

UNIVERSITY OF THE WEST OF ENGLAND

*How I will use my research and other experience
to enhance the curriculum*

Dr. Phil Legg

email@plegg.me.uk

4th November 2014

ABOUT ME

- ▶ I've always had a passion for Computing:
 - ▶ As a child, I started out programming BASIC on a BBC Micro Computer.
 - ▶ As a teenager, I was making web sites and Flash games.
 - ▶ Now, I enjoy being able to use computers to solve real-world problems to improve quality of life.
 - ▶ Application areas include:
 - ▶ Medical analysis
 - ▶ Sports and Entertainment
 - ▶ Cyber security
 - ▶ ... *but always interested to explore more!*



INFORMATION SECURITY

MACHINE LEARNING

DATA VISUALIZATION

MALWARE ANALYSIS

VISUAL ANALYTICS

MOBILE SOFTWARE DEVELOPMENT

COMPUTER GRAPHICS

HUMAN-COMPUTER INTERACTION

IMAGE PROCESSING

Corporate
Insider Threat
Detection

Sports Video
Visualization

Medical Image
Processing

Cyber
Security
Centre,
University of
Oxford

Swansea
University

Cardiff
University

2013-present

2010-2013

2006-2010

INFORMATION SECURITY

MACHINE LEARNING

DATA VISUALIZATION

MALWARE ANALYSIS

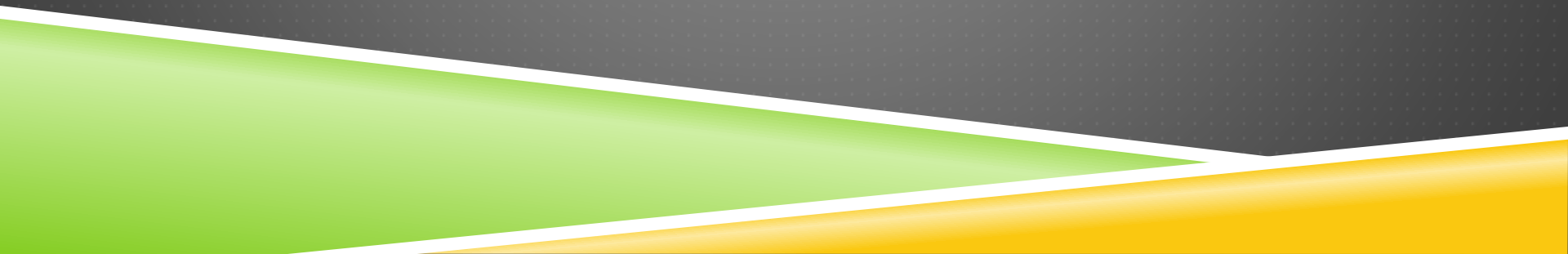
VISUAL ANALYTICS

MOBILE SOFTWARE DEVELOPMENT

COMPUTER GRAPHICS

HUMAN-COMPUTER INTERACTION

IMAGE PROCESSING



INFORMATION SECURITY

MACHINE LEARNING

DATA VISUALIZATION

MALWARE ANALYSIS

VISUAL ANALYTICS

MOBILE SOFTWARE DEVELOPMENT

COMPUTER GRAPHICS

HUMAN-COMPUTER INTERACTION

IMAGE PROCESSING

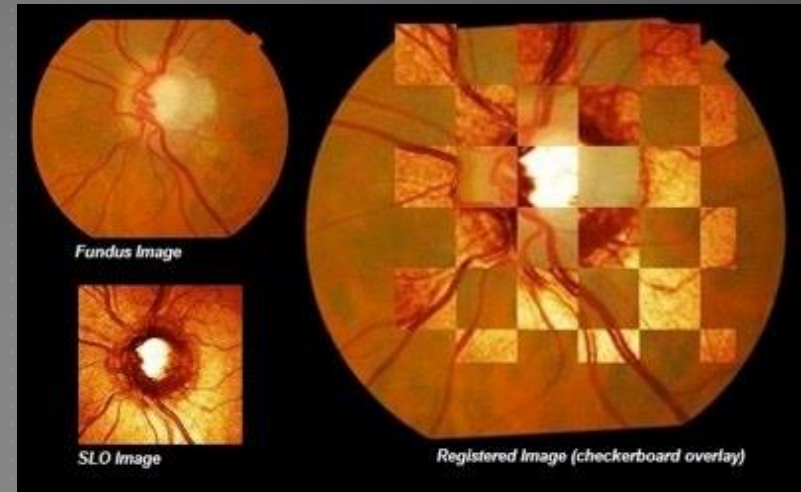
VISUAL COMPUTING COURSE MATERIAL:

- Using OpenCV, WebGL, and D3
- 3D transformations
- Modelling 3D objects
- Lighting and rendering
- Image enhancement
- Image feature extraction
- Object recognition
- Stereo imaging
- Theory and application of visualization



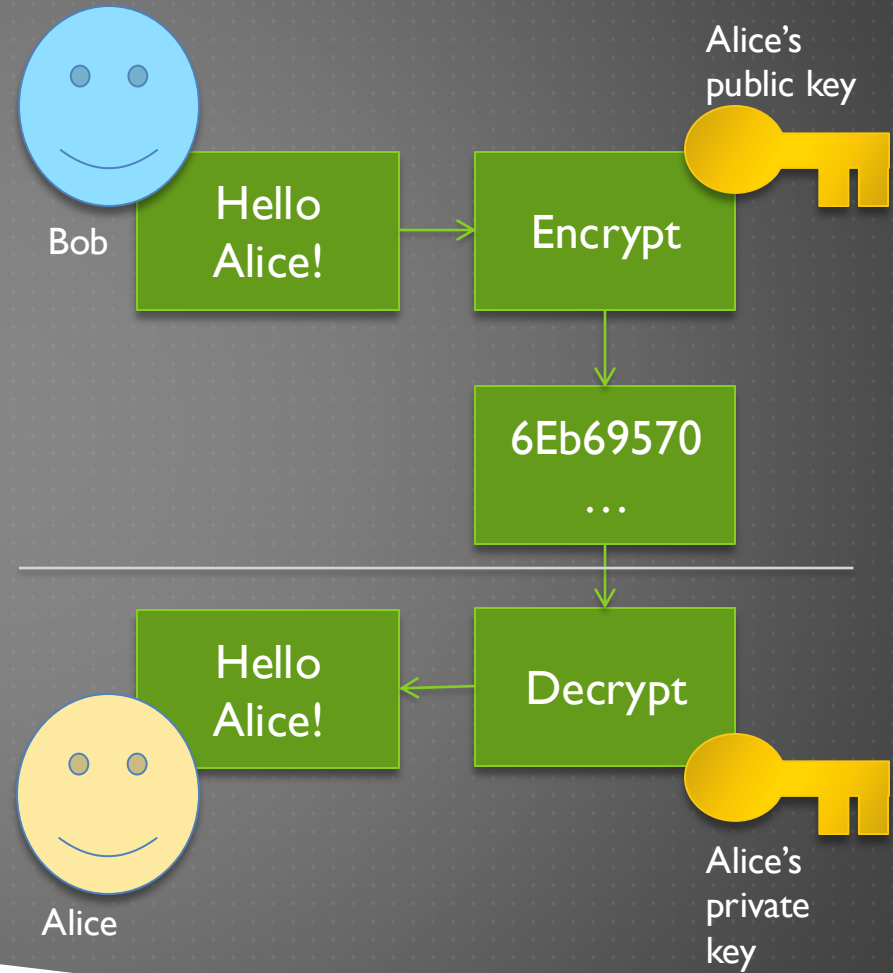
VISUAL COMPUTING ASSESSMENT:

- Coursework:
 - Webcam object / pose recognition.
 - WebGL game.
- Examination:
 - Matrix transformations.
 - Applying image enhancement techniques.
 - Visualization best-practice.



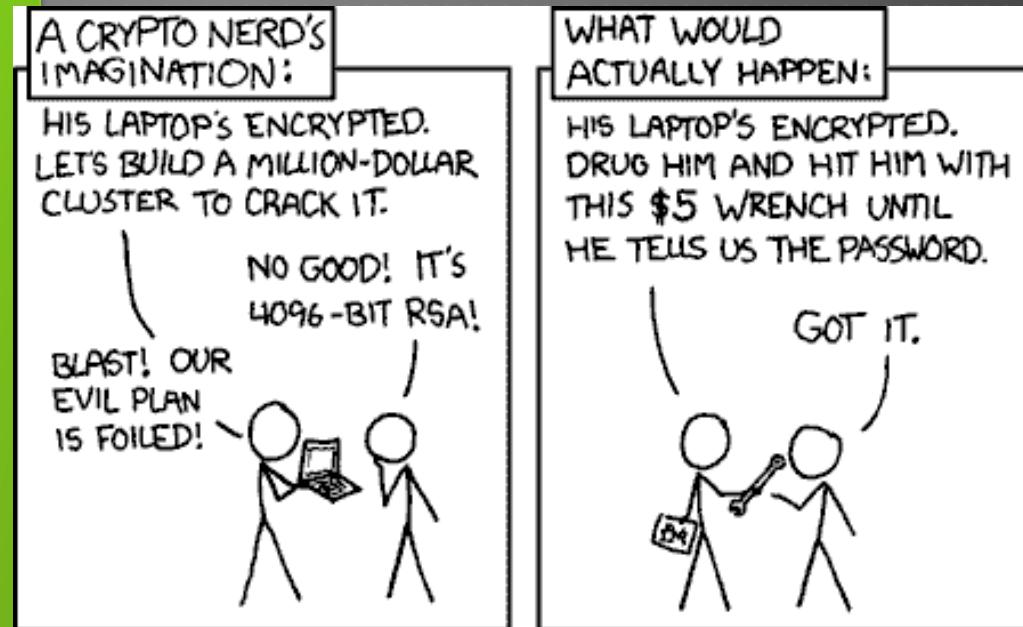
INFORMATION SECURITY COURSE MATERIAL:

- Security essentials (CIA)
 - Confidentiality, Integrity, Availability.
- Authentication
 - Passwords, hashing, salting
- Malware
 - Sandbox experimentation
- Networking
 - TCP/IP and UDP
- Cryptography
 - Public/private key encryption
- Secure programming
 - Code injection attacks



INFORMATION SECURITY ASSESSMENT:

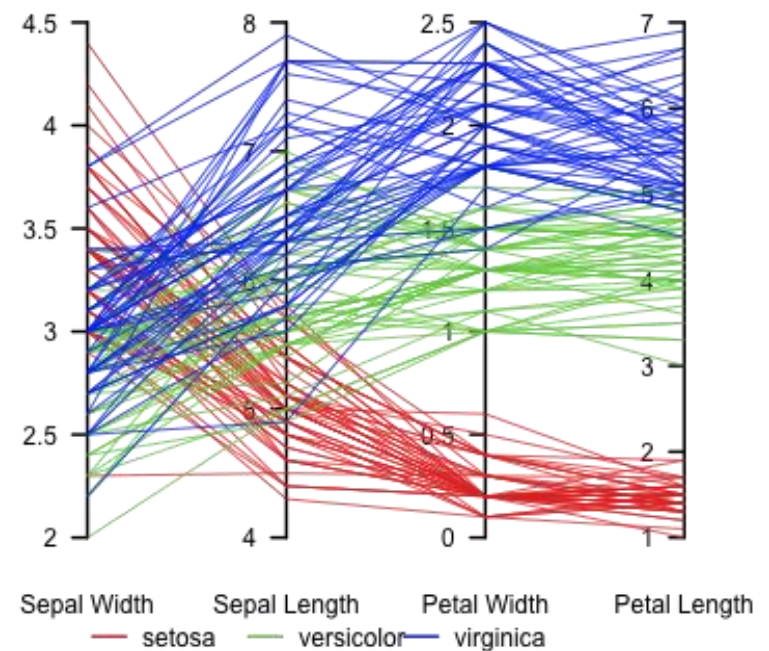
- Coursework:
 - Implementation of encryption and decryption techniques.
 - Malware analysis (within sandbox environment).
 - Penetration testing exercise.
- Examination:
 - Cryptography techniques.
 - How to maintain CIA in business context?
 - Preventing social engineering attacks?



DATA ANALYTICS COURSE MATERIAL:

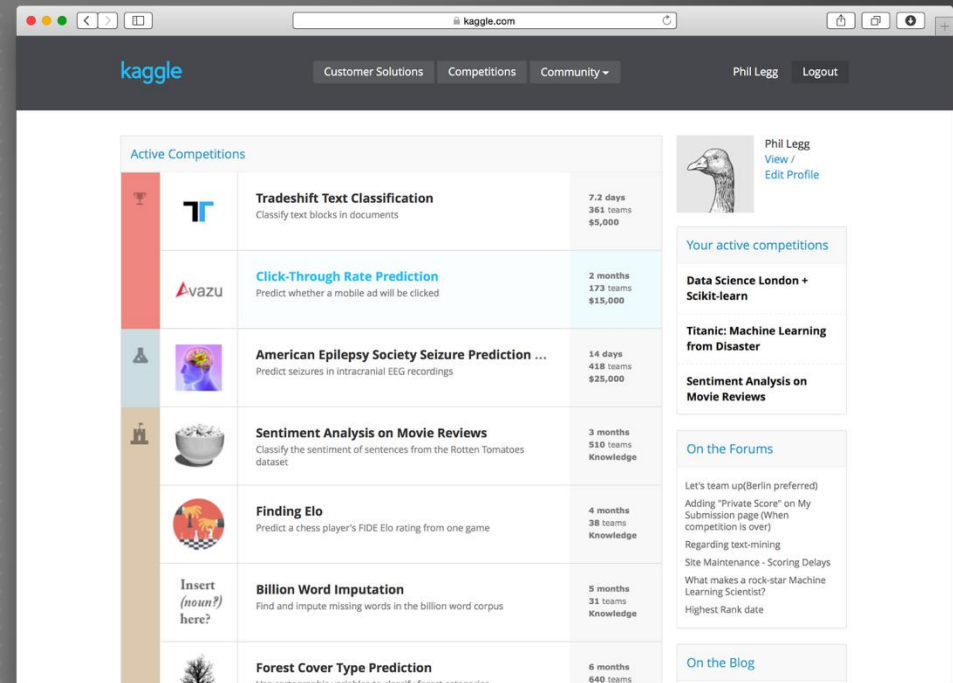
- Foundations of data analytics.
- Data mining.
- Multi-variate data analysis.
- Statistical analysis.
- Classification and clustering.
- Supervised and Unsupervised learning.
- Semi-supervised and Active learning.
- Precision and recall.

Parallel coordinate plot, Fisher's Iris data



DATA ANALYTICS ASSESSMENT:

- Coursework:
 - “Kaggle”-based exercises for large data analytics.
 - Use of machine learning and visualization for data exploration.
- Examination:
 - How can we make sense of data using visualization?
 - How can we improve machine learning using visualization?



INFORMATION SECURITY

MACHINE LEARNING

DATA VISUALIZATION

MALWARE ANALYSIS

VISUAL ANALYTICS

MOBILE SOFTWARE DEVELOPMENT

COMPUTER GRAPHICS

HUMAN-COMPUTER INTERACTION

IMAGE PROCESSING

MOBILE APPLICATION DEVELOPMENT COURSE MATERIAL:

- Fundamentals of mobile device development
- iPhone and Objective-C
- Android Development Toolkit
- Web-based development (Python / Flask / Javascript)
- Games development (Cocoas2d, Box2d)
- Mobile sensors (GPS / accel. / camera)

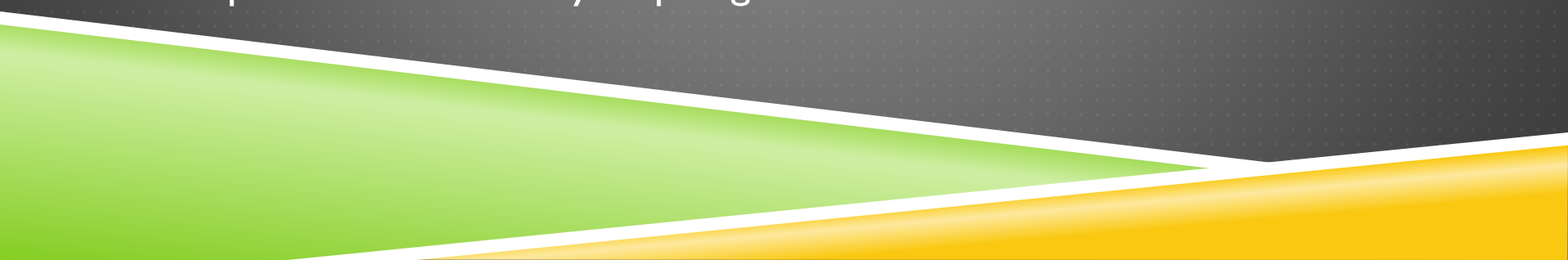


MOBILE APPLICATION DEVELOPMENT ASSESSMENT:

- Coursework:
 - Design a mobile application that makes use of at least two mobile-specific sensors (e.g., location, accelerometer).
- Examination:
 - Considerations of software development for mobile platforms?



CONCLUSION

- ▶ A brief overview of my research interests to date.
 - ▶ Discussion of how my research activities could contribute towards the final year undergraduate degree:
 - ▶ Visual Computing
 - ▶ Information Security
 - ▶ Data Analytics
 - ▶ Mobile Application Development
 - ▶ Discussion of topics that could be incorporated for each course, along with possible coursework and examination areas.
 - ▶ Keen to deliver stimulating courses that would inspire undergraduates to pursue further study to postgraduate level.
- 

Thank you
for listening.

Dr. Phil Legg

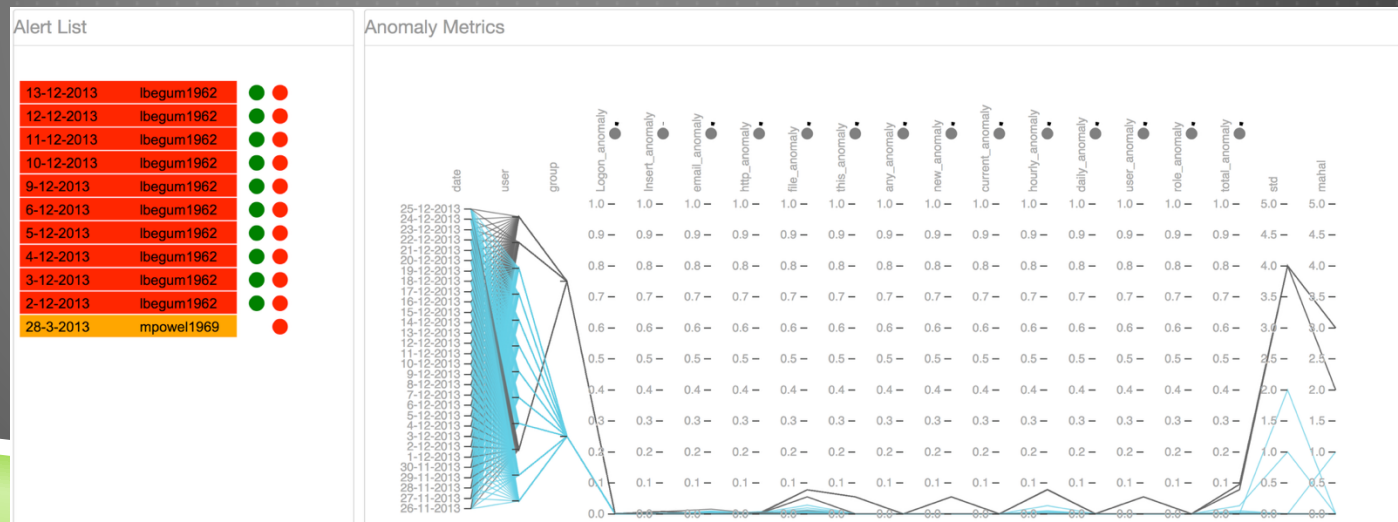
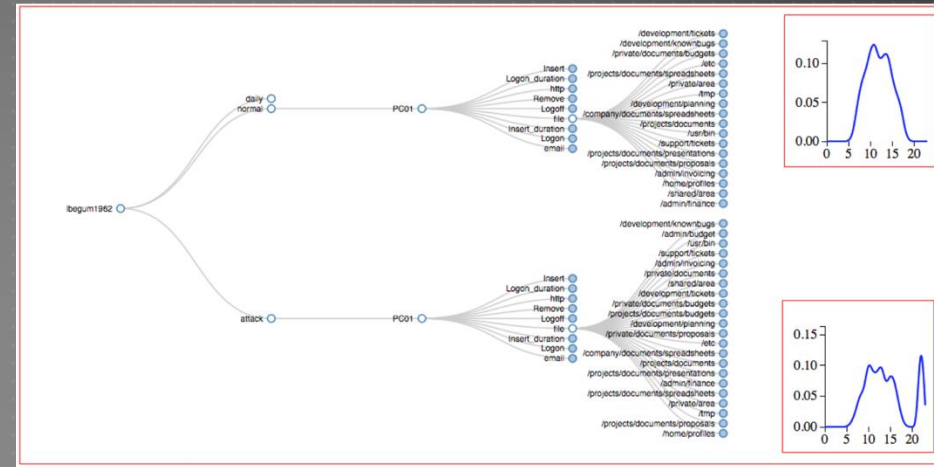
email@plegg.me.uk

Appendix

EXAMPLES OF PREVIOUS WORK

INSIDER THREAT DETECTION

- Can we identify anomalous behaviour from large employee records?
- Can we relate anomalous behaviour to threatening behaviour?



SPORTS VIDEO VISUALIZATION

Rugby (Welsh Rugby Union)

- ▶ Glyph-based Visualization

Snooker (Terry Griffiths)

- ▶ 3D Scene Reconstruction
- ▶ Event Visualization



RUGBY EVENT CLASSIFICATION

- ▶ Notational analysis generates mass of 'training' data.
- ▶ PHOW features (dense SIFT) extracted from video frames.
- ▶ SVM used to generate classifications (lineout, scrum, ruck, maul, none).



*Work conducted in collaboration with
Jelena Mojasevic and
Prof. Dave Marshall (Cardiff)*

SPORTS STATISTICAL ANALYSIS

- ▶ Football premier league (Opta) data mining.
- ▶ Can we identify interesting patterns in this large dataset?
 - ▶ Player contributions to game.
 - ▶ Winning/losing trends.
- ▶ Weka analysis software
 - ▶ Machine Learning toolkit

Work conducted in collaboration with
Alex Thomas (MPhil Student, Swansea)



Input parameters determine a numerical 'impact' value that each player has had on the match.
Could define a set of rules from this learnt data to characterize player performance over a full season.

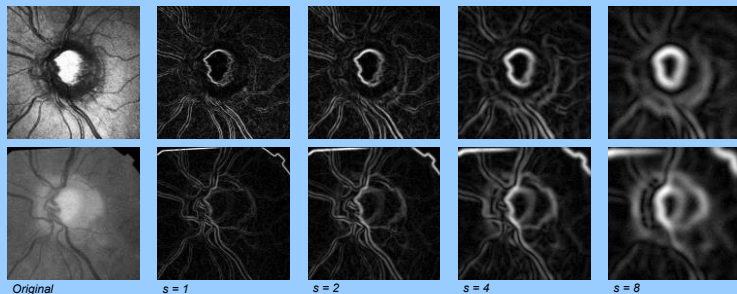
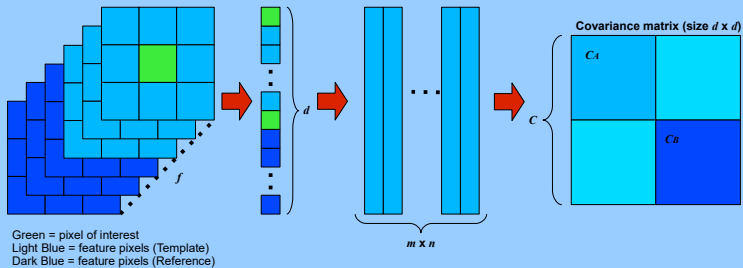
MULTI-MODAL RETINAL IMAGING

Feature Neighbourhood Mutual Information

- We aim to find the rigid registration that can successfully align the floating image (SLO) to the reference image (fundus).
- Simplex algorithm used to search for correct translation and rotation parameters.
- Multi-resolution pyramid used to improve search time using coarse-to-fine approach.
 - Rotation range between ± 3 degrees at coarse level – restricted at each lower level.
 - Result at each level acts as initialization for next level down in pyramid.

At each possible transformation:

- For each pixel within the registration area, we create a vector consisting of the pixel and its 8 neighbours for the original image and the feature images for both modalities.
- The collection of vectors makes up a matrix that represents the current registration.
- This matrix is reduced to a covariance matrix to show the relation between elements.
- FNMI can then be defined as: $\text{entropy}(C_A) + \text{entropy}(C_B) - \text{entropy}(C)$

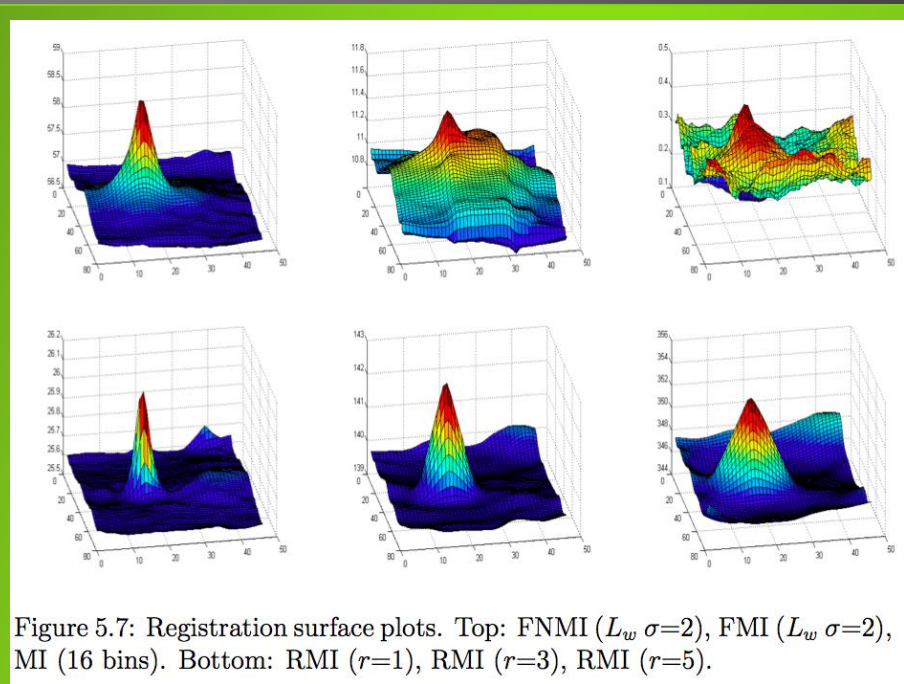


Template image and its corresponding region in reference image, along with feature images taken at multiple scales.

- Study of the Mutual Information registration algorithm.
- Proposed an improved similarity measure, “Feature Neighbourhood MI”

REGISTRATION OPTIMIZATION

- ▶ Possible transformation space is too large to search brute force.
- ▶ Exploration of how to search transformation space optimally to find registration that maximizes the similarity measure.
 - ▶ Nelder-Mead Simplex algorithm.
 - ▶ Simulated Annealing
 - ▶ Gradient Descent.



A smooth similarity measure can dramatically improve the chances of finding the maximized solution using search optimization...

3D STEREO DISPLAY PRO (SDPRO)

- ▶ Registration of intra-modal images for 3D stereo display.
- ▶ Emphasizes retinal curvature, and blood vessels.
- ▶ Software deployed with University Hospital Wales and NHS.



CHINESE CHECKERS INTELLIGENT OPPONENT

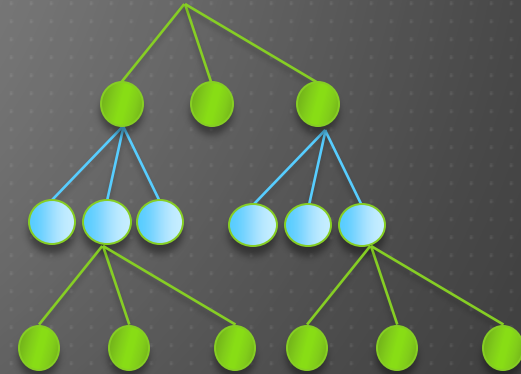
- ▶ Undergraduate Final Year Project.
- ▶ Mini-max algorithm used to determine 'best' move.
- ▶ Tree structure that examines each move and assigns a success weight value (3-ply implementation).
- ▶ Aims to maximize computer success criterion and minimize human success criterion.
- ▶ Alpha-beta pruning disregards poor path results



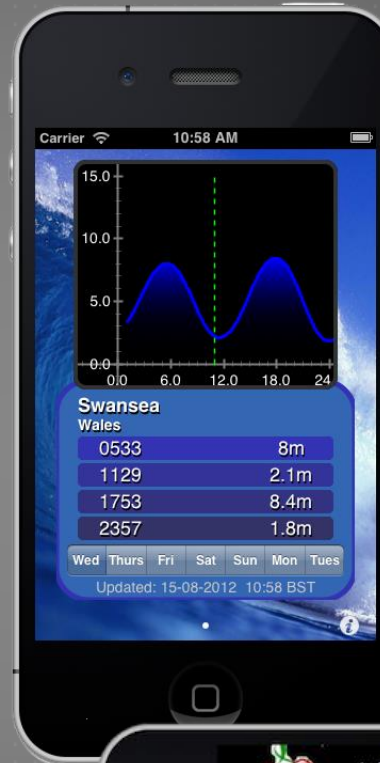
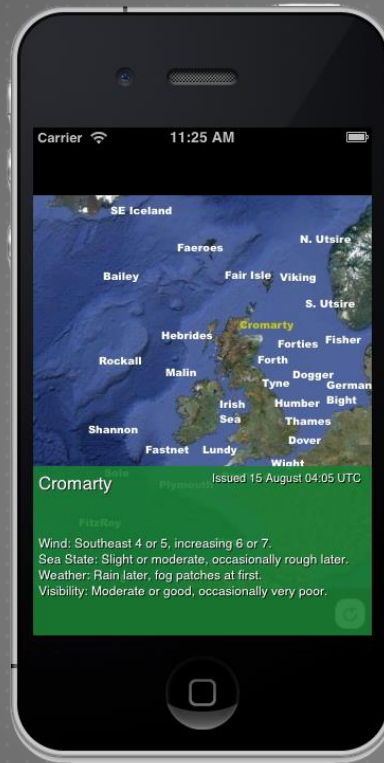
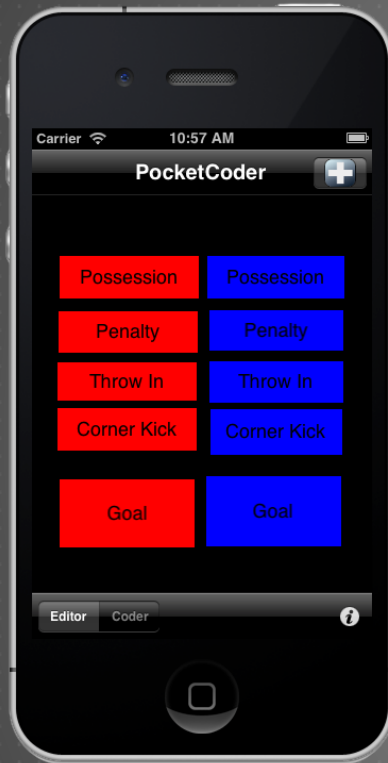
Computer

Human

Computer



MOBILE APP DEVELOPMENT



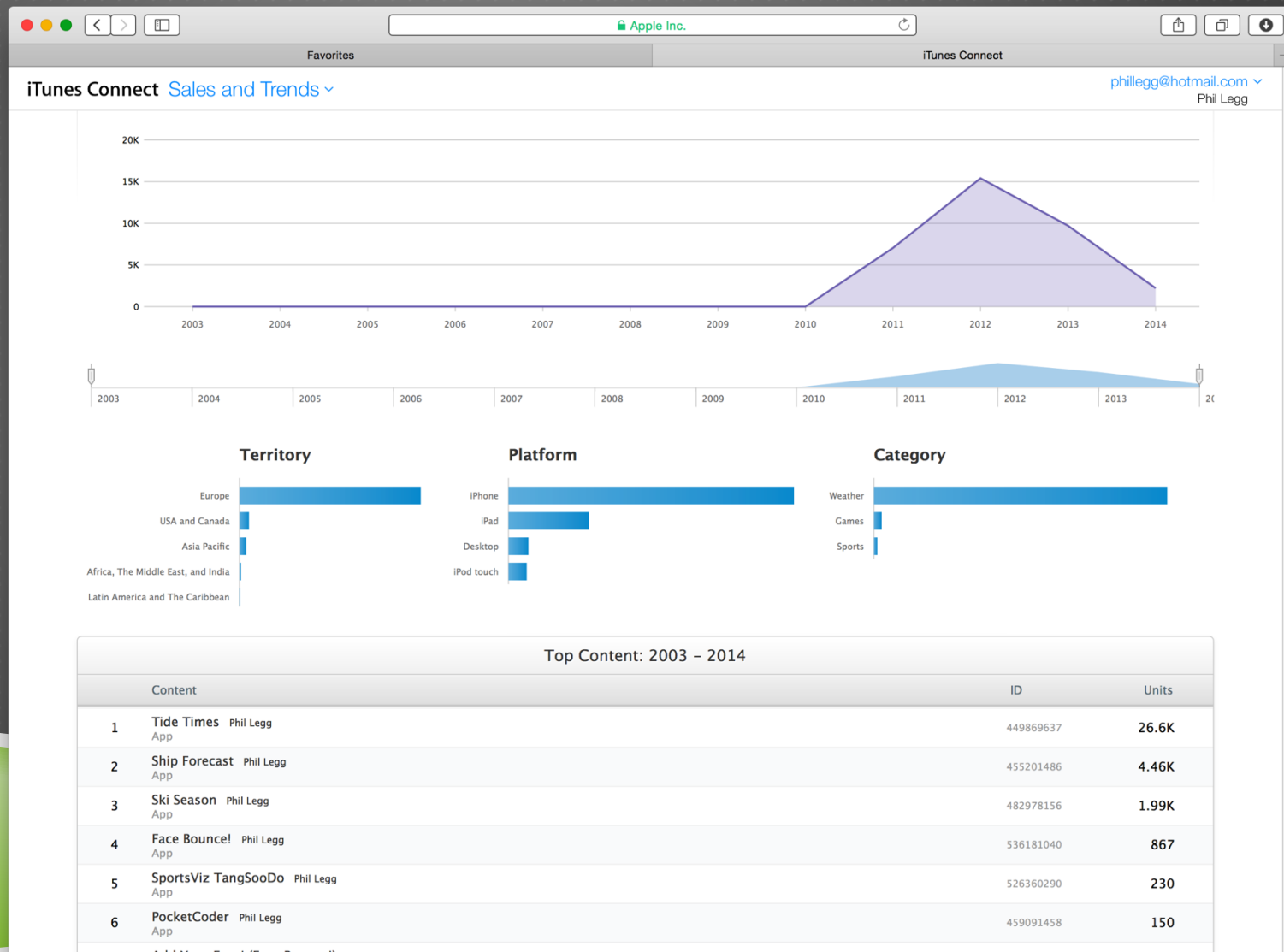
PocketCoder
Ship Forecast
Tide Times
GeoCaption
FaceBounce
MatchPad



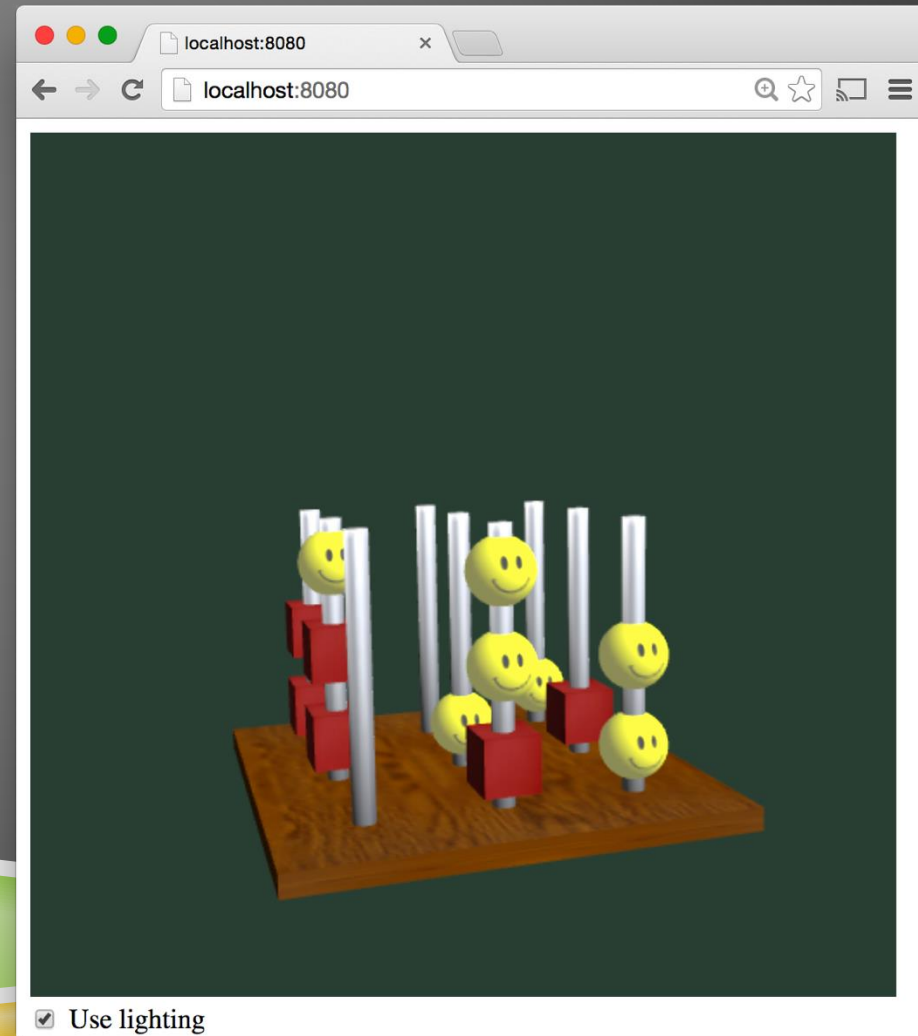
MOBILE APP DEVELOPMENT



IPHONE APP STORE



WEBGL GAME COURSEWORK



PUBLIC KEY ENCRYPTION EXAMPLE

A worked example [\[edit\]](#)

Here is an example of RSA encryption and decryption. The parameters used here are artificially small, but one can also [use OpenSSL to generate and examine a real keypair](#).

1. Choose two distinct prime numbers, such as

$$p = 61 \text{ and } q = 53$$

2. Compute $n = pq$ giving

$$n = 61 \times 53 = 3233$$

3. Compute the [totient](#) of the product as $\phi(n) = (p - 1)(q - 1)$ giving

$$\phi(3233) = (61 - 1)(53 - 1) = 3120$$

4. Choose any number $1 < e < 3120$ that is [coprime](#) to 3120. Choosing a prime number for e leaves us only to check that e is not a divisor of 3120.

$$\text{Let } e = 17$$

5. Compute d , the [modular multiplicative inverse](#) of $e \pmod{\phi(n)}$ yielding,

$$d = 2753$$

Worked example for the modular multiplicative inverse:

$$e \times d \pmod{\phi(n)} = 1$$

$$17 \times 2753 \pmod{3120} = 1$$

The **public key** is $(n = 3233, e = 17)$. For a padded [plaintext](#) message m , the encryption function is

$$c(m) = m^{17} \pmod{3233}$$

The **private key** is $(n = 3233, d = 2753)$. For an encrypted [ciphertext](#) c , the decryption function is

$$m(c) = c^{2753} \pmod{3233}$$

For instance, in order to encrypt $m = 65$, we calculate

$$c = 65^{17} \pmod{3233} = 2790$$

To decrypt $c = 2790$, we calculate

$$m = 2790^{2753} \pmod{3233} = 65$$