The sixth EWU-IPU International Exchange Program In Computer Science 2013

Informatics Society

Sponsored by Informatics Society

Publication Office
Informatics Laboratory
3-41, Tsujimachi, Kitaku, Nagoya 462-0032, Japan

Publisher
Tadanori Mizuno, President of Informatics Society

ISBN: 978-4-902523-36-2

General Co-Chairs:

Paul Schimpf, Eastern Washington University

Yoshitaka Shibata, Iwate Prefectural University

Program Co-Chairs:

Carol Taylor, Eastern Washington University

Kosuke Imamura, Eastern Washington University

Yuko Murayama, Iwate Prefectural University

Program Committee:

Paul Schimpf, Eastern Washington University

Yoshitaka Shibata,, Iwate Prefectural University

Masakatsu Nishigakki, Shizuoka University

Yoshia Saito, Iwate Prefectural University

Yoshikazu Watanabe, Iwate Prefectural University

Local Chair:

Catherine Dixon, Eastern Washington University

Local Supporters:

Geancarlo Palavicini, MS Student, Eastern Washington University

Kyle Gwinnup, MS Student, Eastern Washington University

Publishing Chair:

Yoshia Saito, Iwate Prefectural University

Web Chair:

James Lamphere, Eastern Washington University

Contents

Preface

It is our great pleasure to have the sixth workshop of the Eastern Washington University (EWU)- Iwate Prefectural University (IPU) International Exchange Program in Computer Science published by the Informatics Society. The exchange program started in the summer of 2008 after an administrative meeting the previous year. Since then, the workshop has been held every year.

This year as the sixth workshop, we had the keynote speech by Masakatsu Nishigaki from Shizuoka University, followed by seven presentations by the faculty members and graduate students from Iwate Prefectural University and Eastern Washington University. Those presentations span a wide variety of topics in computer science, networking, security, human aspects of technology and disaster communications

We had three graduate students joined from Iwate, this year, as well as two more students from Shizuoka University We hope that the workshop is a good basis for more participants in this international research exchange program and leads to further research collaboration.

Finally, but not least, we appreciate the Informatics Society for publishing the proceedings from this summer workshop.

July 2014

General Co-Chairs: Yoshitaka Shibata and Paul Schimpf
Program Co-Chairs:Carol Taylor, Kosuke Imamura and Yuko Murayama

2013/08/29 6th EWU-IPU Workshop

Humanics security and Entertainment security

Masakatsu NISHIGAKI
Shizuoka University
nisigaki@inf.shizuoka.ac.jp

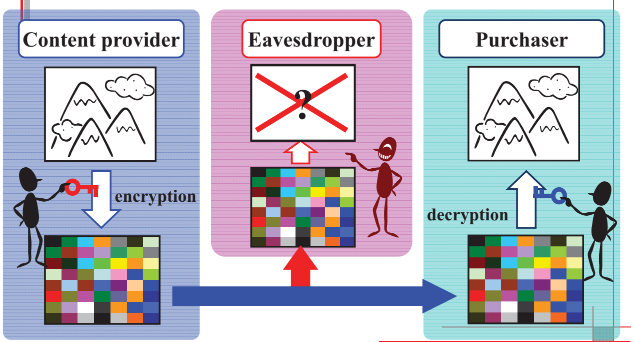
1

Humanics security and Entertainment security

- What is “humanics security”?
- What is “entertainment security”?

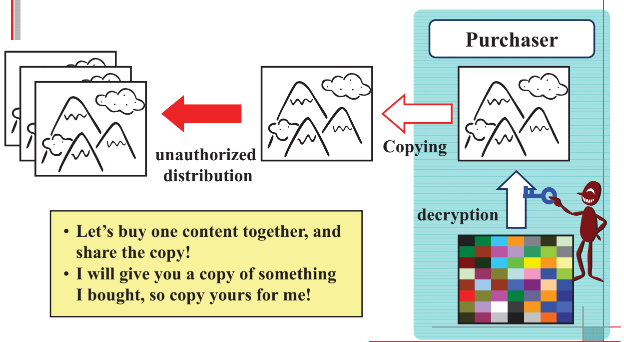
2

Does encryption really work as unauthorized copy prevention?



3

If purchaser is malicious…



4

Humanics Security

- Security techniques alone is not perfect.
- System security is achieved by managing security techniques properly.
- Who uses the system? Human beings!!
- Who attacks the system? Human beings!!

In addition

Humanics security

System security

Managing Security Techniques properly

with consideration of User Characteristics

5

Security with human aspects

Ex: If a digital data was just like your wife, …

You won’t copy it for anyone

This sweetheart is only mine

No unauthorized copy!

Ex: If authentication was your hobby, …

You love to punch your password.

Let me punch password again

Usability is not degraded!

6

ISBN978-4-902523-36-2

Humanics security and Entertainment security

- What is “humanics security”?
  - Security enhancement that is achieved by combining security technology and human aspects.
- What is “entertainment security”?
  - Subset of Humanics security in which entertainment aspect is focused on.

7

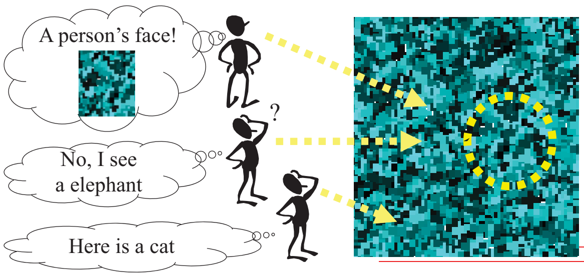
User Authentication using Unclear images

A combination of security and human cognitive aspect

8

Gestalt’s law

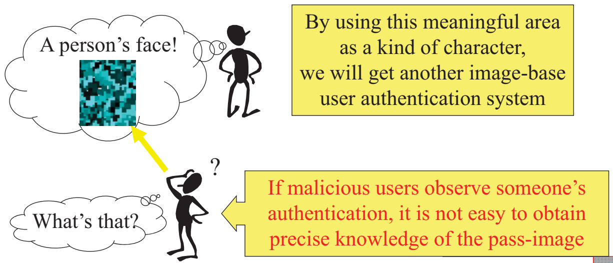
- A user can see some meanings even in random-dot image
- It is difficult for the other users to find the same areas and meanings



9

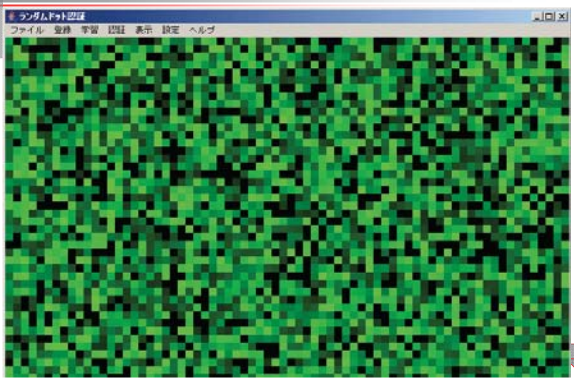
Gestalt’s law

- A user can see some meanings even in random-dot image
- It is difficult for the other users to find the same areas and meanings



10

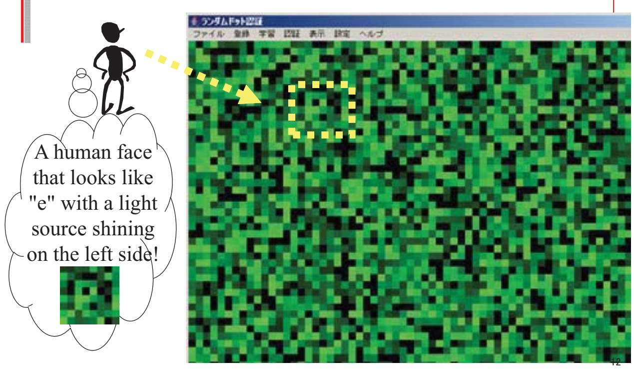
we made something like this!



11

Enrollment phase

1. Choose a meaningful area as pass-image

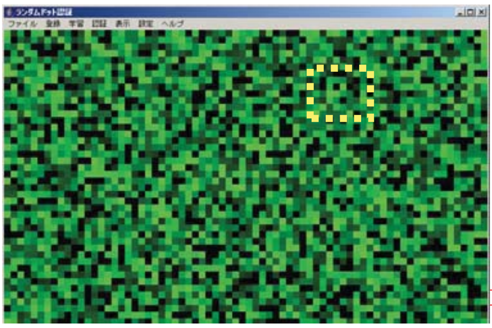


12

Authentication phase

Nish!gaki Laboratory

1. System shows new random dots with the pass-image some where
2. User is required to find the "pass-image" in a short time



13

One more idea

Nish!gaki Laboratory

Random dots authentication

- What users do is just watch-and-click
- If cracker observes, it is not easy to obtain precise knowledge of the pass-image

Finding a meaningful area in random dots is very difficult even for the legitimate user

14

One more idea

Nish!gaki Laboratory

unclear image

- User does not understand what it is

unclear image + the original image

- User can easily remember the unclear images using the original image as a clue

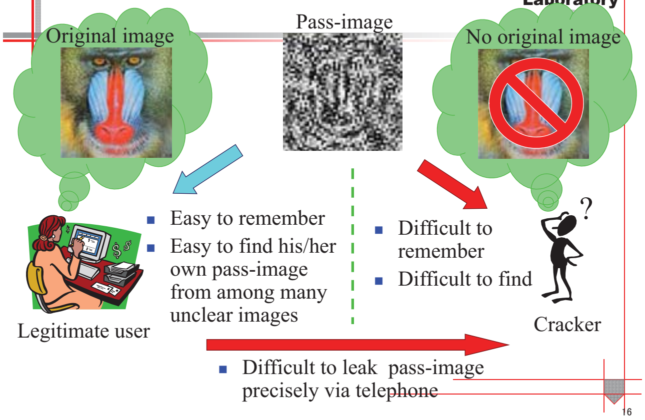
Use as a clue

- Monotoning
- Mosaicing
- Adding noize

15

Unclear image-based authentication

Nish!gaki Laboratory



16

Nish!gaki Laboratory

Biometric User Authentication using human reflex

A combination of security and human neuro-biological aspect

17

Background (1/4)

Nish!gaki Laboratory

User authentication method

- Authentication by human memory
  Password
- Authentication by possession
  Token, IC card
- **Authentication by physical characteristic (biometric authentication)**
  Fingerprint, iris pattern

Emphasis on biometric authentication that does not require remembering password and has no danger of loss of token

18

18

Background (2/4)

However,

Biometric information tends to leak easily

- Fingerprints → residual fingerprints
  - A rubber (gummy) false fingers made from residual fingerprints could pass through a fingerprint authentication devices.
- Iris pattern → photograph
  - Photographs of iris patterns attached to spectacles could pass through a iris authentication devices.
- Etc…

19

19

Background (3/4)

To overcome the problem:

- Authentication using biometric information that does not leak easily
  - Vein patterns on palm or finger
    - Leakage from authentication server
    - Fraudulent extraction of biometric information
    - Phishing of biometric information
- Authentication using behavioural biometric information
  - Hand-written signature
    - Mastery by practice

20

Background (4/4)

Biometric authentication

- which cannot be abused, even if biometric information is leaked
- which cannot be mastered by practice

is required,
particularly with authentication used when accessing highly confidential information

⇒ **Proposal of authentication method utilising human reflexes**

21

21

Reflexes

When a sensory organ is stimulated, a response is induced in muscles or other parts of the body, regardless of consciousness

- In our study, we take a slightly broader interpretation of reflexes as responses at a level that cannot be controlled.

  Examples:
  - Light reflexes (pupil contraction and dilation)
  - Blinking
  - Knee-jerk reflex (utilised when testing for beriberi)
  - Etc…

22

22

Utilisation of reflexes

1st type of utilisation:
When there are differences in a certain reflex between individual people, that reflex itself can be utilised in authentication

2nd type of utilisation:
Even when there are not sufficient differences in a certain reflex between individual people, it can be combined with physiological biometric information that differ between individual people, to enable its use in authentication

23

23

Even when there are not sufficient differences in a reflex between people...

2nd type of biometric reflex authentication

Biometric information | Biometric reflex

(Extract differences in reflexes between individual people indirectly, by submitting "stimuli that induce human reflexes" to "areas in which physiological biometric information have differences between people")

Reflex is used
not only for liveness detection (if he/she lives),
but also for distinction of user (who he/she is)

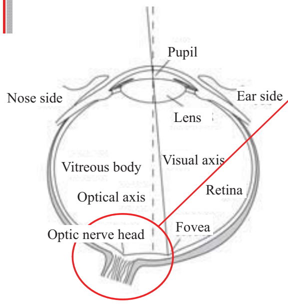
Biometric information (biometric authentication) + Biometric reflex (liveness detection)

24

24

Blind Spot

Nish!gaki Laboratory



There are no photoreceptor cells here that can sense light

When seen from a distance of 1 m, the area of the blind spot is a circle of diameter of about 10 cm

Even when human sees something with one eye, the eyesight information at the blind spot is compensated for within the brain by extracting images from the eyesight information around the blind spot, so humans do not usually notice the blind spot

25

25

Saccades (Jerky Eyeball Movements)

Nish!gaki Laboratory

- Rapid and jerkily eyeball motions induced when the point-of-gaze is directed towards an objective stimulus (target)
- There is a latent time of 100 ms to 500 ms from appearance of the target in the peripheral part of vision until the onset of saccades

26

26

Saccades (Jerky Eyeball Movements)

Nish!gaki Laboratory

1st type of Reflex Authentication can not be realised

There are some differences in saccade response time between individual people, but there are also large variations in saccade response time for each individual person, so it is basically not considered possible to utilise saccade response time alone in authentication.

We try to implement 2nd type of Reflex Authentication

Position of blind spot ⇨ **Biometric information**

Saccades ⇨ **Reflexes**

27

Authentication method

Nish!gaki Laboratory

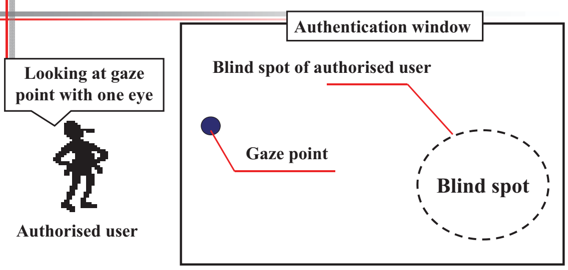
1. Authentication with one eye, to utilise the blind spot in authentication
2. Target (objective stimulus) is displayed in authentication window
3. The user immediately looks at the target as soon as the user notices the target displayed
4. System measures the saccade response time, and authentication is done based on the saccade response time

28

28

Authentication procedures

Nish!gaki Laboratory

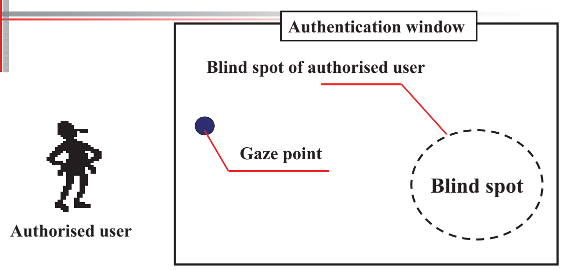


1. The user is instructed to always look at the gaze point with one eye.
   - The broken line is the blind spot when the user is looking at the gaze point (measured previously during enrolment).
   - The user is instructed to move his eye towards a target as soon as it appears within his field of view.

29

Authentication procedures

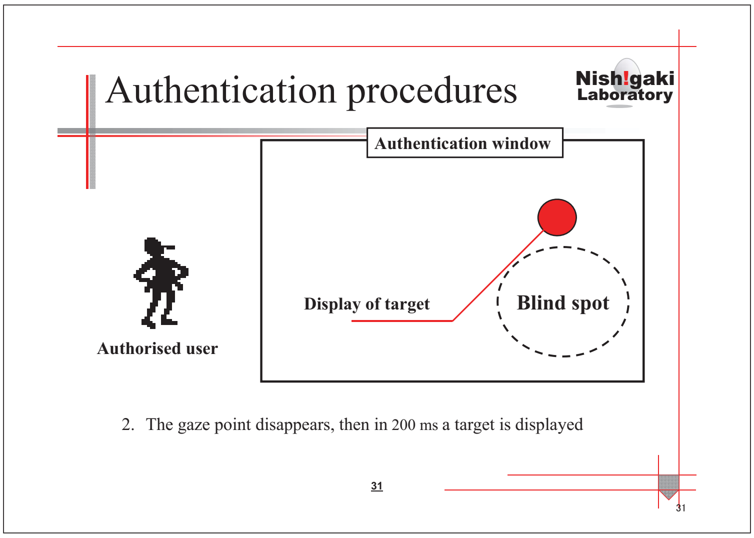
Nish!gaki Laboratory

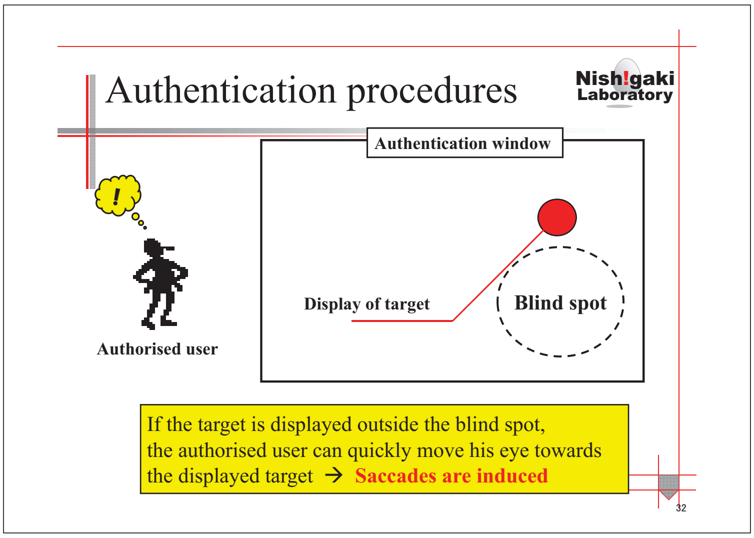


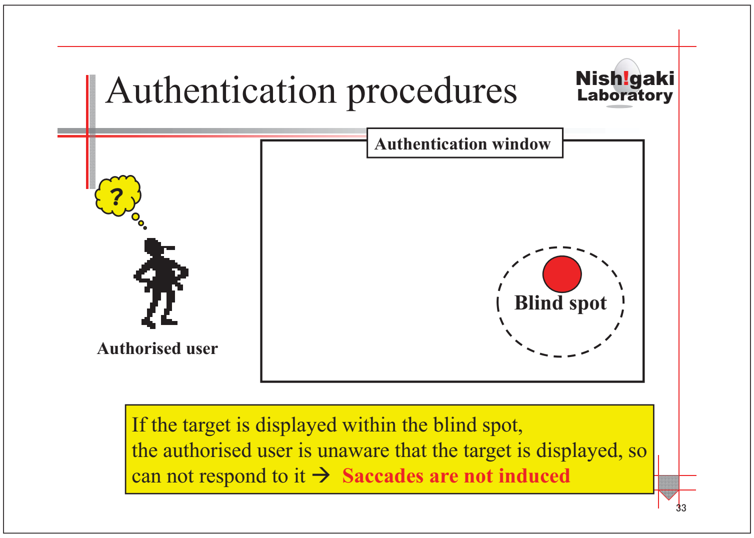
2. The gaze point disappears, then in 200 ms a target is displayed

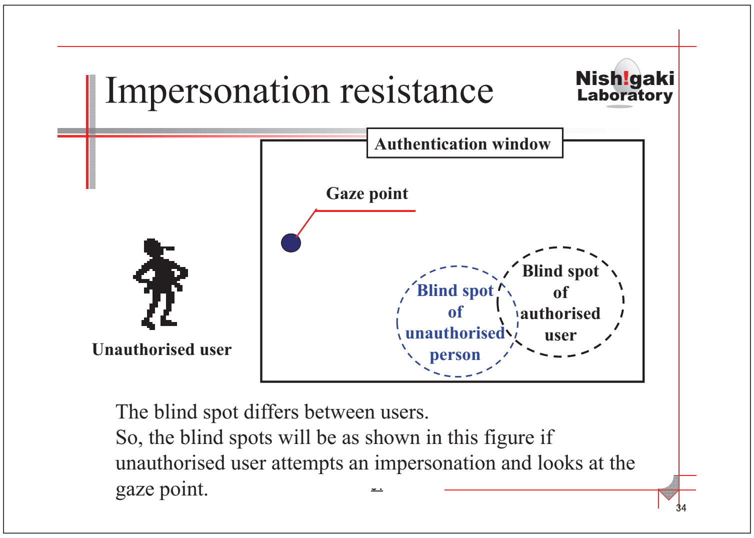
30

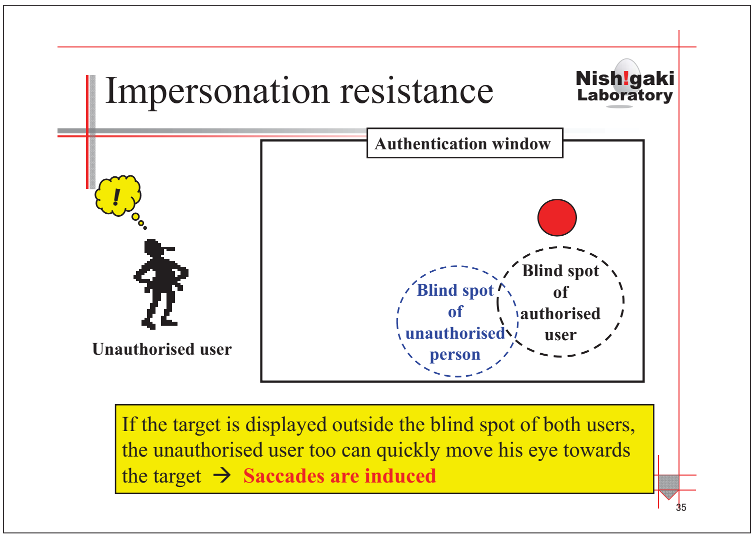
30

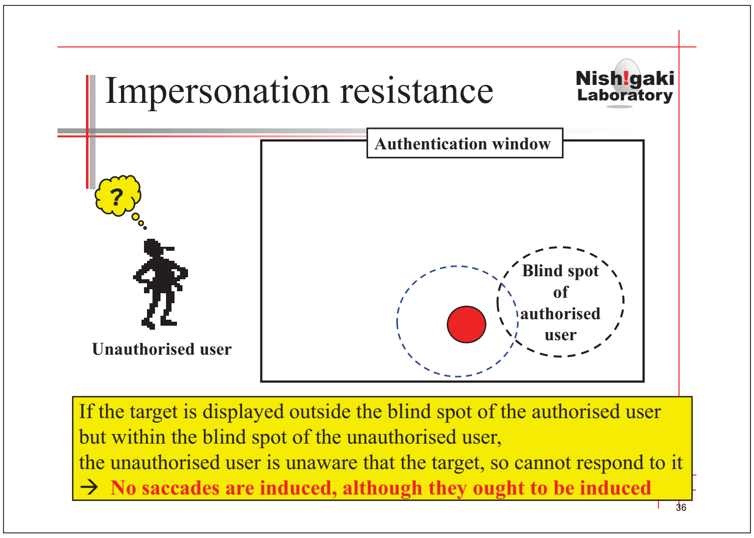

Authentication procedures
Nish!gaki Laboratory
Authentication window
Display of target
Blind spot
Authorised user
2. The gaze point disappears, then in 200 ms a target is displayed
31
31


Authentication procedures
Nish!gaki Laboratory
Authentication window
!
Display of target
Blind spot
Authorised user
If the target is displayed outside the blind spot,
the authorised user can quickly move his eye towards
the displayed target → Saccades are induced
32


Authentication procedures
Nish!gaki Laboratory
Authentication window
?
Blind spot
Authorised user
If the target is displayed within the blind spot,
the authorised user is unaware that the target is displayed, so
can not respond to it → Saccades are not induced
33

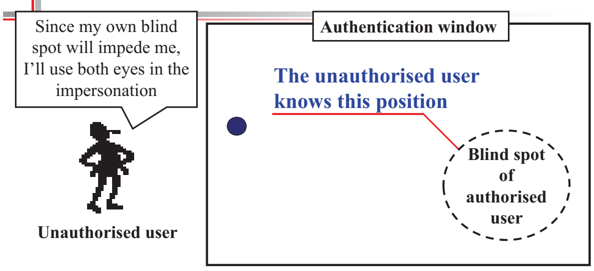

Impersonation resistance
Nish!gaki Laboratory
Authentication window
Gaze point
Blind spot of unauthorised person
Blind spot of authorised user
Unauthorised user
The blind spot differs between users.
So, the blind spots will be as shown in this figure if
unauthorised user attempts an impersonation and looks at the
gaze point.
34


Impersonation resistance
Nish!gaki Laboratory
Authentication window
!
Blind spot of unauthorised person
Blind spot of authorised user
Unauthorised user
If the target is displayed outside the blind spot of both users,
the unauthorised user too can quickly move his eye towards
the target → Saccades are induced
35


Impersonation resistance
Nish!gaki Laboratory
Authentication window
?
Blind spot of authorised user
Unauthorised user
If the target is displayed outside the blind spot of the authorised user
but within the blind spot of the unauthorised user,
the unauthorised user is unaware that the target, so cannot respond to it
→ No saccades are induced, although they ought to be induced
36

Resistance to Active Impersonation

Nish!gaki Laboratory

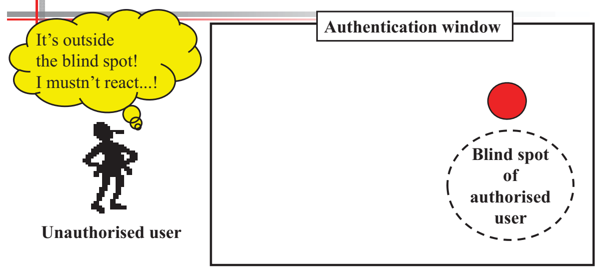


The active unauthorised user:
- Uses both eyes in the impersonation
- learns beforehand the range of the blind spot of the authorised user
- Practices beforehand to ensure his eyes move only when the target is displayed outside the blind spot of the authorised user

37

Resistance to Active Impersonation

Nish!gaki Laboratory

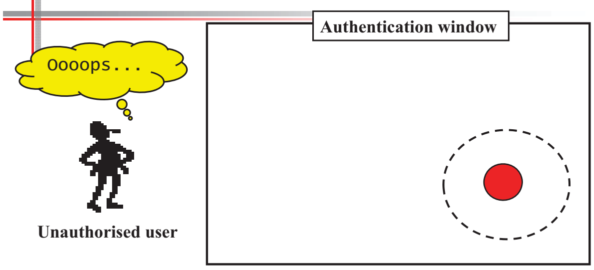


When the target is displayed outside the blind spot of the authorised user, the unauthorised user can quickly move his eye towards the target → **However, the response time is delayed**

38

Resistance to Active Impersonation

Nish!gaki Laboratory



When the target is displayed within the blind spot of the authorised user…
→ **The unauthorised user could be bound to move his eyes towards the target by mistake**

39

Conclusions

Nish!gaki Laboratory

Humanics Security

- Security techniques
  +
- Management
  +
- Human aspects
  - Entertainment

Enterteinment Security

40

Conclusions

Nish!gaki Laboratory

- User authentication using unclear images
- Biometric user authentication using human replex

41

A Concept of Emotion Sharing for Human-friendly Automobile Society

Yoshia Saito, Yuki Nakano, Dai Nishioka and Yuko Murayama

Iwate Prefectural University, Japan

Background

- **Automobiles are essential tools**
  - Automobiles in Japan: 76,000,000
  - Automobiles in World: 1,000,000,000
- **Danger to Human**
  - Road accidents: 660,000
  - Death:4,400
  - Injured: 8,200,000

Toward human-friendly automobile society

1

Limit of mechanical approaches

- **Mechanical approaches**
  - Electronic Stability Control (ESC)
  - Antilock Brake System (ABS)
  - Driving Safety Support Systems (DSSS)
  - Advanced Driver Assistance Systems (ADAS)
- **Road accidents decreased**
  - From 950,000 to 660,000 in Japan in this decade
  - However, the decrease ratio declines…

2

Applying human approaches

- **Emotion affects performance of drivers**
  - **Road rage:** angry behaviors by drivers causing fatal and injury accidents
- **8 basic and 8 advanced emotions [Plutchik2001]**
  - **Basic:** Joy, Trust, Fear, Surprise, Sadness, Disgust, Anger, Anticipation
  - **Advanced:** Optimism, Love, Submission, Awe, Disappointment, Remorse, Contempt, Aggressiveness

Robert Plutchik: The nature of emotions, American Scientist, pp.344–350 (2001).

3

Related work

How to detect the emotion of the drivers

How to affect and utilize the emotion of the drivers

4

How to detect

- **Sensing driver's emotion**
  - Speech [Jones2005]
  - Heart rate variability [Riener2009]
  - Brain signals [Haak2010]
  - Face surface temperature [Anzengruber2012]

Christian Martyn Jones and Ing-Marie Jonsson: Automatic recognition of affective cues in the affective cues in the speech of car drivers to allow appropriate responses, OZCHI'2005, pp. 1-10 (2005).

Andreas Riener, Alois Ferscha and Mohamed Aly: Heart on the road: HRV analysis for monitoring a driver's affective state, AutomotiveUI'09, pp. 99-106 (2009).

Paul van den Haak, Rinde van Lon, Jaap van der Meer and Léon Rothkrantz: Stress assessment of car-drivers using EEG-analysis, CompSysTech'10, pp. 473-477 (2010).

Bernhard Anzengruber and Andreas Riener: "FaceLight" – Potentials and Drawbacks of Thermal Imaging to Infer Driver Stress, AutomotiveUI'12, pp. 210-216 (2012).

5

ISBN978-4-902523-36-2

How to affect and utilize

- **Effect of matched emotion [Clifford2005]**
  – If driver’s emotion matched car voice emotion, drivers had fewer accidents
  – Happy/energetic and upset/subdued
- **Difference of angry and fearful drivers [Jeon2011]**
  – Angry drivers showed more errors than fearful drivers
  – Fearful state showed numerically higher workload than those in the angry state

Clifford Nass, Ing-Marie Jonsson, Helen Harris, Ben Reaves, Jack Endo, Scott Brave and Leila Takayama: Improving Automotive Safety by Pairing Driver Emotion and Car Voice Emotion, CHI’05, pp. 1973-1976 (2005).

Myounghoon Jeon, Jung-Bin Yim and Bruce N. Walker: An Angry Driver Is Not the Same As a Fearful Driver: Effects of Specific Negative Emotions on Risk Perception, Driving Performance, and Workload, AutomotiveUI’11, pp. 137-140 (2011).

Research challenge

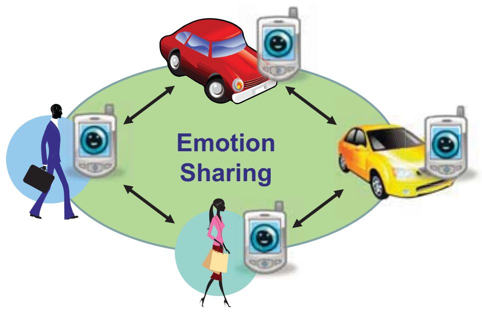
How to affect and utilize
the emotions of the other people

Our hypothesis

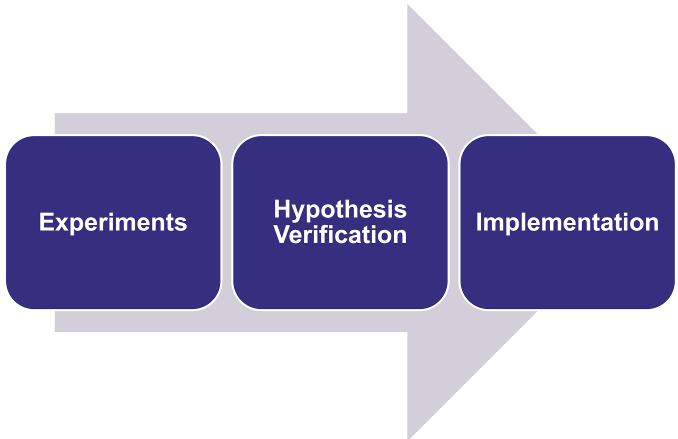
Sharing of emotion enables drivers and pedestrians to take friendly and safe actions if appropriate emotions are shared in appropriate situations

Proposed scheme

- **Emotions are shared by smart devices using emoticon and some other ways**
  – Drivers and pedestrians can select and share emotions
  – Neighboring drivers and pedestrians can receive it



Research plan



Driving simulator

Simulation scenarios

- **Joy Sharing scenario**
  – whether people drive a car friendly when sharing joy emotion among drivers and pedestrians
- **Fear sharing scenario**
  – whether people drive a car avoiding risk when sharing fear emotion among drivers and pedestrians

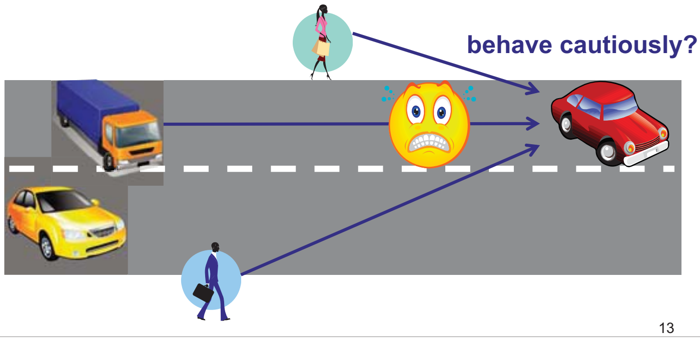
Joy sharing scenario

- A pedestrian thanks a driver sending joy emoticon when stopping at a crosswalk
- We observe whether it makes the driver to stop at the next crosswalk for other pedestrians

12

Fear sharing scenario

- Pedestrians/drivers see an aggressive automobile and send a fear emoticon circumferentially
- We observe whether it makes other people to behave cautiously to avoid the risk



13

Next steps

- **Prepare the two simulation scenarios**
- **Conduct experiments**
- **Analyze the results and verify our hypothesis**
- **Implement an emotion sharing application for drivers and pedestrians on smart devices**

14

Conclusion

- **An emotion sharing scheme for human-friendly automobile society**
  - Applying human approaches to decrease road accidents
- **Two scenarios**
  - Joy sharing scenario
  - Fear sharing scenario
- **Future work**
  - Experiments and implementation

15

PictCast: Interactive Internet Broadcasting with Better Picture Quality based on Audience Satisfaction

Yuki Nakano*, Yoshia Saito** and Yuko Murayama**

*Graduate School of Software and Information Science, Iwate Prefectural University, Japan
y.nakano@comm.soft.iwate-pu.ac.jp
**Faculty of Software and Information Science, Iwate Prefectural University, Japan
{y-saito, murayama}@iwate-pu.ac.jp

Abstract - Live Internet broadcasting services which are available on smartphones are increasing along with the popularization of Internet broadcasting and smartphones. The smartphone users, however, cannot perform Internet broadcasting adequately due to lack of the 3G transmission speed for video streaming in real time. To solve this issue, we propose PictCast, which is a still picture Internet broadcasting system with dynamic picture quality adjustment based on audience requests for smartphone broadcasters. We report an experiment to measure minimum acceptable quality and the percentage of quality improvement requests from the audience.

Keywords: Internet broadcasting, 3G network, smartphones

1 INTRODUCTION

Live internet broadcasting services which are available on smartphones are increasing, along with the popularization of Internet broadcasting and smartphones. Typical services are Bambuser, Qik, Stickam, and Ustream. On these services, 3G Internet connections are required for Internet broadcasting with smartphones in outdoor areas where wireless LAN connections are unavailable. In particular, there are also such environments as rural areas and developing cities. However, the smartphone users cannot perform Internet broadcasting adequately due to lack of the 3G transmission speed for video streaming in real time. Data traffic should be reduced to achieve stable Internet broadcasting via 3G networks without delay. The smartphone users can use LTE to stream live video in real time. However, cell phone carriers often restrict the upload and download speeds of LTE when a after amount of data is transmitted. Data traffic should be reduced as much as possible even if the smartphone users have LTE. Furthermore, cell phone carriers tend to shift flat-rate data services to pay-as-you-go data services. 3G data traffic should be optimized to save packet communication fees.

Our goal is to minimize the amount of data by effective use of bandwidth giving satisfaction to the audience.

For example, S.McCanne [1] adjusts video quality depending on available network bandwidth as a method to achieve effective use of bandwidth. Similarly, recent research for a mobile broadcasting study maximized bandwidth utilization. However, these schemes may use redundant network bandwidth in excess of audience satisfaction. The quality should be determined from the viewpoint of audience satisfaction, not available network bandwidth. In our work, the new aspect is dynamic quality adjustment by audience participation during a live broadcast. The amount of data traffic is optimized by dynamic quality adjustment which change quality based on audience requests. We have adjusted not video quality but picture quality for the proposed system to reduce data traffic as much as possible and to take a closer look at user interaction. As use of pictures to reduce the data traffic, Okada [2] realizes a conferencing system which uses still pictures so that it can work in a narrowband network. The conferencing system detects the direction of users' eyes and assists users by changing still pictures of users' faces without videos. The use of still pictures, reduces data traffic significantly. Moreover, the still picture is made clear in situations where the audience wants high quality. However, we will use the video in future work.

In this paper, we present PictCast which is a prototype system with functions of still picture Internet broadcasting and dynamic picture quality adjustment. The PictCast achieves stable Internet broadcasting anywhere via 3G networks using still picture instead of video and optimizes the amount of data traffic by changing picture quality based on audience requests. For the functions of dynamic picture quality adjustment, firstly it sends a minimal quality picture which satisfies the audience, secondly it retransmits picture data to the audience from the broadcaster when it receives a certain number of quality improvement requests from the audience. We report an experiment to measure minimum acceptable quality and the percentage of quality improvement requests from the audience.

2 PICTCAST

Figure 1 shows the model of our proposed system. A broadcaster sends still pictures and voice to the audience via 3G wireless network. The audience watches a broadcast program from their PC via high-speed network. The voice is compressed and broadcast to the audience in real time. The still pictures are compressed in a progressive format. To reduce data traffic, the broadcaster sends the still pictures to the audience at the minimum picture quality which is acceptable to the audience at first. When the audience requires higher quality still pictures, they can send quality improvement requests to the broadcaster. The broadcaster retransmits higher quality still pictures responding to a certain number of audience requests. In this case, the first low-quality still picture is replaced simply by retransmitting a high-quality one. Therefore, we use progressive decoding

ISBN978-4-902523-36-2

which is represented by progressive JPEG. The progressive decoding makes a picture gradually sharper as the download progresses. To apply the mechanism, the broadcaster can improve the quality of a still picture progressively without wasting transmitted picture data.

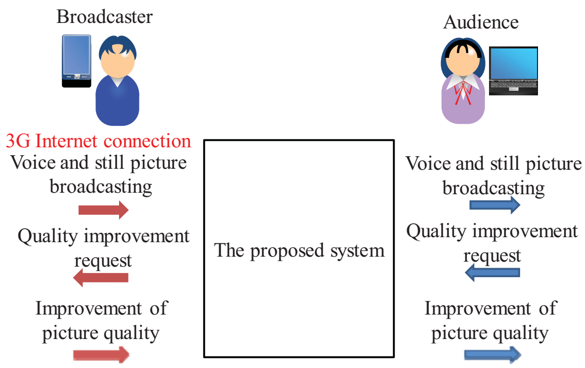


Figure 1: System Model.

3 EXPERIMENT

We studied to predefine minimal quality and percentage of quality improvement requests in all audiences. This section shows our method of testing subjective picture quality and its result.

3.1 Method

There are many subjective assessment methods which are defined by ITU-T and ITU-R recommendations. We selected ACR (Absolute Category Rating) methodology on a 5-point scale based on total assessment time and ease of evaluation. The ACR methodology is defined by ITU-T Rec. P910. In the ACR, subjects evaluate quality of pictures within 10 seconds after watching the pictures which are displayed in random order. Random order eliminates the possibility of affecting the assessment by indicating a sequence for the pictures. For example, a medium quality picture having a high rating after watching a low quality picture. The quality of the pictures is assessed by MOS (Mean Opinion Score) which shows the average score.

Moreover, we investigated the percentage of quality improvement requests in all audiences on the subjective picture quality assessment by a question item: " Would you like a higher quality picture?" for all resolutions.

3.2 Environment

We conducted the assessment in the environment described by ITU-R Rec. BT.500. The pictures were displayed in a 17-inch LCD monitor (LCD-A173KW) with the resolution 1024x768. Subjects perform the assessment at a distance of 120cm away from the display screen.

The pictures are JPEG format with 5 resolutions, from 40x30 to 640x480. The size of the picture display field is 640x480 pixels because it is popular size for Internet broadcasting sites.

Table 1: The result of the assessment

	MOS	**The percentages of quality improvement requests**
640x480	4.46	18%
320x240	3.30	59%
160x120	2.20	96%
80x60	1.66	100%
40x30	1.23	100%

We selected ten kinds of pictures to conduct a subjective picture quality assessment with. The type of the pictures are "Person", "Group", "Painting", "Cat", "Paper", "Meal", "Building", "Tree", and "Standard Image". The "Standard Image" is one of the pictures which is standardized by The Institute of Image Electronics Engineers of Japan (IEEJ). The picture was ratified by the International Standards Organization (ISO). These are selected based on typical topic categories of live video broadcasting from mobile devices on the Internet. The number of subjects should be more than fifteen according to ITU-R Rec. BT.500. The assessment was conducted by 23 subjects who are students of our university.

3.3 Result

Table 1 shows the result of the assessment. We determined 160x120 resolution for minimal quality of the still pictures because this resolution got a MOS score of around 2.5 for the all assessments, while 320 x 240 resolution got a MOS score of more than 2.5 for all the assessments. The MOS score of 2.5 is called the acceptability limit because it includes over 50% of subjects who give 3 points. Therefore, the progressive decoding in the prototype system is offered by three steps from 160x120 to 640x480.

Moreover, the percentages of quality improvement requests of 160x120 and 320x240 were above 50 %. From the result, we temporally determined a threshold for the picture quality improvement of 50% of total unique users.

4 CONCLUSION

We proposed PictCast which is a prototype system with functions of still picture Internet broadcasting and dynamic picture quality adjustment. We decided minimal quality and percentage of quality improvement requests in all audience. For future work, we will evaluate the system in rural areas and developing cities.

REFERENCES

[1] K.Okada, Y.Matsushita, A Multiparty Conferencing System Using still pictures for Narrow Band Networks, Information Processing Society of Japan, vol.39, no.10, pp.2762-2769 (1998)

[2] Steven McCanne, Van Jacobson, and Martin Vetterli, “Receiver-driven layered multicast. In Conference proceedings on Applications, technologies, architectures, and protocols for computer communications, SIGCOMM ’96, pp. 117–130 (1996).

An image-based CAPTCHA using mental rotation

Yuki Ikeya*, Junya Kani*, Yuta Yoneyama*, and Masakatsu Nishigaki*

*Graduate school of Informatics, Shizuoka University, Japan
{gs13002, gs12012, gs12040}@s.inf.shizuka.ac.jp, nisigaki@inf.shizuoka.ac.jp

Abstract - The Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) [1] has been widely used as a technique that will allow a machine to distinguish between input from a human and that of another machine. However, as many researchers have already reported, conventional CAPTCHAs can be overcome by state-of-the-art malwares since the capabilities of computers are approaching those of humans. Therefore, CAPTCHAs need to be based on even more advanced human-cognitive-processing abilities. Such CAPTCHAs are already proposed. However, there are challenge to automatic generation of image questions and the resistance to decipherment by malwares. In this paper, we propose an image-based CAPTCHA that focuses on mental rotation. Mental rotation is the advanced human-cognitive-processing ability to rotate mental representations of 2D/3D objects. We implement a prototype of the Mental Rotation CAPTCHA, and carry out basic experiments to confirm its usability. Also, we make a comparison between proposed CAPTCHA and existing CAPTCHA.

Keywords: Turing Test, CAPTCHA, mental rotation, image recognition, Web security

1 INTRODUCTION

With the expansion of Web services, denial of service (DoS) attacks by malicious automated programs (e.g., bots) are becoming a serious problem as masses of Web service accounts are being illicitly obtained, bulk spam e-mails are being sent, and mass spam blog posts are being created. Thus, the Turing test is becoming a necessary technique to discriminate humans from malicious automated programs.

The simplest CAPTCHA presents distorted or noisy text (Fig.1) to users who visit Web sites and want to use their services.

Figure 1: text recognition based-CAPTCHA by Google [2]

However, many researchers have recently pointed out that automated programs with optical character reader (OCR) and/or machine learning can answer these conventional text recognition based-CAPTCHA [3].

In this paper, we propose an image-based CAPTCHA that focuses on mental rotation. Mental rotation is the advanced human-cognitive-processing ability to rotate mental representations of 2D and 3D objects.

2 MENTAL ROTATION CAPTCHA

Humans are good at spatial reasoning capacity. For this reason, it is easy for humans to understand the 3D shape of the object from the 2D image. This ability is considered to be an advanced human-cognitive-processing ability [4]. By looking at the 2D images of the two sheets of copies from different viewpoints in the 3D object, humans infer the shape of the 3D object, and understand the change of the viewpoint.

Mental Rotation CAPTCHA automatically generates a pair of 2D images (*question image* and *response image*) of a 3D object from the two different viewpoint. In the *question image*, a marker (like a red sphere) is added to any portion of the 3D object. There is no marker in the *response image*. The user clicks the location on the *response image* where the site corresponding to the position of the marker of the *question image* is located. If the user is a human, he/she can use mental rotation to click the correct position of the response image.

3 IMPLEMENTATION

We implemented a prototype Mental Rotation CAPTCHA (type α). Fig.2 shows the authentication screen example of our Mental Rotation CAPTCHA: the *question image* in the left of Fig.2; the *response image* is the right of Fig.2. The red sphere that is drawn on the question image is the marker. The visitor needs to identify the location on the *response image* where the site corresponding to the position of the marker on the *question image* is, so they can click the correct position on the *response image*. If the distance between clicked position and correct position (both pixel coordinates on the display) is less than or equal to the threshold value, he/she certified as human. In the example of Fig.2, because the marker is pointing to the right ear of the cat in *question image*, it is correct if the visitor clicks the right ear of the cat in the *response image*.

Figure 2: prototype Mental Rotation CAPTCHA (Left: question image; Right: response image)

ISBN978-4-902523-36-2

4 VERIFICATION EXPERIMENT

4.1 Experiment Method

The subjects included twenty volunteers, subjects 01-20, who all are college students of Faculty of Informatics and Faculty of Engineering. Each subject solved five Mental Rotation CAPTCHA in a row. For our CAPTCHA the first and second trial are treated as practice. We only evaluate the remaining three trials.

In addition, after the experiment, we do a survey on the object for usability. Questions of the survey are as follows. Question 1, 3, 5 are answered on a 5-point scale.

Q1. Is it easy solving the CAPTCHA? (Easy) : Yes (5) – No (1)
Q2. If you choose 1 or 2 in Question 1, please write what the reason is.
Q3. Is it user-friendly? (User-friendly) : Yes (5) – No (1)
Q4. If you choose 1 or 2 in Question 3, please write what the reason is.
Q5. Is it pleasant? (Pleasant) : Yes (5) – No (1)
Q6. If you choose 4 or 5 in Question 5, please write what the reason is.
Q7. How many questions would you be able to continuously solve? Also, please write what the reason is.
Q8. Which would you choose: text recognition based-CAPTCHA or Mental Rotation CAPTCHA in ad real Web service? Also, please write what the reason is.

4.2 Experiment result

4.2.1. Correct response rate and response time

The experiment results are shown in Table 1. The details of the results are omitted due to space limitations.

The correct response rate of the Mental Rotation CAPTCHA is 77.3% (a total of 60 times, 44 success, 16 failures) on average over all the subjects.

The average response time per challenge is 5.4 seconds (the shortest time is 3.2 seconds, and the maximum time is 8.9 seconds). Given that it takes about 10 seconds to solve character CAPTCHAs in general, it can be said that the proposed CAPTCHA can be solved in a short time compared with text recognition based-CAPTCHA.

Table 1: the experiment result

	Correct response rate	Response time [sec]
Average	73.3% (44/60)	5.4

4.2.2. Usability

The results of the survey are shown in Table 2. The details summarized for space reasons.

In Question 8, five subjects chose the text recognition based-CAPTCHA, while 15 subjects chose the Mental Rotation CAPTCHA. We believe subjects who felt the inconvenience of text recognition based-CAPTCHA chose the Mental Rotation CAPTCHA. We found that suitable CAPTCHA varied among subjects by personal preference.

Table 2: result of survey

	Q1. Easy	Q3. User-friendly	Q5. Pleasant	Q7. How many
Average	3.3	4.3	4.3	2.7

5 DISCUSSION

5.1 Automatic generation

Mental Rotation CAPTCHA can generate a new question image using 3D computer graphics every time and achieves the automatic generation of the images. Our system can generate the pair of images (*question image* and *response image*) innumerably by registering a large number of 3D models with a system, and changing some parameters (the object, size of the object, marker position, and viewpoint).

5.2 Security

Mental Rotation CAPTCHA does not take the answer form of choosing the nearest image from a candidate list, so it is expected to improve resistance to the template matching attack. It becomes difficult to archive past images by generating countless pair of images.

Further, for the attack using a 3D recognition techniques, the system addresses these by deformation (α type) or replacement (β type) of the 3D object between *question image* and *response image*.

However, the attack techniques of malware are varied, and our CAPTCHA's resistance to decipherment is not proved theoretically. We plan to consider machine learning attack, as soon as possible in the future.

6 CONCLUSION AND FUTURE WORK

In this paper, we proposed a Mental Rotation CAPTCHA, and evaluated the system in a verification experiment. The results show that the correct response rate is 77.3% and the average response time per one challenge is 5.4 seconds. Although the response time required per question is short, the correct response rate will have to be improved in future. Our survey of the results of usability is satisfactory.

At present, there is still room for improvement in terms of both security and usability, so we plan to make improvements to the proposed method based on the knowledge obtained through the experimental results in this paper. Furthermore, we will also conduct studies to determine whether the Mental Rotation CAPTCHA is truly resistant to malware attacks.

REFERENCES

[1] The Official CAPTCHA Site, http://www.captcha.net
[2] Unlocking Google's Gmail CAPTCHA, http://www.gmailhelp.com/2009/10/unlocking-googles-gmail-captcha/
[3] PWNtcha-Captcha Decoder, http://caca.zoy.org/wiki/PWNtcha
[4] Shepard, R and Cooper, L, Mental images and their transformations., MIT Press, Cambridge, MA, 1982

Investigating Entropy of User-retained Authentication Information

Takuya Kaneko[*], Masakatsu Nishigaki[*]

[*]Faculty of Informatics, Shizuoka University, Japan
gs13010@s.inf.shizuoka.ac.jp
nisigaki@inf.shizuoka.ac.jp

Abstract -User authentication schemes wage a war between security (resistance to attack) and usability (memory load). This trade-off causes the security of user authentication to depend greatly on the attackers' techniques and knowledge. As such, we expect that known attacks against user authentication can be used to control such a trade-off. This paper proposes to effectively increase the entropy of user supplied information in password-based authentication by using the brute force attack, which is a classic attack technique against password-based user authentication. The proposed scheme improves password authentication by ensuring resistance against attacks, even when the adversary's ability increases, while reducing the burden of password memorization.

Keywords: User authentication, Entropy-enhanced, Brute Force Attack, Memory load

1 INTRODUCTION

User authentication relies on user supplied information, such as a password, biometric information or the solution to a CAPTCHA. We refer to this type of user supplied information as "secret information". In order to ensure password authentication resistance against Brute Force attacks, we should set secret information whose entropy is larger than computer literacy of attacker. Password entropy means the variety of the password. Brute Force attacks or exhaustive search are common attacks against user authentication. It involves systematically attempting all possible solutions until reaching the correct one. As processing power increases, the feasibility of Brute Force attacks also increases, and computational power increases daily. On the other hand, password length that a human can remember or an individual's biometric information do not increase over time and basically fixed. Therefore, if we ensure that entropy of secret information is large enough to be robust against Brute Force attacks, user authentication would be impossible, as the user would not be able to remember their secret information.

Accordingly, it is important to design a solution that takes into consideration the entropy of the secret information and the time it would take to successfully Brute Force it. Namely, we change the authentication procedure for a legitimate user to act like the attacker, using the Brute Force technique to augment the authentication information. We then combine the Brute Force results with the secret information that the user can remember. As a result, the user authentication changes from "a user enters secret information, which has low entropy, for authentication only" to "a user benefits from information constructed from computational power (the brute force results) coupled with the advantage of the secret information for authentication".

2 IDEA

In this paper, we propose the user authentication method in which a legitimate user leverages known attacking techniques, using the system much like an attacker. Our authentication method is based on the idea of using the system's processing power coupled with the secret information that the user can remember to strengthen the overall entropy of the user supplied portion of the authentication process.

2.1 Concept

The Brute Force or exhaustive search approach has a trait that a time required to try all patterns grows exponentially with the bit length of the authentication information. Thus, authentication information which has a short bit length would require less time to succumb to a brute force attack than one containing a long bit length. By using this trait, our method requires that the user input a part of the authentication information to complement the remnant of the authentication information. Together with this, we can mitigate the scarcity of entropy in the authentication information, and authenticate the user within a reasonable time. Hence forth, we will call the input information provided by the user as "secret information", and the information complemented by the exhaustive search approach in our method as "assistance information". The authentication information is derived by concatenating the secret information with the assistance information.

It is noteworthy that we can set the entropy of the authentication information at will by adjusting the entropy of the assistance information in our proposed method. This allows us to computational power increases thus decreasing the time required for a successful brute force attack, without increasing the secret information that the legitimate user must input.

ISBN978-4-902523-36-2

2.2 Basic Authentication Procedure

The proposed authentication method, shown in Figure 1, works as follows.

1. There is a twofold hash value for the authentication information P$(= P_u|P_r)$, H(H(P)) in the authenticating server. Now, P_u is the secret information that the user input, P_r is the assistance information which is derived by an exhaustive search approach.
2. The authenticating server sends the client H(H(P)).
3. The user inputs P_u on the client terminal.
4. The client executes an exhaustive search for P_r to make $H(H(P_u|P_r))$ equal to H(H(P)) on the client terminal.
5. The client sends $H(P_u|P_r)$ to the authenticating server.
6. The server authenticates the client when $H(H(P_u|P_r))$ equals H(H(P)).

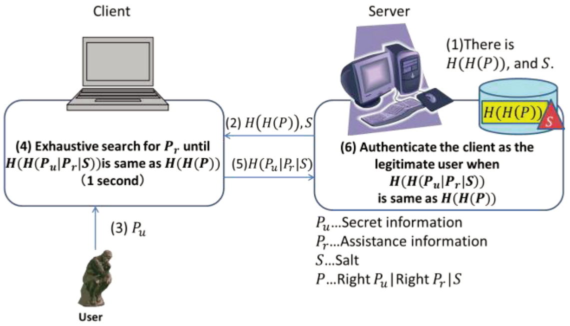


Figure 1: Basic Procedure

2.3 Extended Procedure includes Salt

To enhance the security of our approach, we consider resistance to Rainbow Table Attacks [1]. We extended the authentication procedure to include a salt [2]. The authentication procedure, including the salt, works with the following modifications.

1. There is the twofold hash value for the authentication information P$(= P_u|P_r|S)$, H(H(P)), and salt S.
2. The server sends the client H(H(P)), S.
3. The user inputs P_u on the client terminal.
4. The client executes an exhaustive search for P_r to make $H(H(P_u|P_r|S))$ equal to H(H(P)) on the client terminal.
5. The client sends the authenticating server $H(P_u|P_r|S)$.
6. The server authenticates the client when $H(H(P_u|P_r|S))$ equals H(H(P)).

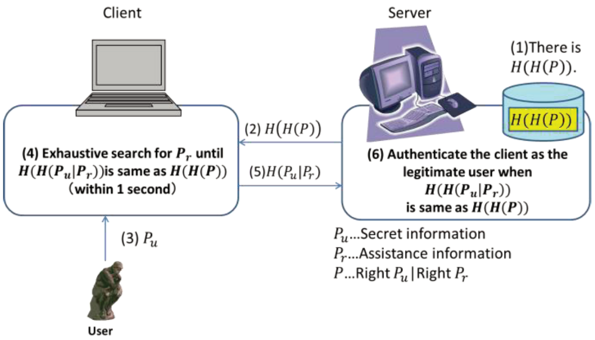


Figure 2: Extended Procedure

3 EVALUATION OF THE RESISTANCE TO THE BRUTE FORCE ATTACK

In our method, we set the entropy of the secret information P_u, and the assistance information P_r to ensure that the exhaustive search ends within a reasonable time, one that a legitimate user can wait.

The resistance to Brute Force Attacks in our method will be kept even as computational power improves. Since the computer was invented, computational power has improved rapidly. Resistance to Brute Force Attacks deteriorates when computational power improves, because the time required for an exhaustive search decreases. We assume that the entropy of P is E, the entropy of P_u is E_u and the entropy of P_r is E_r, and the computational power increases twofold. As such, the time required for an exhaustive search is reduced by half. Because of this, the time that the legitimate user needs to exhaustive search for P_r is kept, when we increase the bit numbers to make E_r twofold. Moreover, E increases twofold by making E_r twofold because $E = E_u \times E_r$. So, the time the attacker needs to exhaustive search for the authentication information $P_u|P_r$ is kept.

The difference in time to exhaustively search for the authentication information P for a legitimate user (one that knows P_u), and an attacker (does not know P_u) does not depend on computational power, but rather on the size of E_u. By setting the secret information P_u to have the desired resistance, we can safely use our proposed authentication method regardless of computational improvements. We assume that it is sufficient safe when an attacker needs 1 year to Brute Force attack and a legitimate user can wait 1 second to exhaustively search, E_u is only 3×10^7 because 1 year is 3×10^7 seconds.

4 CONCLUSIONS AND FUTURE WORKS

In this paper, we propose the user authentication method that ensures safety and usability. It leverages the Brute Force attacking technique used against user authentication, and considers the entropy of user supplied secret information in user authentication.

Using this method, the client can ensure there is sufficient resistance to a Brute Force Attack when the user inputs only secret information with little entropy. However, there exists a vulnerability to Dictionary Attack, if the user sets their secret information to an easily guessed string. As such, the user should set a more complex password, by following existing password complexity guidelines.

The proposed method possesses the advantage of not placing a large strain on the authenticating server, as it performs the exhaustive search in the end client. However, this means that the entropy of the authentication information depends on the computational power of the end user's computer. Because of this, we cannot ensure the desired resistance when an attacker uses a higher computational powered machine to attack authentication information generated by an end user's lower powered one. In the future we want to examine a method that would use cloud computing to separate the strength of the authentication from the power of the user's computer.

Wireless Networked Omnidirectional Video Distribution and Collection System based on Delay Tolerant Networking Protocol in a Multiple Communication Environment

Kenta Ito[*], Kazuma Tsuda[**], Yoshitaka Shibata[**]

[*]Graduate School of Software and Information Science, Iwate Prefectural University, Japan
g231l001@s.iwate-pu.ac.jp
[**]Faculty of Software and Information Science, Iwate Prefectural University, Japan
shibata@iwate-pu.ac.jp

Abstract – In this paper, we introduce a wireless networked omnidirectional video distribution and collection system for a multiple communication environment using Delay Tolerant Networking (DTN) protocol. Data gathered is transmitted to all of the users through a web application. The user can see the data gathered on GIS map as a web service. The system configuration and architecture are explained and a prototype system is constructed to evaluate the performance of our system.

Keywords: Road Monitoring System, Omnidirectional Camera, DTN, GIS

1 INTORODUCTION

Japan is prone to natural disasters occurring including earthquakes, tsunami, typhoon, heavy rain and snow. A wide range and quick information gathering systems are needed after a disaster has occurred. But for disaster surveillance, usually fixed point video monitoring by a single directional camera is used.

Recently location information acquisition technology and omnidirectional camera technology has been developed. Thus, wide area video surveillance considering the location information is possible.

When a disaster occurs, wireless networks are useful because we can build a network quickly using moving vehicles. But there is a challenging communication environment where communication is disabled.

On the other hand, implementation of monitoring by the omnidirectional image and vehicle mobile wireless network has been made recently. We use the omnidirectional image and vehicle mobile wireless network, for monitoring road conditions, disaster areas, snow cover and flooded rivers and considering a multiple communication environment.

Our purpose is to build a wireless networked omnidirectional video distribution and collection system based on DTN protocol in a multiple communication environment. In detail, to be available normally and after a disaster has occurred, to be available without internet access, to construct a DTN based system and to support for changes in network conditions.

2 SYSTEM CONFIGURATION

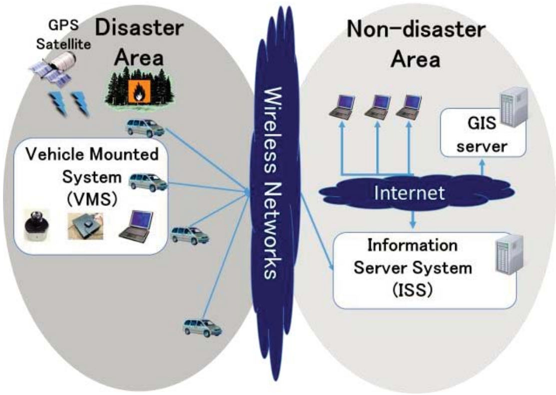


Figure 1 System configuration

Our system is composed of mainly two subsystems, including a vehicle equipped with a Vehicle Mounted System (VMS) and a server PC equipped with an Information Server System (ISS). Further, the VMS consists of a GPS receiver, omnidirectional camera, environmental sensor and control PC. The VMS collects video images around the vehicle, location and environmental sensor data, and transmits this data to the ISS through wireless networks. ISS provides the data as a web application.

This system, we equipped with two modes of video distribution, Live View (LV) mode and Storage View (SV) mode. LV mode is for real-time monitoring such as disaster areas, road conditions in heavy rain and snow, traffic conditions and the state of a tourist destination. SV mode is for monitoring the situation in a challenging communication environment such as monitoring the status of disaster areas and monitoring of mountainous areas.

3 OMNIDIRECTIONAL EXPANSION PROCESS

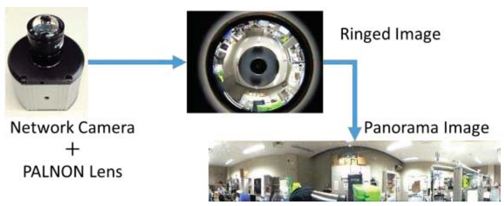


Figure 2 Omnidirectional expansion process

Figure 2 shows a PALNON lens which is attached to the network camera. The image acquired from the omnidirectional camera is a ringed image. But it is difficult to visually recognize.

ISBN978-4-902523-36-2

The original ringed image is converted to a panorama image by an omnidirectional expansion process. It is now easy to visually recognize.

4 DELAY TOLERANT NETWORKING (DTN) PROTOCOL

DTN is an approach to the problem of a “challenging computer network” that provides interoperable communication where continuous end-to-end connectivity cannot be assumed.

To realize interoperable communication under poor network environments, DTN creates a “store-carry-forward” protocol for its routing. That is, each node stores the transmission data if there is no available node nearby, and the data is transmitted when a node comes close enough to other nodes.

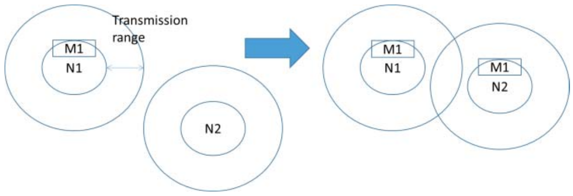


Figure 3 Image of data transmision by DTN

Figure 3 shows the image of data transmission by DTN. Node N1 holds the message data M1, when there is no available node nearby. If N1 comes close enough to Node N2, M1 is transmitted to N2. Then, M1 will be carried to other nodes in the same way until the data reaches the goal node.

5 PROTOTYPE SYSTEM

Figure 3 Our prototype system

We propose a prototype system using four devices, Vehicle Mounted PC, camera device, environmental sensor device and Information Server PC. Figure 4 is the prototype VMS

6 SYSTEM EXECUTION EXAMPLE

These are the results of SV mode.

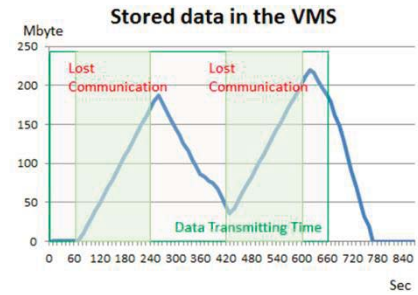


Figure 5 Stored data in the VMS

Figure 5 shows stored data in the VMS. When communication is lost, the VMS can't transmit data to the ISS, stored data increases. When communication is connected, the VMS resumes transmitting data to the ISS and stored data decreases.

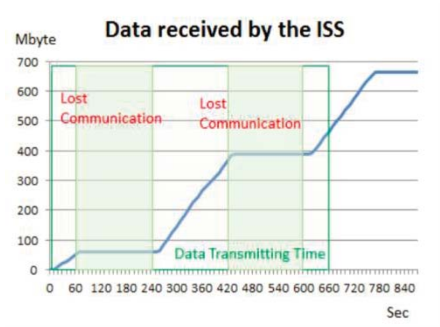


Figure 6 Data received by the ISS

Figure 6 shows data received by the ISS. When communication is lost, data can’t be transmitted by the VMS, so the ISS doesn’t receive data. When communication is connected, the VMS resumes transmitting data, and the ISS resumes receiving data.

7 CONCLUSION

We propose to build a wireless networked omnidirectional video distribution and collection system based on the Delay Tolerant Networking protocol in a multiple communication environment. Our system realizes gathering and sharing video and environmental data around the vehicle, considering real-time and non-real-time environments, construction of a system using usual and a challenging communication environment. In the future, we will use the system in mountainous and disaster areas as a field test.

REFERENCES

- Keita Saito, Yoshitaka Shibata, Koji Hashimoto: Implementation of Disaster Information System with Omni-directional Camera and Geological Sensors, ieice2011 p640
- Delay Tolerant Networking Research Group: http://www.dtnrg.org/wiki/
- Welcome OpenCV wiki: http://opencv.willowgarage.com/wiki/

Research on Mobile Cloud-based Disaster Information System based on the DTN Protocol

Yosuke Kikuchi[*], Yoshitaka Shibata[**]

[*]Graduate School of Software and Information Science, Iwate Prefectural University, Japan
g2311008@s.iwate-pu.ac.jp
[**]Faculty of Software and Information Science, Iwate Prefectural University, Japan
shibata@iwate-pu.ac.jp

Abstract - In this paper, we propose a disaster information system that can deal flexibly failure of the server group and rapid load change. We will operate the system of the previous research in the cloud infrastructure.

In addition, this system provides high operability and functionality for mobile terminal.

Keywords: Disaster Information System, Cloud Computing, System Virtualization, Load Balancing, Delay Tolerant Networking

1 INTRODUCTION

Japan is a disaster-prone country, and was severely damaged in the Great East Japan Earthquake that occurred in March 2011. To prepare for them, disaster information Web-based systems have been created, contributing to rapid information sharing after the disaster in recent years. In addition, cloud technology is popular now, and the reduction in the cost of operation and maintenance of the servers, such as the expansion of the server as needed is possible. From this, many advantages are present when creating a Web-based system.

In this paper, we propose a disaster information system that can respond flexibly to failure of the server group and rapid load change. A Distributed Disaster Information System in consideration of the mobile communication environment[1] was a previous study. In this study, we migrate a disaster information system to a cloud server. Thus, we are able to dynamically allocate server resources as needed to several different municipalities. This enables the risk and management in the system, and changes the server configuration in accordance with the type disaster. In the application, we optimized the system to work correctly on smartphones and tablets. In addition, map information is saved locally to provide service without relying on Web-GIS.

2 SYSTEM OUTLINE

Figure 1 shows an overview of this system. The system is composed of a cloud server, the DTN Server, and the Mobile Disaster Cloud. The role of the client changes depending on the place and status of the infrastructure.

The Cloud server manages the disaster information system. In addition, it registers disaster information in a database for local government officials, and has functionality to browse for the general user. The system performs the registration of disaster information from the mobile client in areas that have an Internet connection in the affected area. It is equipped with relay vehicles in areas that don't have access the Internet, such as geography or damage of communication infrastructure, Mobile Disaster Cloud devices patrol the affected areas. The system is equipped with wireless communication devices using 3G, WiMAX, LTE etc. the relay vehicle, register the disaster information from the client.

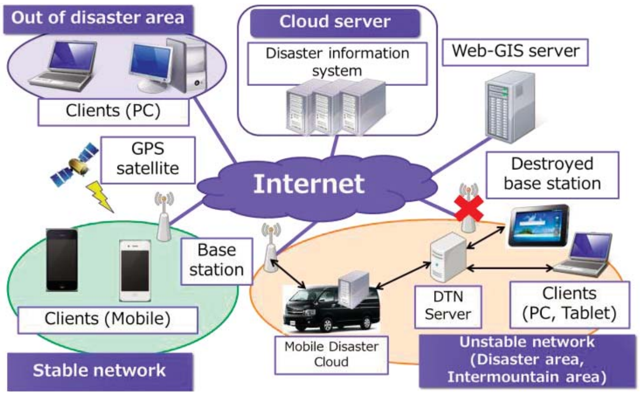


Figure 1: System outline

3 SYSTEM ARCHITECTURE

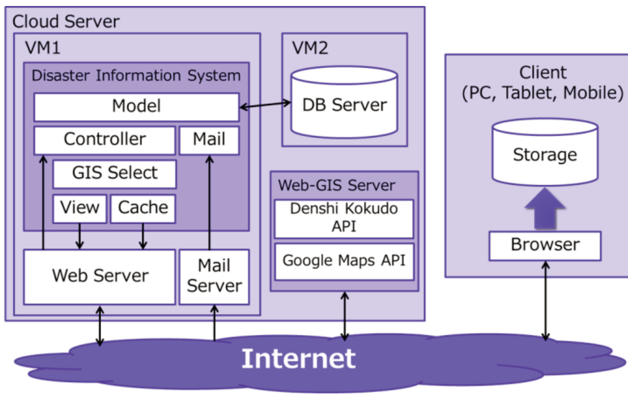


Figure 2: System architecture

Figure 2 shows the architecture of the Cloud Server. We create multiple virtual machines which each run their own module to distribute the load of the whole system. We configured Web Server and Mail Server on VM1, and DB Server on VM2. By using a template virtual machine that you created, and copying the disk image, it is possible to

ISBN978-4-902523-36-2

create a new virtual machine if necessary. We perform dynamic control of the virtual machine using this template.
Unlike the Cloud Server, DTN Server performs the registration of disaster information, so that it can be viewed in a way that does not depend on Web-GIS. If the system can't communicate with Web-GIS, the View module generates a HTML response to the client via the map data that is cached in client storage.

4 SYSTEM BEHAVIOR

4.1 Normal Operation

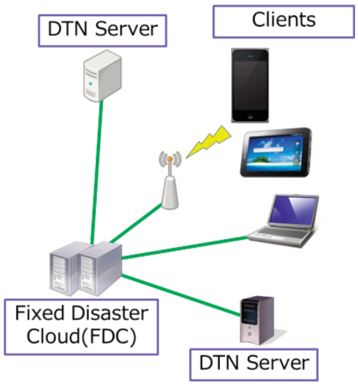


Figure 3: The behavior of the system if an Internet connection is available

Figure 3 shows the behavior of the system if an Internet connection is available. In this case, the DTN Server is able to communicate directly with Fixed Disaster Cloud. Information in the server from all groups is aggregated to the FDC. Also, in response to failure after the disaster or load change to the server system, it automatically controls the network configuration and server. Specifically, it processes the arrangement of best server group, extension, reduction, and merging data. As a condition for controlling these, the network status and the size of the load for the FDC are assumed.

4.2 When the Internet connection disabled

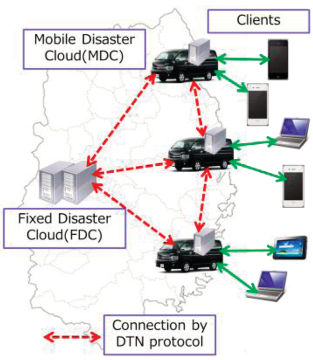


Figure 4: The operation of the system in the image if it can't connect to the Internet

Figure 4 shows the operation of the system if it can't connect to the Internet. Information stored in the DTN Server are all aggregated to the FDC. Wireless communication devices for 3G, WiMAX, LTE, etc. IEEE802.11a/b/g/n/j are mounted on the DTN Server. Relay vehicles equipped with the MDC after a disaster has occurred move to the affected areas, and register the disaster area information from a variety of clients. The MDC without relying on the Internet registers the disaster area information locally. Once Internet is restored, relay vehicles patrol the affected areas again, and synchronize the information between all MDC and the FDC. It is assumed that the DTN protocol is used to communicate here.

5 PROTOTYPE SYSTEM

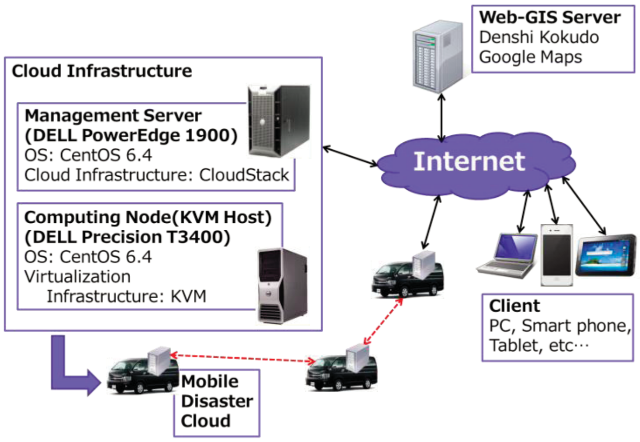


Figure 5: The prototype of system environment

Figure 5 shows the prototype of the system environment. The Cloud infrastructure environment is composed of a Computing Node and a Management Server. The system uses CentOS 6.4 as the OS. It uses CloudStack as the cloud infrastructure software and KVM as the virtualization infrastructure. In addition, the node that the DTN Server and the MDC are also a similar configuration.

6 CONCLUSION

In this study, we have proposed a cloud-based disaster information sharing system that takes into account a large-scale disaster. With this system, it is possible to mitigate the risk of down-time caused by a physical failure of the server due to external factors such as the earthquake and tsunami.
In the application, high operability and functionality can be obtained even in the case that you want to use the system with smartphones and tablets, registration of information in the map-based view is possible even in an environment not available to the Internet.
In the future, I will recreate previous studies using this new cloud-based system. Also, I will consider the information we gathered on optimizing map-based systems such as Web-GIS for independent operation on mobile terminals.

REFERENCES

[1] Y. Sasaki, and Y. Shibata, Construction of Distributed Disaster Information System in consideration of the mobile communication environment, The Institute of Electronics, Information and Communication Engineers (IEICE), "S-65"-"S-66" (2011)
[2] Y. Sasaki, and Y. Shibata, Construction of Disaster information system that enables the display time series uniform, Information Processing Society of Japan (IPSJ), "3-427"-"3-428" (2010)

MapReduce Framework for Distributed Computation

Daniel McDermott

Eastern Washington University
Cheney, WA, U.S.A

August 29, 2013

Outline

Outline

Defined

Data-Intensive Text Processing with MapReduce, 2010

"MapReduce is a programming model for expressing distributed computations on massive datasets and an execution framework for large-scale data processing on clusters of commodity servers."

First described in *"MapReduce: Simplified Data Processing on Large Clusters"* by Jeffery Dean and Sanjay Ghemawat, Google Inc, 2004.

Two Aspects

A Programming Model / Paradigm

- from functional programming
- algorithm design **restriction!**

A Execution Framework / Runtime

Automatic parallel/distributed execution on large cluster computers.

- Scales horizontally, not vertically.
- Assumes failures are common.
- Moves computation to the data.
- Hide system-level details from the programmer.
- Scales seamlessly.

The restirctions of the Programming Model will enable the features of the Exection Framework

Overall Theme of MapReduce

Given a large dataset, apply some transformation to each element or record of the dataset (**map**), producing a temporary intermediate dataset. Then iterate over the intermediate dataset performing an aggregation, summarization, or similar reduction (**reduce**).

A surprising number of problems in Datamining and Computer Science can be phrased in this way.

The "Big Data" Revolution

The Unreasonable Effectiveness of Data, 2009

Problems that involve interacting with humans, such as natural language understanding, have not proven to be solvable by concise, neat formulas like $F = ma$. Instead the best approach appears to be harnessing the power of data...

- Sloan Digital Sky Survey produces 500TB of astronomical images each month [1]
- LHC @ CERN: Estimates 15PB of data generated each year. [2]
- In the future, personal DNA sequencing will become routine

The amount of data in existence doubles roughly every two years.[3]

[1] `www.sciencenewsdaily.org/internet-news/202854792/`
[2] `home.web.cern.ch/about/computing`
[3] Cisco, The Economist

Scope of problems

A word of warning

"To a man with a hammer, every problem looks like a nail."

- MapReduce is a **data parallel** paradigm focused on **scalability** and data **bandwidth**
- Most solutions involve sequentially reading large amounts of **static data** from disks and moving it through a **wide** computation pipeline
- MapReduce is a batch processing system
- Moving data will dominate the cost of computation

MapReduce is not:

- Low latency
- A data retrieval method
- A "supercomputing" method

Data is large, computation is relatively small

Who Uses MapReduce?

Deployed widely at Google, Amazon, Facebook, Yahoo, Ebay, IBM, Nokia, Qualcomm, LinkedIn, CERN, and others.

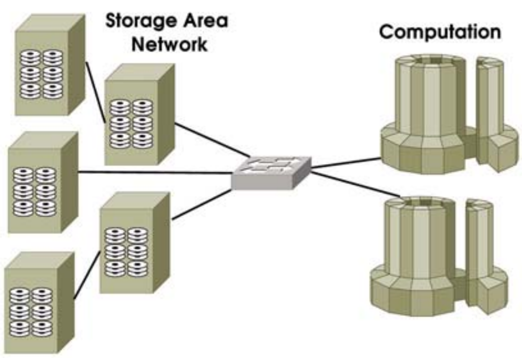
Parallel vs Distributed

- **Parallel**: Special purpose interconnects focused on low latency, shared memory model, computationally intense problems such as physics simulations and dynamic systems modeling. Frequent random access syncronization in small bytes
- **Distributed**: Inexpensive hardware, 1Gbit ethernet, data intensive problems with minimal shared state between compute elements, large streaming reads and writes

Scaling Models

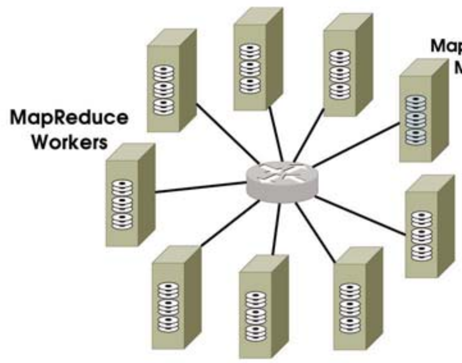
- **vertical**: "scale up": buy better, faster, special purpose hardware → HPC
- **horizontal**: "scale out": buy more hardware of same type → MapReduce

Traditional HPC Datacenter



- Must scale *vertically*
- Parallel system focused on low latency

The MapReduce Datacenter



- Scales *horizontally* with cheap, consumer-grade, hardware
- Distributed system focused on wide throughput

Distributed File Systems

MapReduce file systems oriented towards large, sequential, reads and writes. Streaming data to and from the disk.

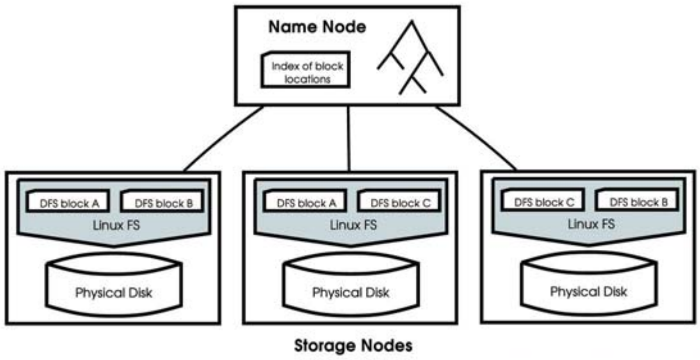
- Fault tolerant via block replication
- Logical
- Generally not POSIX compatible

Examples:

- Google's BigTable (*Bigtable: A Distributed Storage System for Structured Data*, Dean, Burrows, et.al. 2006)
- HDFS - Hadoop Distributed File System
- DDFS - Disco Distributed File System

Distributed File System Architecture

- Large Block Size (typically 64MB)
- With K replication factor, $K-1$ nodes can fail
- Name node serves metadata about all files on file system



Outline

1. What is MapReduce?
2. Functional Programming Roots
3. MapReduce Execution Framework
4. Thesis Work

Functional Programming Review

- Applications of functions do not modify data, always create new data
- Original data structures always exist unmodified
- Data flow is implicit in program design

$$\Longrightarrow$$

- Order of application across threads or functions does not matter
- There are no **side-effects** and thus no **shared-state** between function applications or threads

Common Functional Programming Patterns

Functional programming often operates over *lists*...

Just as in procedural programming, functional programming has common patterns which are built into the languages

- **Map**: Element-wise transform a list
- **Fold**: Accumulate a list into a single value

Map

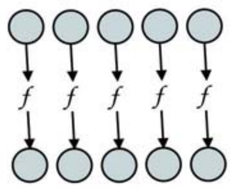
Map Function

map(*func*, *list*)

Input: **list**: A list to map over. **func**: A function to apply to each element in the list, which returns a new element.

Output: A new list, representing *func* applied to every element of *list*

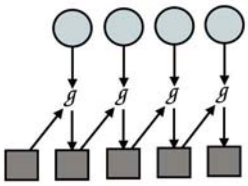
newlist ← **new empty list**
foreach *element in list* **do**
  newlist.append(*func*(*element*))
return *newlist*



Fold or Accumulate (Reduce)

Fold Function

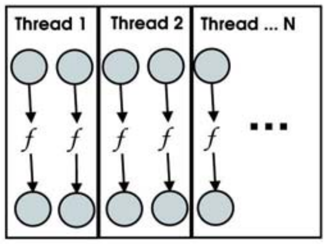
fold(*acc*, *func*, *list***)**
Input: **acc**: An accumulator value. **func**: A function which takes a list element and a value and returns a new value. **list**: A list to read.
Output: The final value of *acc*.
foreach *element in list* **do**
  acc = *func*(*acc*, *element*)
return *acc*



Can *acc* be a list?

Parallelizing Map

- In a purely functional setting, there are no side effect from elements of a list being computed by map
- The order of application of "func" to the list elements is *commutative*, thus we can parallelize
- This is the core property of MapReduce as a programming model



Outline

Redefining Map

- Instead of a list, the input to map will be records from a data source, supplied as *key*, *value* pairs (ex. filename,contents)
- Mapping over the entire data source is accomplished by mapping over each separate record in parallel (a "two level" map)
- Each map process will output one or more intermediate *key*, *value* pairs
- User code is responsible for iteration and application

User Map Function

method MAP(docid a, doc d)
  forall the *term t* ∈ *doc d* **do**
    EMIT(term t, count 1)

Redefining Reduce

- After map phase, all intermediate values for a given key are aggregated into a list
- Reduce summarizes or combines the intermediate values per key into one or more final values
- In practice, there is usually one final value per key
- Again, the user code is responsible for iteration and application

User Reduce Function

method REDUCE(term t, counts [c_1, c_2, ...])
  sum ← 0
  forall the *count c* ∈ *counts [c_1, c_2, ...]* **do**
    sum ← *sum* + *c*
  EMIT(term t, count sum)

Programming Model to Runtime

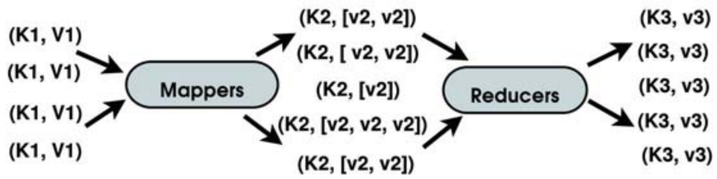
The programmer defines a map and a reduce function with the types:

$$map(K1, V1) \rightarrow (K2, [v2])$$
$$reduce(K2, [v2]) \rightarrow (K3, v3)$$

The framework:

1. Splits the input into chunks or blocks
2. Assigns each block to a map task, assigns all tasks to worker machines (mappers)
3. Each worker applies the map function to each element of its assigned block outputing keys and values
4. Aggregates these values by key (shuffle and sort)
5. Assigns (partitions) each key to a reduce task, assign all tasks to worker machines (reducers)
6. Each worker applies the reduce function over the values for its keys

Programming Model to Runtime

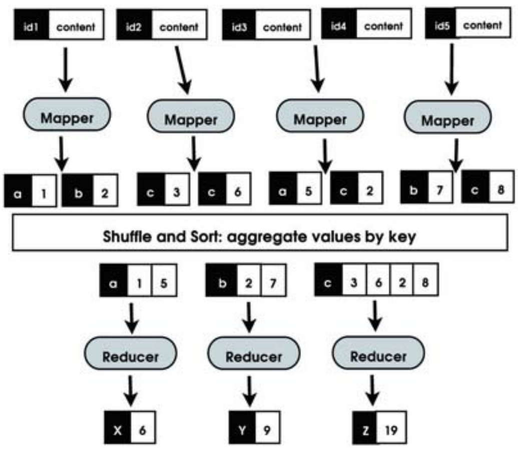


Wordcount example

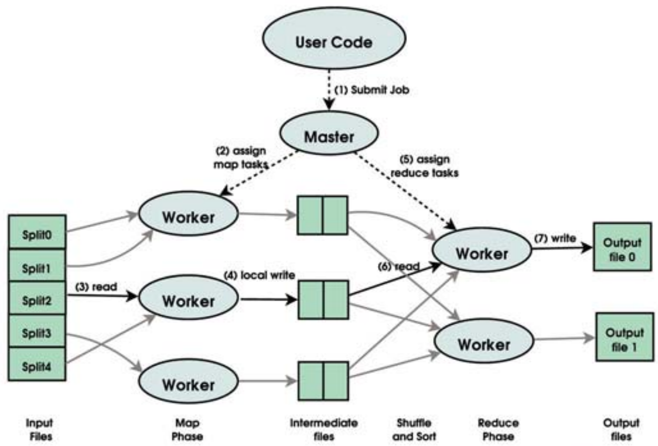
WordCount

class JOB
  method MAP(docid a, doc d)
    forall the *term* $t \in$ *doc* d **do**
      EMIT(term t, count 1)
  method REDUCE(term t, counts $[c_1, c_2, ...]$)
    $sum \leftarrow 0$
    forall the *count* $c \in$ *counts* $[c_1, c_2, ...]$ **do**
      $sum \leftarrow sum + c$
    EMIT(term t, count sum)

Wordcount Data Flow



MapReduce Systems Perspective



Fault Tolerance

Inexpensive, commodity, hardware

- **Re-Execution**: machine or rack failure → run task again. (note we must re-run all completed tasks on that node as well, why?)
- **Bad Record Skipping**: user code crashes on certain input → log error and skip
- **Speculative Execution**: stragglers → use idle machines to replicate in-progress jobs

Outline

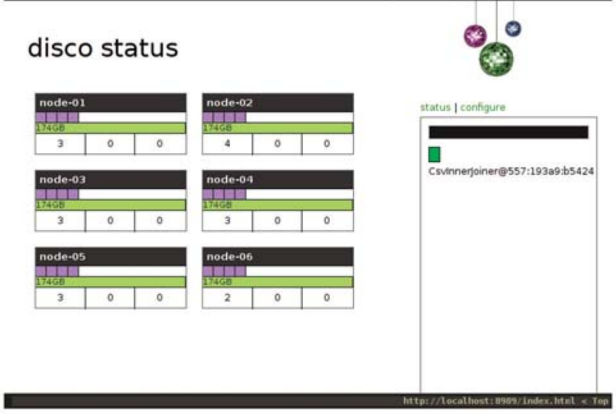
Cluster Setup

- Six Machines, each:
  - 4x 2.8Ghz Intel Xeon
  - 5GB Memory
  - 4x 73GB 10,000rpm SCSI U320 in RAID 5 (175GB after OS + formatting)
- 30GB Memory Total
- 24 Processors Total
- 1TB Distributed Storage
- 1Gbit switched network

Cluster Setup

Disco Framework

MapReduce runtime in Erlang + Python



Further Resources

Runtimes / Frameworks:

- Disco - MapReduce in Python + Erlang `http://discoproject.org`
- Hadoop - MapReduce in Java `http://hadoop.apache.org`

Free Online Books:

- Data Intensive Text Processing with MapReduce, Jimmy Lin and Chris Dyer. `http://lintool.github.io/MapReduceAlgorithms`
- Mining of Massive Datasets, Anand Rajaraman and Jeffery Ulman. `http://infolab.standford.edu/~ullman/mmds.html`
- The Datacenter as a Computer: Introduction to the Design of Warehouse-Scale Machines, Luiz Barroso and Urz Holze. `http://www.morganclaypool.com/doi/abs/10.2200/S00193ED1V01Y200905CAC006`

Further Resources

Papers:

- *Bigtable: A Distributed Storage System for Structured Data*, Dean, Burrows, et.al. 2006)
- *MapReduce: Simplified Data Processing on Large Clusters*, Dean & Ghemawat 2004

Vidoes:

- Google Developer Series on Cluster Computing and MapReduce `http://youtu.be/yjPBkvYh-ss`

Questions?