. The spastic type is most common, with its main symptom being stiff muscles. People with this type often have trouble using their hands and/or arms. According to the Centers for Disease Control and Prevention, "each year about 10,000 babies born in the U.S. will develop cerebral palsy."[1] The number of children born who will develop cerebral palsy has remained about the same over the past 30 years despite medical advances due to the higher survival rate of premature infants.



Toys have a significant impact on a child's cognitive, social, and physical development, but children with cerebral palsy have a difficult time playing with them.[4] There are devices known as switches available to help the physically disabled access computers and other electronic devices, but very few toys are adapted for switch access.

2. OBJECTIVE

Develop a computer interface that a child with cerebral palsy could use to interact with a robotic adaptive toy.

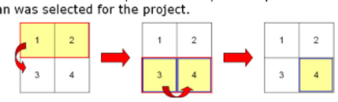
3. MATERIALS/METHODS

Mayer-Johnson's **Boardmaker® Plus!** is educational software that teachers can use to create computer-interactive or printable materials known as "boards" for disabled children. It supports alternative methods of computer access such as switches and can interact with external programs.

Boardmaker® Plus! version six splash screen

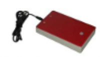
an example board

People with cerebral palsy interact with computers by using one or more switches and a method called scanning. Computer software highlights possible selections by row then by column until the user's selection is highlighted. There are three forms: auto-scan, inverse scan, and step-scan. Auto-scan was selected for the project.



Two types of switches were used with Boardmaker® Plus!, each connected to the PC via a USB switch interface that emulates keyboard keys. Both switches emulated the spacebar.

Jelly Beamer wireless switch



QuizWorks slammer wired switch

QuizWorks USB Switch Interface Plus

A toy piano and a robotic arm were also used for the project.

Little Tikes® Baby Tap-a-Tune piano

Lynxmotion AL5D robotic arm kit

4. RESULTS

Three boards were created. Each had buttons to command the robot to hit keys on the piano and to switch between boards. Two boards had selectable childrens' songs.

main piano board (key group selected)

song board #1 (navigation group selected)

song board #2

Each time a key or song is selected in Boardmaker® Plus!, an argument representing the selection is passed to an external Microsoft Windows batch file. Each key, key combination, and song is represented by a series of commands for the robot.

```
:BLUE-KEY

echo #4 P2050 >com4
echo #0 P1875 >com4
ping -n 2 127.0.0.1 >nul

echo #2 P1925 >com4
echo #2 P1840 >com4
ping -n 2 127.0.0.1 >nul

EXIT
```

This command group instructs the robot to hit the blue piano key.

The robot was connected to the PC via a serial port and all commands were sent to it through **COM4**.

#4 represents one of the robot's servomotors while **P2050** represents a position.

127.0.0.1 is the IP address of the local computer (localhost).

5. CONCLUSIONS

Tools that can be used to give children with cerebral palsy access to nonadaptive devices already exist, but setting up a system can be complicated. More research should be conducted on using commercially-available software such as Boardmaker® Plus! to give disabled children access to nonadaptive toys.

6. ACKNOWLEGEMENTS

Team members:
- Terrence Trapp, Elizabeth City State University, Elizabeth City, NC (batch file programming)
- Naquasia Jones, Spelman College, Atlanta, GA. (robotics)

Sponsored by:
- Georgia Institute of Technology (Georgia Tech), Atlanta, GA.
- Dr. Ayanna M. Howard, Assistant Professor, Georgia Tech School of Electrical and Computer Engineering
- The Human-Automation Systems (HumAnS) Lab

Funded by:
- The National Science Foundation
- Agilent Technologies Foundation
- Advancing Robotics Technology for Societal Impact Alliance

7. REFERENCES

1. National Institute of Neurological Disorders and Stroke (NINDS). (2010, April 12). Cerebral palsy: Hope through research. *NINDS homepage* [Online]. Available: http://www.ninds.nih.gov/disorders/cerebral_palsy/detail_cerebral_palsy.htm.
2. S. Winter, A. Autry, C. Boyle and M. Yeargin-Allsopp. (2002, December). Trends in the prevalence of cerebral palsy in a population-based study. *Pediatrics* [Online, Print]. 110(6), pp. 1220-1225. Available: http://pediatrics.aappublications.org/cgi/content/full/110/6/1220.
3. National Center on Birth Defects and Developmental Disabilities. (2004, October 29). Cerebral Palsy. *CDC homepage* [Online]. Available: http://www.cdc.gov/ncbddd/dd/cp3.htm.
4. A. M. Howard, "A Robot Playmate for Engaging Children with Severe Physical Disabilities," 2009.

SENSOR EQUIPPED PARKING LOT

Prapti Shrestha
PShrestha06@winona.edu

Introduction

Everyone who has driven a car has experienced the frustration of finding an empty spot in a crowded parking lot. To help drivers overcome this problem, we propose the use of an iPhone app that is integrated with a sensor-equipped parking lot that will direct its user to the closest empty parking spot.

Hypothesis

By integrating an iPhone app with a parking lot that is equipped with zigbee enabled distance sensors, it is possible to accurately detect whether or not a parking spot is empty in 80% of possible weather conditions, including temperature ranges between -20F and 115F and environmental conditions involving precipitation, cloudy conditions, dusty, and humid conditions.

Methodology

Testing environments for the distance sensor:

- Low temperature, without snow
- Low temperature, with snow
- High temperature
- All the temperature range between the lowest to the highest
- Rainy weather
- Dusty environment
- Windy weather

Design of the parking lot:

- Parking lot was set up with the infrared proximity sensor
  - Two sensors were planted so that a parked car would come between them
  - This set up would help distinguish whether the data obtained was an actually from a parked car or other small objects such as soda can, twig etc.

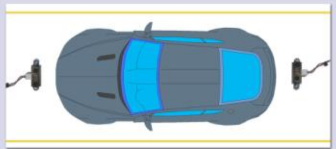


Fig 1: Set up of the parking lot with two distance sensors

Data Collection

Fig 2: Flow of data from sensors to gateway to idigi cloud and to iPhone application

iPhone Application

Fig 3: Data input and output for iPhone app users to assist them in finding a free parking spot

Results

Temperature (ºC)	Temperature (F)	Sensor Works
Below -17	Below 1.39	No
-17 to 46.53	1.39 to 115.75	Yes
Above 46.53	Above 115.75	No test performed

Table 1: Results from experiments with different temperatures

Condition	Sensor Works	Correct Results
Drizzle	Yes (but not accurate)	67%
Light Rain	Yes (but not accurate)	50%
Heavy Rain	Yes (but not accurate)	50%
Light Snow Fall	Yes (but not accurate)	50%
Snow Fall	Yes (but not accurate)	33%
Windy Environment	Yes	100%
Dusty Environment	Yes	86%

Table 2: Results from experiments with different levels of precipitation, wind and dust

Analysis

- Use of zigbee nodes to establish a wireless network was efficient and energy saving.
- It is possible to get real time data from parking lot where infrared proximity sensor used.
- Using two distance sensors in parking lot to differentiate car from other objects was helpful in finding out if data from sensor was from car or smaller objects lying in the parking spot.
- Users of application can be notified of what parking spaces are available in the closer proximity.

Conclusion

This research project gives us an idea of how the proximity sensor and zigbee modules can be integrated with the mobile phone application to set up a smart parking lot system to let the drivers worry less about parking spaces in the parking lot.

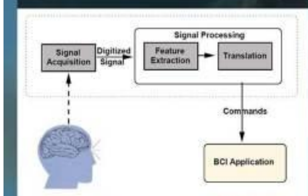
WINONA
STATE UNIVERSITY
Computer Science Department
http://cs.winona.edu

Real and Virtual World navigation with the Help of Brain-Computer Interfaces (BCI's)

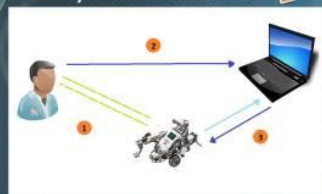
Research Student: Athanasios Vourvopoulos (vourvopa@uni.coventry.ac.uk)
Supervisor: Dr Fotis Liarokapis (F.Liarokapis@coventry.ac.uk)

1 Introduction

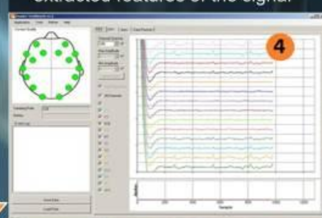
- Extracting valuable information from user's brain activity by interacting with both real world objects and virtual world environments
- Lego NXT Robot, a computer simulation and commercial BCI headsets
- Comparison on how fast the brain adapts on sensory motor coordination and control by getting neuro-feedback in a closed loop



2 System Overview

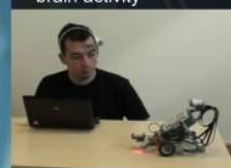


- User is visually stimulated
- Raw data are filtered on the EEG headset chip and sent to the computer
- A client/server application
- Robot moves based on the extracted features of the signal



3 Between two worlds...

- Lego NXT Mindstorms Robot paired with a commercial BCI headset
- Basic manoeuvring based on the users brain activity



- A game has been designed using a 3D reconstruction of the robot, navigating through a simple maze using the same BCI

4 Conclusions

- Identifying and extracting features from brainwaves in a closed neuro-feedback loop through serious games and multimodal interfaces
- Include the combination of more sophisticated non-invasive devices equipped with more electrodes and sensors

Website: http://www.vourvopoulos.com
iWARG: http://wwwm.coventry.ac.uk/researchnet/iwarg/Pages/iWARG.aspx
Videos: http://www.youtube.com/user/vourvopa
Twitter: http://twitter.com/athanv

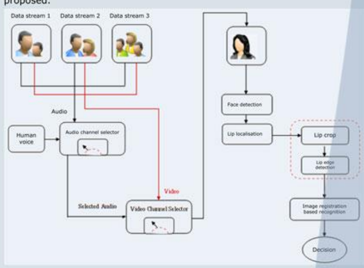
SPEAKER IDENTIFICATION FOR VIDEO CONFERENCE

S.Saravi, I.Zafar, E.A.Edirisinghe

research school of informatics

INTRODUCTION

Automatic speaker identification in videoconferencing will allow conference attendees to focus on the conference rather than manually identifying the active channel and the speaker. In this work we present a real-time, audio-video based approach to address this problem, but focus more on the video analysis side. The initial stage consists of a face detector, followed by a lip-localization algorithm. A novel approach for lip movement detection based on *image registration* and using the *Coherent Point Drift (CPD)* algorithm is proposed.



PROPOSED SYSTEM

Step 1: Face detection

For this purpose the OpenCV face detector is used

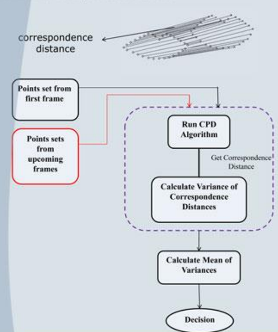
- ❑ The problem is false and undesirable object detections.
- ❑ As a solution, first step is to get the position of the biggest rectangle (not necessarily the face) and next step is to compare its position with that of the rectangle from the previous frame; set to the previous rectangle's position if necessary.

Step 2: Lip Localisation

A closer crop of the lips results in easier edge detection. Lips are located in the bottom third and middle two quarters of face. Then Canny edge detection is used to detect lip corners point by point. These points are saved as data sets for further use.

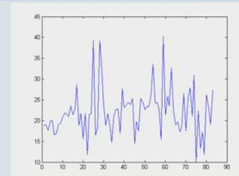
Step 3: Lip movement detection

Proposed approach for lip movement detection is based on image registration. Usage of this method is in evaluation or combination of the data acquired from different measurements. Coherent Point Drift (CPD) is a new technique for registration of point sets. The idea is to move one point set coherently to align with the other set and measure the change of shape using the variance of correspondence distance.



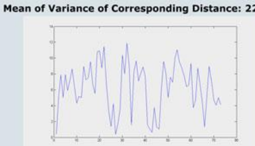
By calculating mean of variances it is obvious that average below 15 belongs to non talking and above15 belongs to talking face.

EXPERIMENTAL RESULTS



Results of a talking human video

Mean of Variance of Corresponding Distance: 22.1025



Results of a not talking human video

Mean of Variance of Corresponding Distance: 6.2881

CONCLUSION

1. Improvement of the OpenCV face detector
2. Design and Implementation of an algorithm for lip localisation
3. Modification and use of CPD algorithm in lip movement detection

REFERENCES

1. Andriy Myronenko. 2006. Coherent Point Drift (CPD) [Online] Available at: http://www.bme.ogi.edu/~myron/matlab/cpd/
2. A.Myronenko, X. Song, M._A. Carreira-Perpi~n_an: Non-rigid point set registration: Coherent Point Drift, NIPS'19.
3. Andriy Myronenko, Xubo Song, and Miguel Carreira-Perpinan. Non-rigid point set registration: Coherent point drift. In B. Sch□olkopf, J. Platt, and T. Ho_man, editors, Advances in Neural Information Processing Systems (NIPS) 19.
4. OpenCVWiki. 2009. FullOpenCVWiki. [Online] Available at: http://opencv.willowgarage.com/wiki/FullOpenCVWiki

Digital Imaging Research Group
Computer Science Department
Holywell Park
Loughborough University
LE11 3TU

Website: http://lboro.ac.uk/departments/co
Sara Saravi: s.saravi@lboro.ac.uk
Iffat Zafar: i.zafar@lboro.ac.uk
Eran A. Edirisinghe: e.a.edirisinghe@lboro.ac.uk

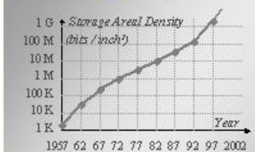
Loughborough University

Dynamic Encoding for Optical Storage Systems

Leo Selavo, Donald M. Chiarulli, Steven P. Levitan
University of Pittsburgh

We propose dynamic encoding for page oriented memories.

1. Motivation

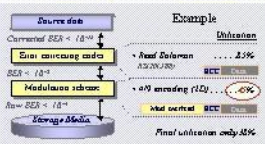


- Data density doubles every 9 months for magnetic storage
- There is a theoretical limit due to superparamagnetism
- What are the alternatives?
- Optical volumetric storage
- Problem: **Data Integrity**
  Solution: Data Encoding

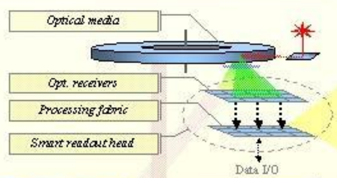
2. Typical solutions

- Improving bit-error-rate (BER) at the cost of media utilization

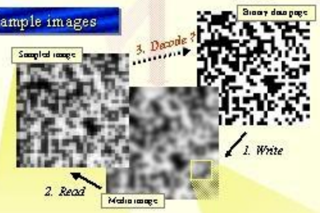
$$BER = \frac{\text{Wrong bits}}{\text{Total bits}} \qquad Utilization = \frac{\text{Source data bits}}{\text{Encoded data bits}} (\%)$$



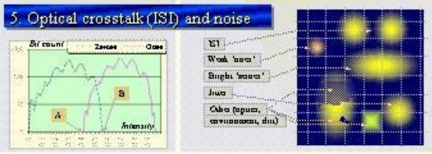
3. Optical disk readout system architecture



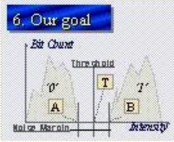
4. Sample images



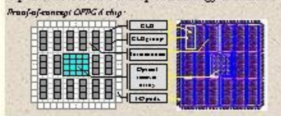
5. Optical crosstalk (ISI) and noise



6. Our goal



Optical detectors-on-chip technology is feasible.

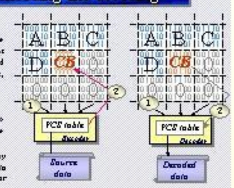


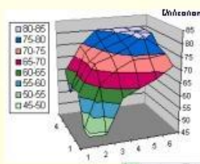
7. Static vs. dynamic encoding

8. Approach: dynamic encoding and decoding

1. Determine the set of valid code blocks (VCS)
   - Enumerate the code blocks for the CB, thus creating VCS. A code is considered valid if it does not create destructive ISI. Note, that the whole data page is available and blocks A, B, C and D are used for VCS generation. VCS can be computed in various ways, trading utilization for computational complexity.
2. Map the data using the computed VCS
   - VCS is used as a translation table. Thus, source data is mapped to appropriate CB for the encoding, or CB is mapped to a source data for the decoding.

In order for the decoding to take place, each pixel is read by the detector array using a threshold. The resulting binary raw data array is transformed into array of light intensities taking into account ISI. Now VCS can be found for each CB location, which will be the same as used for the encoding.





Various size CBs and exponential time algorithm yield up to 81% of utilization.

Dyn X ->			Thresholds:		0.37	0.43
Y v	1	2	3	4	5	6
1	49	49	62	65	68	72
2	49	66	71	74	74	75
3	61	72	74	77	81	76
4	61	71	76	78	81	
5	57	73	77	80	80	
6	64	74	80			

Utilization vs. various CB sizes

9. Simulation results

The noise margins are measured

Changing the threshold the utilization can be increased to 83%. Noise margin should be below 4%

Conclusions

- The novel modulation scheme **Dynamic Data Encoding** is a good candidate for page oriented memories
- Good code rates (utilization):
  - Dynamic exponential time algorithm: 83%
  - Dynamic linear time algorithm: 55%
  - Static encoding: only 45%
- There is a potential for good algorithms
- "Smart readout head" architecture is feasible

Contour Simplification

Ethan Yong-Hui Goh

DUKE COMPUTER SCIENCE

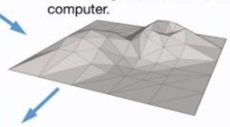
Problem

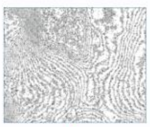
The advent of modern LiDAR technology has allowed for geographic data to be gathered *en masse*. However, high resolution measurements cause programmatically generated contour maps to be large and noisy. Our goal is to produce a scalable algorithm to simplify contours via edge operations on the Triangulated Network.

Background

Planes scan the terrain using lasers and take **billions** of height measurements of the ground.

These points can be displayed as a **Triangulated Mesh** on a computer.





From the triangulation, we intersect the surface with level planes to **generate contours**, but they are noisy.

The final output is a neat, simplified version of the contours.

Goals

- Smartly simplify the Triangulated Mesh to produce “neat” and smooth contours.
- Target and remove less important features of the terrain such as bushes and small crevices.
- Simplify the terrain enough to fit in memory.

Approach

Edge Flip

Motivation

- Thin triangles result in a higher number of contour segments, increasing the storage size.
- Edge Flips change the convexity of the surface, measured by the **dihedral angle** of the associated tetrahedron.

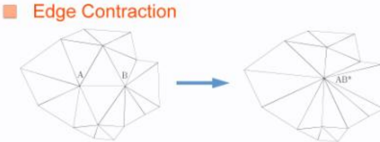
Delaunay Edge Flip

- **Delaunay Edge Flips** maintain the visually pleasing Delaunay property, and also makes the TIN are more accurate for interpolation.

Long Edge Flip

- **Long Edge Flips** reduces the number of thin triangles when a contraction is performed on them.

Edge Contraction

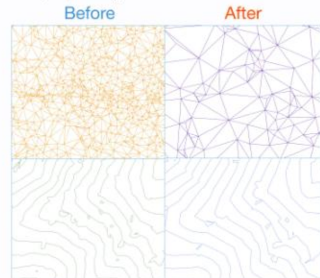


Motivation

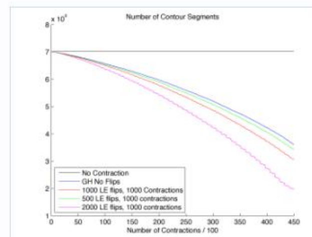
- Reduction of vertices and edges.
- Edge operations are intuitive and versatile.
- **Garland and Heckbert** devised an algorithm (GH) for surface simplification based on edge operations.
- Modify GH to control contour output.
- **Shorter edges** are more favorable to contract, since the error induced will be lower.
- Placement of the vertex is important - we attempt to **minimize distortion** to the surface.

Results

For a dataset of over 2 million triangles and 1 million vertices, the algorithm takes approximately **60 minutes** to perform 1,000,000 edge contractions.



The figure above shows before and after of contractions with Delaunay Flips. The error metric used in this experiment is a quadratic error metric. Intuitively, it measures the new vertex's **distance from edge** that has been contracted.



We compare the number of contour segments after several runs of the algorithm with alternation between contractions and Long Edge Flips. Note that long edge flips prepare triangles for contraction, and tend to decrease the total number of contour segments.

Special thanks to my advisor Pankaj K. Agarwal and mentor Thomas Mølhave.