

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC,
Petitioner,

v.

HUMAN DIFFERENTIAL INTELLIGENCE, LLC,
Patent Owner.

Case No. TBD
Patent No. 9,192,861

DECLARATION OF MARY K. BOLIN, PH.D.

Google Exhibit 1021 Google v. HDI

I, Mary K. Bolin, declare as follows:

1. I am Emeritus Professor at the University of Nebraska, Lincoln Libraries. I have held the following positions: Professor and Catalog and Metadata Librarian, Digital Initiatives and Special Collections Department, University of Nebraska, Lincoln Libraries (2015-2020); Professor and Chair, Discovery and Resource Management and Coordinator of Collection Development, University of Nebraska, Lincoln Libraries (2004-2015); Lecturer, San José State University School of Information (2008-present); Head of the Technical Services Department, University of Idaho Library (1993-2003; promoted to Professor in 1999); Head of the Cataloging Department, University of Idaho Library (1986-1993; promoted to Associate Professor and tenured in 1991); Head of Records Maintenance Section, Cataloging Department, University of Georgia Libraries (1981-1986).
2. Over the course of my work as a librarian, professor, researcher, student research supervisor, and author of numerous scholarly papers and other publications, I have had extensive experience with cataloging records and online library management systems built around Machine-Readable Cataloging (MARC) standards. I also have substantial experience in authenticating printed documents and establishing the date when they were accessible to ordinarily skilled researchers.
3. Exhibit A is my full resume.

4. I have been retained by Wolf, Greenfield, & Sacks, P.C., counsel for Petitioner Google LLC, to determine the authenticity and dates of public availability of certain documents in the *inter partes* review proceedings of U.S. Patent No. 9,192,861 (the “’861 Patent”). For this service, I am being paid my usual fee of \$100 per hour, plus actual expenses. My compensation is not dependent in any way upon the outcome of the *inter partes* review of the ’861 Patent.

I. DOCUMENTS OF INTEREST

5. The documents that are the subject of this declaration are the following:

Document 1. Sajad Shirali-Shahreza and M. Shirali-Shahreza, "CAPTCHA for Children," *2008 IEEE International Conference on System of Systems Engineering (SoSE)*, Monterey, California, 2008, pp. 1-6, doi: 10.1109/SYSOSE.2008.4724188. Ex. 1008.

Document 2. Luis von Ahn. *Human Computation*. Dissertation, Carnegie Mellon University, 2005. Ex. 1009.

Document 3. G. Kochanski, D. Lopresti, and C. Shih. “A Reverse Turing Test Using Speech,” *Proceedings of the Seventh International Conference on Spoken Language Processing*, September 2002, Denver, CO, pp. 1357-1360. Ex. 1015.

II. METHODOLOGY

6. I searched for each of these documents (1) in subscription databases (large repositories of reliable scholarly content from well-known publisher) such as *IEEE Xplore*, *SpringerLink*, and *ACM Digital Library*, and (2) in *Google Scholar* (an open access database that aggregates content from subscription sites as well as other freely available repositories of scholarly and research data). I searched for Document 2, a dissertation, in the Online Computer Library Center (“OCLC”) database. I searched the conference proceeding volumes for Documents 1 and 3 in OCLC as well. I also searched the library catalogs of institutions such as the University of Nebraska, Lincoln and other large research libraries. My goal was to find a record in one or more of these databases that contained a date indicating when the work in question was available to the public.

7. *Use of MARC Records.* The “Machine Readable Cataloging” standard, also known as “MARC,” is an industry-wide, standard method of organizing library catalog information. MARC was first developed in the 1960s by the Library of Congress. A MARC-compatible library is one that has a catalog consisting of individual MARC records for each of its works. Today, MARC is the primary communication protocol for the transfer and storage of bibliographic metadata in libraries.

8. When an OCLC participating institution acquires a work, it creates a MARC record for this work in its computer catalog system in the ordinary course of its business, and OCLC automatically supplies the date of creation. The MARC record creation date reflects the date on which (or shortly after which) the item was first acquired and catalogued. Once the MARC record is created by a cataloger at an OCLC participating member institution, it is instantaneously available to any OCLC participating members, and, therefore, available to the public.

9. A MARC record comprises several fields, each of which contains specific data about the work. Each field is identified by a standardized, unique, three-digit code corresponding to the type of data that follow. For example, a work's title is recorded in field 245, the primary author of the work is recorded in field 100, an item's International Standard Book Number ("ISBN") is recorded in field 020, an item's Library of Congress call number is recorded in field 050, and the publication date is recorded in field 264 under the subfield "c." If a work is a periodical, then its publication frequency is recorded in field 310, and the publication dates (*e.g.*, the first and last publication) are recorded in field 362, which is also referred to as the enumeration/chronology field. The library that created the record is recorded in field 040 in subfield "a" with a unique library code.

10. OCLC provides its members online access to MARC records through its OCLC Connexion database. When viewing the MARC record online via the OCLC Connexion database, hovering over this code with the mouse reveals the name of the library. I used this method of “mousing over” the library codes in the OCLC database to identify the originating library for all the MARC records in this declaration. In the MARC records in the OCLC Connexion database, MARC field 040 contains the OCLC symbols of institutions transcribing, creating, and modifying the record.

11. OCLC was created “to establish, maintain and operate a computerized library network and to promote the evolution of library use, of libraries themselves, and of librarianship, and to provide processes and products for the benefit of library users and libraries, including such objectives as increasing availability of library resources to individual library patrons and reducing the rate of rise of library per-unit costs, all for the fundamental public purpose of furthering ease of access to and use of the ever-expanding body of worldwide scientific, literary and educational knowledge and information.”¹ Among other services, OCLC and its

¹ Third Article, Amended Articles of Incorporation of OCLC Online Computer Library Center, Incorporated (available at <http://www.oclc.org/en-US/membership/councils.html>).

members are responsible for maintaining the WorldCat database

(<http://www.worldcat.org/>), used by independent and institutional libraries

throughout the world. OCLC is the international cooperative to which libraries catalog records and others pay to access MARC records. The MARC records referenced in this declaration, extracted from the OCLC database, were generated in the ordinary course of business. Further, I personally located and downloaded each of these records.

12. MARC records created at the Library of Congress are tape-loaded into the OCLC database through a subscription to MARC Distribution Services daily or weekly. Once the MARC record is created by a cataloger at an OCLC member institution or is tape-loaded from the Library of Congress, it is then made available to any other OCLC members online, and, therefore, made available to the public. As noted before, when an OCLC member institution creates a new record, OCLC automatically supplies the date of creation for that record. The MARC record creation date reflects the date on which, or shortly after which, the item was first acquired or cataloged.

13. The date of creation for the MARC record appears in the fixed field (008), characters 00 through 05. Field 005 is a 16-digit field that record the Date characters yyymmdd include 4 for the year, 2 for the month, and 2 for the day. The Date entered on file never changes. These dates are automatically supplied by

the OCLC system and cannot be changed by the user. When the MARC record is created in OCLC, it is available throughout the world to other libraries and in WorldCat, the public version of OCLC Connexion. Thus, the date of creation of the MARC record by a cataloger at an OCLC member institution reflects when the underlying item is accessible to the public.

14. For each of Documents 1-3, I searched OCLC, [www. oclc.org](http://www.oclc.org), for the conference proceedings (Documents 1, 3) or the dissertation (Document 2).

15. For those documents for which there is a record in OCLC, I determined when the record was created and which libraries own the item. I then visited the website of the library or libraries that own the item, searched their library catalog, and determined when the item was added to the library's collection.

16. I am familiar with many online catalogs, databases, and search engines. In preparing for this declaration I used authoritative information systems such as WorldCat (<https://www.worldcat.org>), the online catalog of the Library of Congress (<https://catalog.loc.gov>), the online catalog of a number of large research libraries such as the University of Nebraska, Lincoln, the public catalog of the United States Copyright Office (<https://cocatalog.loc.gov/>), LexisNexis, IEEEExplore, Google Books, and Google Scholar search for records. These records are identified and discussed in this declaration.

III. AUTHENTICATION OF DOCUMENT 1

17. Document 1 was found in IEEE Xplore at:

<https://ieeexplore.ieee.org/document/4724188>. The face of the document accurately reflects the title, author, and publication information listed on the webpage at that URL, and document appears to be complete. It states that the document was added to IEEE Xplore December 22, 2008. The PDF properties show that the PDF was created on April 4, 2008. (The “date modified” is when I downloaded and saved it.) A MARC record for the conference proceedings was found in OCLC. It was added to the OCLC database on March 6, 2009. The conference proceedings for the *2008 IEEE International Conference on System of Systems Engineering (SoSE)*—of which Document 1 was a part—appears in the Library of Congress copyright database (cocatalog.loc.gov), where it states that the record for the conference proceedings for the *2008 IEEE International Conference on System of Systems Engineering (SoSE)* was created on March 5, 2009, and that the proceedings were published on December 12, 2008. The authors of Document 1 compiled and published a “Bibliography of Works Done on CAPTCHA” later in 2008, and the bibliography includes Document 1. It is found in IEEE Xplore at <https://ieeexplore.ieee.org/abstract/document/4730926>. The face of that document accurately reflects the title, author, and publication information listed on the webpage at that URL, and document appears to be complete.

18. Attachment 1 is a screenshot of the PDF properties for the article.
19. Attachment 2 is a PDF of the results screen from IEEE Xplore, saying that the article was added on December 22, 2008.
20. Attachment 3 is a MARC record for the conference proceedings.
21. Attachment 4 is the record for the conference proceedings from the Library of Congress copyright database.
22. Attachment 5 is a PDF of the IEEE results screen for “Bibliography of Works on CAPTCHA,” showing that it was added to IEEE Explore on December 30, 2008.
23. Attachment 6 is a PDF of the article “Bibliography of Works Done on CAPTCHA.”

IV. PUBLIC AVAILABILITY OF DOCUMENT 1

24. Based on the fact that Document 1 was added to IEEE Xplore in December 2008, on the properties of the PDF file, and on the citation to Document 1 in the “Bibliography of Works on CAPTCHA” later in 2008, this document would have been available publicly by late 2008 and could have been retrieved by a skilled researcher. Based on the records for the conference proceedings in OCLC and the Library of Congress copyright database, the document also would have been available in early 2009 and could have been retrieved by a skilled researcher.

V. AUTHENTICATION OF DOCUMENT 2

25. Document 2 was found in the online library catalog of Carnegie Mellon university at MARC Record:

https://cmu.primo.exlibrisgroup.com/discovery/sourceRecord?vid=01CMU_INST:01CMU&docId=alma991000901079704436&recordOwner=01CMU_INST where it states that the record was created October 20, 2006.

26. Document 2 was also found in Dissertation Abstracts: <https://search-proquest-com.libproxy.unl.edu/pqdt/docview/305006687/7F821E62E4614922PQ/4?accountid=8116> where it states that it was made available by ProQuest dissertation publishing in 2005.

27. Attachment 7 is a PDF of the MARC record for the dissertation from the Carnegie Mellon University online library catalog.

28. Attachment 8 is a PDF of record from the Dissertation Abstracts database.

VI. PUBLIC AVAILABILITY OF DOCUMENT 2

29. Based on the fact that the MARC record in the Carnegie Mellon library catalog was created in October 2006, and the record in the Dissertation Abstracts database was created in 2005, Document 2 was available sometime in 2005, and at the latest by October 2006, and could have been retrieved by a skilled researcher.

VII. PUBLIC AVAILABILITY OF DOCUMENT 3

30. This article was retrieved from https://www.isca-speech.org/archive/archive_papers/icslp_2002/i02_1357.pdf. The Properties of this PDF file show that it was created on July 30, 2002. The conference proceedings are found at: <https://www.semanticscholar.org/paper/Proceedings-of-the-7th-International-Conference-on-Tan-Dalsgaard/f2d898947f5f0c7ae107a005386c1301ddc662bf>. That page states that the proceedings were published in 2002. The PDF link from the conference proceedings to the paper is <http://www.cse.lehigh.edu/~lopresti/Publications/2002/icslp02.pdf>, the faculty website of one of the authors. Apart from the blue text at the top of the first page in the isca-speech.org PDF, the two documents are substantively identical. The properties of the Lehigh University PDF show that it was created on April 1, 2002. That website was archived by the Internet Archive (web.archive.org) at least as early as September 1, 2004, indicating that the paper was publicly accessible on that website by that date. *See* <http://web.archive.org/web/20040901075237/http://www.cse.lehigh.edu/~lopresti/Publications/2002/icslp02.pdf>. The face of the document accurately reflects the title, author, and publication information listed on the webpage at that URL, and document appears to be complete.

31. Attachment 9 is the PDF from isca-speech.org.
32. Attachment 10 is the PDF from Lehigh University
33. Attachment 11 is a screenshot of the PDF from isca-speech.org, showing the creation date.
34. Attachment 12 is a screenshot of the PDF from Lehigh University, showing the creation date.
35. Attachment 13 is a screenshot of the web page for the conference proceedings, where it states that the proceedings were published in 2002.
36. Attachment 14 is a screenshot of the web.archive.org web page for the Lehigh University website, showing that the paper was available on Lehigh University's website by September 1, 2004.

VIII. PUBLIC AVAILABILITY OF DOCUMENT 3

37. Because PDFs of this document in multiple locations were created in 2002, because the conference proceedings state that they were published in 2002, and because web.archive.org indicates the document was available online by September 1, 2004, this document was publicly available in 2002, or at the latest in September 2004, and could have been found by a skilled researcher.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements are made with the knowledge that willful false statements and the like are punishable by fine, imprisonment, or both, under Section 1001 of Title 18 of the U.S. Code.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on **September 11, 2020**



Mary K. Bolin, Ph.D.

EXHIBIT A

Mary K. Bolin, PhD

Professor Emeritus
University Libraries
University of Nebraska—Lincoln
mbolin2@unl.edu

Lecturer,
School of Information
San José State University
mary.bolin@sjsu.edu

EDUCATION

PhD, Educational Studies (Educational Leadership and Higher Education), 2007, University of Nebraska

Dissertation: *A Typology and Discourse Analysis of the Status and Appointments of Librarians at Land Grant Universities* (available at digitalcommons.unl.edu)

MA, English, 1999, University of Idaho
Thesis: *Grace: A Contrastive Analysis of a Biblical Semantic Field* (available at digitalcommons.unl.edu)

MSLS, 1981, University of Kentucky

BA, Linguistics, 1976, University of Nebraska—Lincoln

WORK EXPERIENCE

Center for Digital Research in the Humanities. Fellow, 2019- Emeritus, 2020-

University of Nebraska--Lincoln Libraries: Professor and Catalog and Metadata Librarian, Digital Initiatives and Special Collections, 2015-2020. Emeritus, 2020-

University of Nebraska—Lincoln Libraries: Professor and Chair, Discovery and Resource Management, 2004-2015; Coordinator of Collection Development, 2012-2015

University of Idaho Library: Head, Technical Services Department, 1993-2003. Promoted to

Professor in 1999

University of Idaho Library: Head, Cataloging Department, 1986-1993. Promoted to Associate Professor and tenured, 1991

University of Georgia Libraries: Head, Records Maintenance Section, Cataloging Department, 1981-1986

Teaching:

San José State University School of Information:

LIBR 281, Metadata. 2009-

LIBR 248, Introduction to Cataloging and Classification. 2013-

LIBR 202, Information Retrieval. 2008-2013

American Library Association

Cataloging for Non-Catalogers, Online Continuing Education Course, 2017-

Intermediate Cataloging for Non-Catalogers, Online Continuing Education Course, 2018-

Independent Study in Idaho

Library Science C415, Technical Services for Small Libraries, 2004-2013

Library Science C416, Library Services to Rural Libraries, 2004-2013

Library Science C422, Use of the School Library, 1999-2013

Library Science C425/525, Organization and Management of Small Libraries, 1988-2013

Library Science C427, Library or Media Center Practicum, 1995-2013

Gateway PhD Program (San Jose State University and Queensland University of Technology). SJSU supervisor for two PhD students, 2015-

Consulting

Expert witness for multiple attorneys employed by Wolf, Greenfield & Sacks, P.C., Hughes Hubbard & Reed LLP, and other firms. 2017-

SCHOLARSHIP

Refereed Publications:

(Publications available from digitalcommons.unl.edu)

Pytlík Zillig, Brian, and Mary K. Bolin. (Submitted) "Shakespeare and the Enumeration of Semantic Primes." *Japanese Journal of Digital Humanities*.

Wintermute, Harriet E., and Bolin, Mary K. (2018). "Metadata Generators for Backlog Reduction: Metadata Maker Streamlines Cataloging and Facilitates Transition. *Technical Services Quarterly* 35(2) doi: <https://doi.org/10.1080/07317131.2018.1422879>

Bolin, Mary K. (2018). "Metadata, Catalog Systems, Linked Data, and the Evolving ILS." In: Sandra Hirsh (Ed.), *Information Services Today: An Introduction*. 2nd ed. New York: Rowman and Littlefield.

Bolin Mary K. (2017). *The 21-century Academic Library: Global Patterns of Organization and Discourse*. Oxford: Chandos Publishing. (Chandos Information Professional Series)

Bolin, Mary K. (2017). Linguistics and LIS: A Research Agenda." *SLIS Student Research Journal*, 7:1.

Retrieved from <http://scholarworks.sjsu.edu/slissrj/vol7/iss1/2>

Bolin, Mary K. (2014). "Open Access Web Resources for Library Continuing Education and Training." In S. Hines (Ed.), *Revolutionizing the Development of Library and Information Professionals: Planning for the Future* (pp. 107- 124). Hershey, PA: . doi:10.4018/978-1-4666-4675-9.ch008.

Bolin, Mary K. (2014). "The Language of Academic Librarianship: The Discourse of Promotion and Tenure." *Advances in Library Administration and Organization* 32.

Bolin, Mary K. "Librarian Status at US Research Universities: Extending the Typology." *Journal of Academic Librarianship* 34:4 (September 2008)

Bolin, Mary K. "A Typology of Librarian Status at Land Grant Universities." *Journal of Academic Librarianship*, 34: 3 (May 2008)220:230.

Bolin, Mary K. "The Library and the Computer Center: Organizational Patterns at Land Grant Universities." *Journal of Academic Librarianship*, 31:1 (2005)

Eckwright, Gail Z. and Mary K. Bolin. "The Hybrid Librarian: The Affinity of Collection Management with Technical Services and the Organizational Benefits of an Individualized Assignment." *Journal of Academic Librarianship*, 27:6 (2001)452:457.

Bolin, Mary K. "Catalog Design, Catalog Maintenance, Catalog Governance," *Library Collections, Acquisitions, and Technical Services*. 24: (2000)53-63.

Bolin, Mary K. "The Collegial Environment and the Functional Organization," *Journal of Library Administration*. 29:2(1999):49-61.

Bolin, Mary K. "Cataloging Environmental Impact Statements and Related Documents," *Resource Sharing and Library Networks*. 14:1(1999): 21-40.

Bolin, Mary K. "Waiting for the Electrician or Someone like Him: Client-Centered Technical Services" Proceedings of the Association of College and Research Libraries National Conference, Nashville, April 1997.

< http://www.ala.org/Content/ContentGroups/ACRL1/Nashville_1997_Papers/Bolin.htm >

Grants:

Electronic Theses and Dissertations. Seed Grant from University of Idaho Office of Research, 2002. Co PI with Gail Z. Eckwright. \$6500.

Interoperability of Metadata for Thematic Research Collections. Grant to the Center for Digital Research in the Humanities from the Institute of Museum and Library Services 2005-2008.

Project Team Member.

http://unlcms.unl.edu/cas/center-for-digital-research-in-the-humanities/projects/pages/iom_files/IOM_Final_Narrative_Report_July_2008.pdf

Other Publications:

Library Philosophy & Practice. Peer-reviewed electronic library science journal. Mary K. Bolin and Gail Z. Eckwright, founders and editors. <http://digitalcommons.unl.edu/libphilprac>

Library Science C415, Technical Services for Small Libraries, through Independent Study in Idaho. 2004.

Library Science C416, Library Services to Rural Libraries, through Independent Study in Idaho. 2004.

Library Science C422, Use of the School Library, through Independent Study in Idaho. Revised 1999.

Library Science C425/525, Organization and Management of Small Libraries through Independent Study in Idaho. Revised 2005.

Library Science C427, Library or Media Center Practicum, Independent Study in Idaho. Revised 1999.

Presentations:

Bolin, Mary K. "BibFrame and the MARC Cataloging Environment: an Introduction." Lyris Webinar, June 16, 2020. Recording available <http://lyris.adobeconnect.com/paufo9e0dm30/>

Pytlik Zillig, Brian, and Mary K. Bolin. "A Little More than Kin, a Little Less than Kind": the Semantic Field Grace in Early Modern English" Poster Session, Text Encoding Initiative Meeting, Graz, Austria, September 18, 2019

Pytlik Zillig, Brian, and Mary K. Bolin. "Shakespeare and the Enumeration of Semantic Primes." Research Paper Presentation, Text Encoding Initiative Meeting, Tokyo, Japan, September 13, 2018

"Library Philosophy and Practice: Creating and Maintaining an Open-Access E-Journal," Presentation to UNCL meeting (libraries at campuses of the University of Nebraska), Lincoln, Nebraska, March 20, 2008.

Presentation to "Thinking outside the Borders" participants on the open-access electronic journal Library Philosophy and Practice and its role in the international library community. University of Nebraska—Lincoln Libraries, October 24, 2007

Panel discussion on open access electronic journals. GWLA directors' meeting. Linda K. Hall Library, Kansas City, Missouri. April 2007.

"Waiting for the Electrician or Someone Like Him: Client-Centered Technical Services." Association of College and Research Libraries National Conference, Nashville, April 5, 1997.

" 'Some Problems of an Editor': the Idaho Librarian from Manuscript to Published Issue," Joint Annual Conference of the Idaho Library Association and the Washington Library Association, Spokane, Washington, April 6, 1995.

"Automating Idaho's Libraries: a Historical Perspective." Idaho Library Association Annual Conference, Idaho Falls, October 4, 1990.

"Small Library Management." Idaho Library Association Spring Conference, Lewiston, Idaho, May 13, 1989.

"No More 'Good Workers': Excellence and Academic Library Classified Staff." Association of College and Research Libraries 5th Annual Conference, Cincinnati, April 7, 1989.

"Communication to and from Cataloging Departments." Heads of Cataloging Discussion Group, American Library Association Midwinter Meeting, San Antonio, January 1988.

Discussion Leader at the LAMA (Library Administration and Management) Management Exchange. American Library Association Annual Meeting, San Francisco, June 1987.

"Staff Turnover." Heads of Cataloging Discussion Group, American Library Association Midwinter Meeting, Chicago, January 1987.

SERVICE

Reviewer. *Resources for College Libraries*. Linguistics bibliography, Spring 2020.

Peer reviewer for ALISE National Conference presentations, Spring 2020.

Peer reviewer for *Journal of Academic Librarianship*, 2012-

Peer reviewer for refereed journal, *Western Nigerian Journal of Medical Sciences* (<http://www.wnjms.org/>), a publication of Ladoke Akintola University of Technology (LAUTECH) Teaching Hospital, 2008-

PhD Reviewer for students from Aligarh Muslim University, India, 2010-

Outside reviewer for numerous library faculty promotion and tenure cases in US universities.

Faculty Committee Assignments:

University of Nebraska – Lincoln

Chair, University of Nebraska Libraries Faculty, 2018

Academic Rights and Responsibilities Committee, 2016- Chair, 2018-19

Faculty Senate – 2004-2008; 2008-2011

Faculty Senate Executive Committee 2004-2008

Academic Planning Committee (APC), 2005-2008; Vice Chair, 2006-2007; Chair, 2007-2008

Aesthetic Review Committee 2006-2007

APC monitor for academic program reviews: Department of Political Science, 2005; Department of Educational Psychology 2006

Chancellor's Committee on Wellness, 2007-

University of Idaho:

University of Idaho NASC Accreditation Committee: Chair, Standard 5, Library and Information Resources Subcommittee, 2002-2004.

Faculty Affairs Committee, 2001-2004; 1992-1995; Chair, 1994-1995

Committee on Committees, 2000-2003, Chair, 1991-92; 1995-96

Budget Liaison Committee, 1990-92, 1996-98; Chair, 1991-92; 1997-98

University of Idaho Presidential Search Committee, 1995-96

University of Idaho Provost Search Committee, 1996-97

University of Idaho Strategic Planning Task Force, 1997-98

Search Committee Chair, Lionel Hampton School of Music Director, 1998-99

Disability Affairs Committee, 1998-; Chair, 1999-2000

Faculty Council, Faculty-at-Large representative, 1989-92, 1995-98; Vice-Chair, 1991-92, 1995-96; Acting Chair, Spring 1996

Honors Program Committee, 1988-93; Chair, 1991-92

Student Employee Grievance Committee, 1988-89

Faculty-at-Large (Chair), 1987-89

Pacific Northwest Library Association:

Editor, *PNLA Quarterly*, December 2002-December 2013

Idaho Library Association:

Editor, *The Idaho Librarian*, September 1990-January 1996

Professional Memberships

American Library Association

ATTACHMENT 1

Acrobat Pro DCFileEditViewSignWindowHelp

04724188.pdf

HomeTools

04724188.pdf

1 / 6

100%

Document Properties

Description

Security

Fonts

Initial View

Custom

Advanced

File:04724188.pdf

Title:CAPTCHA for Children

Author:"Sajad Shirali-Shahreza, Mohammad Shirali-Shahreza"

Subject:Human/Machine Systems

Keywords:CAPTCHA (Completely Automated Public Turing test to tell Computers and Human Apart), Childrer Websites, Collage Image, Image Recognition, TTS (Text-To-Speech)

Created:4/4/08, 10:12:40 AM

Modified:8/26/20, 10:41:25 AM

Application:

Additional Metadata...

Advanced

PDF Producer:Acrobat Distiller 8.1.0 (Windows); modified using iText® 5.5.6 ©2000-2015

PDF Version:1.4 (Acrobat 5.x)

Location:/Users/Mary/Documents/consult/

File Size:389.58 KB (398,934 Bytes)

Page Size:8.50 x 11.00 in

Number of Pages:6

Fast Web View:No

Tagged PDF:No

Help

Cancel

OK

Sajad Shirali-Shahreza

Computer Engineering Department

Sharif University of Technology

Tehran, IRAN

shirali@ee.sharif.edu

Mohammad Shirali-Shahreza

Computer Science Department

Sharif University of Technology

Tehran, Iran

shirali@cs.sharif.edu

CAPTCHA for Children

Unfortunately, there are many programs that write programs to make automatic programs on a web site. These programs automatically extract incorrect information to enter the system. Such attacks are known as DoS or DoS.

Various methods have been proposed to prevent such attacks, aiming to distinguish between human users and computer programs. The methods should be their automatic methods by using the computer; because of registration on the Internet requires a great deal of time and effort, such as email services for examining the registration forms is practically impossible. Therefore, it is necessary to use automatic systems to distinguish human users from computer programs.

In the discussions of artificial intelligence (AI), a test

Lightshot Screenshots

to read or type anything

ATTACHMENT 2



BrowseMy SettingsHelp

Institutional Sign In

Institutional Sign In

All



ADVANCED SEARCH

Conferences > 2008 IEEE International Confe...

CAPTCHA for children

Publisher: IEEE

Cite This

Cite This

PDF

Sajad Shirali-Shahreza ; Mohammad Shirali-Shahreza All Authors

4
Paper
Citations

216
Full
Text Views

Export to

Collabratec

Alerts

Manage

Content Alerts

Add to

Citation Alerts



Abstract

Document Sections

- 1 Introduction
- 2 Related works
- 3 Our proposed method
- 4 Advantages
- 5 Conclusions

Authors

Figures

References

Citations

Keywords

Metrics

More Like This

Downl
PDF

Abstract: In some websites it is necessary to distinguishing between human users and computer programs which is known as CAPTCHA (Completely Automated Public Turing test to tell Co... **View more**

Metadata

Abstract:
In some websites it is necessary to distinguishing between human users and computer programs which is known as CAPTCHA (Completely Automated Public Turing test to tell Computers and Human Apart). CAPTCHA methods are mainly based on the weak points of OCR systems and using them are undesirable to human users. In this paper a method has been presented for distinguishing between human users and computer programs on the basis of choice of an object shown on the screen. In this method some objects are chosen randomly and the pictures of these topics are downloaded from the Internet. Then after applying some effects such as rotation, all of the pictures are shown on the screen. Then we ask the user to choose a specific object. Instead of writing the question, it is said using a TTS (Text-To-Speech) system. Therefore children who maybe illiterate and cannot read, can easily pass the test. If the user chooses the right object, we can guess that the user is a human being and not a computer program. This method is specially developed for children websites. The main advantage of this method is its simplicity because the user does not have to read or type anything.

Published in: 2008 IEEE International Conference on System of Systems Engineering

Date of Conference: 2-4 June 2008

INSPEC Accession Number: 10425652

Date Added to IEEE Xplore: 22 December 2008

DOI: 10.1109/SYSOSE.2008.4724188

Publisher: IEEE

ISBN Information:

Conference Location: Monterey, CA, USA, USA

Contents

1 Introduction

Many aspects of human life have been affected by the expansion of the World-Wide Web (WWW), so that, in industrial countries, many daily affairs, from daily shopping to education and commerce, are done on the Internet.

Authors	▼
Figures	▼
References	▼
Citations	▼
Keywords	▼
Metrics	▼

IEEE Personal Account	Purchase Details	Profile Information	Need Help?	Follow
CHANGE USERNAME/PASSWORD	PAYMENT OPTIONS	COMMUNICATIONS PREFERENCES	US & CANADA: +1 800 678 4333	f in t
	VIEW PURCHASED DOCUMENTS	PROFESSION AND EDUCATION	WORLDWIDE: +1 732 981 0060	
		TECHNICAL INTERESTS	CONTACT & SUPPORT	

About IEEE Xplore | Contact Us | Help | Accessibility | Terms of Use | Nondiscrimination Policy | Sitemap | Privacy & Opting Out of Cookies

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

© Copyright 2020 IEEE - All rights reserved. Use of this web site signifies your agreement to the terms and conditions.

IEEE Account	Purchase Details	Profile Information	Need Help?
» Change Username/Password	» Payment Options	» Communications Preferences	» US & Canada: +1 800 678 4333
» Update Address	» Order History	» Profession and Education	» Worldwide: +1 732 981 0060
	» View Purchased Documents	» Technical Interests	» Contact & Support

About IEEE Xplore | Contact Us | Help | Accessibility | Terms of Use | Nondiscrimination Policy | Sitemap | Privacy & Opting Out of Cookies

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

© Copyright 2020 IEEE - All rights reserved. Use of this web site signifies your agreement to the terms and conditions.

ATTACHMENT 3

WorldCat: System of Systems Engineering, 2008, SoSE '08, IEEE International...

OCLC 312711045		LDL Holdings - 218 other holdings 1 LDL holding in GLIMIR cluster; 218 other holdings in GLIMIR cluster							
Books	Rec Stat c	Entered 20090306		Replaced 20181201121101.7					
Type	a	ELvl	4	Srce	d	Audn	Ctrl	Lang	eng
BLvl	m	Form	o	Conf	1	Biog	MRec	Ctry	nju
Desc	a	Cont	b	GPub		LitF	0	Indx	1
		Ills	a	Fest	0	DtSt	s	Dates	2008,

007 c \$b r \$d m \$e n

040 STF \$b eng \$e pn \$c STF \$d WAU \$d OCLCQ \$d OCLCF \$d OCLCO \$d OCLCQ \$d OCL \$d OCLCO \$d OCLCQ \$d IAS \$d BUF \$d CEF \$d LVT

020 \$z 9781424421725

050 _4 TA168

090

049 LDLL

111 2_ IEEE International Conference on System of Systems Engineering \$d (2008 : \$c Monterey, Calif.)

245 10 System of Systems Engineering, 2008, SoSE '08, IEEE International Conference on : \$b date, 2-4 June 2008.

246 30 SoSE '08

260 [Piscataway, N.J.] : \$b IEEE, \$c [2008]

300 1 online resource : \$b illustrations

336 text \$b txt \$2 rdacontent

337 computer \$b c \$2 rdamedia

338 online resource \$b cr \$2 rdacarrier

500 Title from HTML table of contents (IEEE Xplore, viewed on Mar. 6, 2009).

500 Conference held in Monterey, California.

504 Includes bibliographical references.

650 _0 Systems engineering \$v Congresses.

650 _0 Human-machine systems \$v Congresses.

650 _7 Human-machine systems. \$2 fast \$0 (OCoLC)fst00963500

650 _7 Systems engineering. \$2 fast \$0 (OCoLC)fst01141455

655 _7 Conference papers and proceedings. \$2 fast \$0 (OCoLC)fst01423772

655 _4 Electronic books.

776 0_ \$z 9781424421725 \$w (OCoLC)441187743

856 40 \$3 IEEE Xplore \$u http://ieeexplore.ieee.org/servlet/opac?punumber=4695854

856 40 \$u http://ezproxy.uis.edu:2048/login?url=http://ieeexplore.ieee.org/servlet/opac?punumber=4695854

\$x IEEE \$y View online

856 40 \$u https://proxy.library.carleton.ca/login?url=https://ieeexplore.ieee.org/servlet/opac?

punumber=4695854 \$z IEEE Xplore (Access restricted to 50 simultaneous users)

856 40 \$u http://liverpool.idm.oclc.org/login?url=https://ieeexplore.ieee.org/servlet/opac?punumber=4695854

\$z View this e-book online

006 fields for Computer Files Computer File

Audn Form o File d GPub

Action Status Delete Holdings _ Export _ Label _ Produce _ Update Holdings _ Validate _

ATTACHMENT 4



Library buildings are closed to the public until further notice, but the U.S. Copyright Office Catalog is available. [More](#).

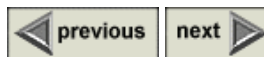
[Help](#)[Search](#)[History](#)[Titles](#)[Start Over](#)

Public Catalog

Copyright Catalog (1978 to present)

Search Request: Left Anchored Title = 2008 IEEE International Conference on System of Systems Engineering,

Search Results: Displaying 1 of 1 entries



Labeled View

2008 IEEE International Conference on System of Systems Engineering (SoSE) ...

Type of Work: Text

Registration Number / Date: TX0006943823 / 2009-03-05

Application Title: 2008 IEEE International Conference on System of Systems Engineering (SoSE)
(08EX2256)

Title: 2008 IEEE International Conference on System of Systems Engineering (SoSE)
(08EX2256)

Description: Book, 462p.

Copyright Claimant: IEEE. Address: 445 Hoes Lane, Piscataway, NJ, 08854, United States.

Date of Creation: 2008

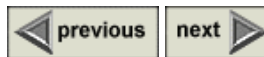
Date of Publication: 2008-12-02

Nation of First Publication: United States

Authorship on Application: IEEE, employer for hire; Domicile: United States; Citizenship: United States.
Authorship: Collective Work.

Rights and Permissions: William J. Hagen, IEEE, 445 Hoes Lane, Piscataway, NJ, 08854, United States,
(732) 562-3966, w.hagen@ieee.org

Names: [IEEE](#)



Save, Print and Email (Help Page)	
Select Download Format	Full Record Format for Print/Save
Enter your email address:	
Email	

[Help](#) [Search](#) [History](#) [Titles](#) [Start Over](#)

[Contact Us](#) | [Request Copies](#) | [Get a Search Estimate](#) | [Frequently Asked Questions \(FAQs\) about Copyright](#) | [Copyright Office Home Page](#) | [Library of Congress Home Page](#)

ATTACHMENT 5

All

Q

ADVANCED SEARCH

Conferences > 2008 3rd International Confer...

Bibliography of works done on CAPTCHA

Publisher: IEEE

Cite This

Cite This

PDF

2 Author(s)

Sajad Shirali-Shahreza ; M.Hassan Shirali-Shahreza

All Authors

9 Paper Citations

2 Patent Citations

269 Full Text Views

Export to

Collabratec

Alerts

Manage

Content Alerts

Add to

Citation Alerts

Top Organizations with Patents on Technologies Mentioned in This Article

ORGANIZATION 4

ORGANIZATION 3

ORGANIZATION 2

ORGANIZATION 1

Abstract	
Document Sections	Downl PDF
1. Introduction	
2. CAPTCHA Methods	Abstract: Nowadays, a great amount of information is circulated through the Internet. Some of them exclusively belongs to a special group of users and requires protection and safeg... View more
3. Applications	
4. Attacks and Analysis	Metadata Abstract: Nowadays, a great amount of information is circulated through the Internet. Some of them exclusively belongs to a special group of users and requires protection and safeguarding against unauthorized access. To this end, a category of systems called HIP (human interactive proof) have been introduced to distinguish between various groups of users.
5. Conclusion	
Authors	
References	Published in: 2008 3rd International Conference on Intelligent System and Knowledge Engineering
Citations	
Keywords	Date of Conference: 17-19 Nov. 2008 INSPEC Accession Number: 10441116
Metrics	Date Added to IEEE Xplore: 30 December 2008 DOI: 10.1109/ISKE.2008.4730926
More Like This	Publisher: IEEE ISBN Information: Conference Location: Xiamen, China

Contents

1. Introduction

Many aspects of human life are affected by the expansion of the World-Wide Web (WWW). In particular, in developed countries, many daily affairs from daily shopping to education and commerce can be done using the Internet. A common action which is done in most websites, especially those belonging to commercial and administrative applications, is to fill out registration forms for certain purposes. After filling out the forms by entering the required information, the individuals are allowed to login into that website and carry out certain jobs. Unfortunately, there are persons who abuse web services by writing programs which do automatic false registration in websites. These programs automatically fill out forms with incorrect information in order to enroll in the site. This wastes a large volume of the resources of the site in favor of the profit-seeking programmers and reduces the performance of the system.

Authors	▼
References	▼
Citations	▼
Keywords	▼
Metrics	▼

IEEE Personal Account

CHANGE USERNAME/PASSWORD

Purchase Details

PAYMENT OPTIONS

VIEW PURCHASED DOCUMENTS

Profile Information

COMMUNICATIONS PREFERENCES

PROFESSION AND EDUCATION

TECHNICAL INTERESTS

Need Help?

US & CANADA: +1 800 678 4333

WORLDWIDE: +1 732 981 0060

CONTACT & SUPPORT

Follow



About IEEE *Xplore* | Contact Us | Help | Accessibility | Terms of Use | Nondiscrimination Policy | Sitemap | Privacy & Opting Out of Cookies

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

© Copyright 2020 IEEE - All rights reserved. Use of this web site signifies your agreement to the terms and conditions.

IEEE Account

» Change Username/Password

» Update Address

Purchase Details

» Payment Options

» Order History

» View Purchased Documents

Profile Information

» Communications Preferences

» Profession and Education

» Technical Interests

Need Help?

» **US & Canada:** +1 800 678 4333

» **Worldwide:** +1 732 981 0060

» Contact & Support

About IEEE *Xplore* | Contact Us | Help | Accessibility | Terms of Use | Nondiscrimination Policy | Sitemap | Privacy & Opting Out of Cookies

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

© Copyright 2020 IEEE - All rights reserved. Use of this web site signifies your agreement to the terms and conditions.

ATTACHMENT 6

Bibliography of Works Done on CAPTCHA

Sajad Shirali-Shahreza
Sharif University of Technology
Azadi Street, Tehran, IRAN
shirali@ce.sharif.edu

M.Hassan Shirali-Shahreza
Amirkabir University of Technology
Hafez Avenue, Tehran, IRAN
shahreza@shirali.ir

Abstract

Nowadays, a great amount of information is circulated through the Internet. Some of them exclusively belongs to a special group of users and requires protection and safeguarding against unauthorized access. To this end, a category of systems called HIP (Human Interactive Proof) have been introduced to distinguish between various groups of users.

CAPTCHA (Completely Automatic Public Turing Test to Tell Computer and Human Apart) methods are one of the important branches of HIP systems which are used to distinguish between human users and computer programs automatically. These methods are based on Artificial Intelligence (AI) topics. The goal of these systems is to ask questions which human users can easily answer but current computer programs cannot.

During past years, many researchers worked on HIP and CAPTCHA systems. In this paper, we try to collect different works which are done on HIP and CAPTCHA systems and create a complete bibliography of published works. We collect 87 published works and classify them into a number of categories. This paper contains different works which are done for creating CAPTCHA methods, attacking CAPTCHA methods and applications of CAPTCHA methods. We think that this paper can help new researchers in CAPTCHA domains to quickly find the works which are done previously.

1. Introduction

Many aspects of human life are affected by the expansion of the World-Wide Web (WWW). In particular, in developed countries, many daily affairs from daily shopping to education and commerce can be done using the Internet. A common action which is done in most websites, especially those belonging to commercial and administrative applications, is to fill out registration forms for certain purposes. After filling out the

forms by entering the required information, the individuals are allowed to login into that website and carry out certain jobs. Unfortunately, there are persons who abuse web services by writing programs which do automatic false registration in websites. These programs automatically fill out forms with incorrect information in order to enroll in the site. This wastes a large volume of the resources of the site in favor of the profit-seeking programmers and reduces the performance of the system.

Various methods have been presented in order to prevent such attacks, aiming at distinguishing human users from computer programs. The main characteristic of these methods is their automatism so that they can be implemented automatically by computers; because the examination of a large bulk of registrations on the Internet websites by human requires a great deal of time and expense and in some cases, such as email services websites, may even be practically impossible. Therefore, it is necessary to use automatic systems to distinguish human users from computer programs.

In artificial intelligence (AI), a test known as the Turing test [76] is proposed for proving the intelligence of a computer. In this test, a human person and a computer are put in two different rooms and a human interrogator in a third room asks them questions. If the interrogator cannot recognize which room the computer is in and which one the human, it is said that the computer has passed the Turing test. A similar method to the Turing test can be used to distinguish human users from computer programs with the difference that the human interrogator is replaced with a computer. The computer interrogator asks questions from the applicant to distinguish between the human user and the computer program. These methods are known as CAPTCHA (Completely Automated Public Turing test to tell Computers and Human Apart), after the CAPTCHA project which is done at Carnegie Mellon University [79]. Therefore, the main focus of these methods is on questions that the human user can easily answer but the present computer programs are hardly likely to be able to answer.

978-1-4244-2197-8/08/\$25.00 ©2008 IEEE

CAPTCHA methods can be generally divided into three groups: OCR-Based, Visual Non-OCR-Based and Non Visual. Optical Character Recognition (OCR) programs are used for automatically reading the texts, but they have difficulty reading texts printed with a low quality and can only recognize high-quality typed texts that use common standard formats. However, the defects of the OCR systems can be taken as an advantage by changing the picture of a word so that it can only be recognized by a human and not by any OCR system.

In OCR-Based methods, the image of a word with distortion and various pictorial effects is shown to the user and he must type that word. Due to presence of various pictorial effects, the computer will encounter problems in the recognition of the word and only a human user can recognize the word. We explain these methods in section 2.1. But these methods usually result in dissatisfaction of users. On the other hand, efforts have been made for breaking these methods such as [43]. In section 4 we discuss some of these attacks.

In contrast, we can talk about Visual Non-OCR-Based and Non Visual methods which are easier to pass for users than OCR-based ones. These methods are studied in sections 2.2 and 2.3. For example, in Collage CAPTCHA method [57], the image of some objects with distortion is shown to the user and he is asked to click on a certain object.

CAPTCHA systems are usually used to prevent fake registration by computer programs in websites, but can be applied to other applications such as anti spam applications. We explain these applications in section 3.

CAPTCHA is one of the important branches of HIP systems. HIP is the abbreviation of Human Interactive Proof and is used to call systems in which human users prove their membership in a special group through a challenge/response protocol. Some examples are: human versus machine, himself versus any other person, adult versus a child, etc [7]. Most of HIP works have been done in field of CAPTCHA and few works have been done in other fields of HIP such as distinguishing between a special group of users and other users. We also survey some of these HIP.

In this paper we try to collect different works which are done on CAPTCHA during past years. The main goal of this paper is to create a comprehensive bibliography of works done on CAPTCHA. Because of the lack of space, we only group similar works and describe the main ideas of some method.

In section 2 we will briefly survey the different CAPTCHA methods proposed. Then we will survey the applications of CAPTCHA methods in section 3. Section 4 contains attacks and analysis which are done on CAPTCHA methods. The last section is the conclusion.

2. CAPTCHA Methods

The method designed in AltaVista in 1997 is known as one of the first CAPTCHA methods [7].

von Ahn defined CAPTCHA method formally in [78]. Their CACM paper [79] is a brief description of methods created in the CAPTCHA project.

Baird had a survey of some the CAPTCHA methods in [2]. His paper in DAS 2002 workshop is one of the first papers which introduces the CAPTCHA problem [7]. His preface on the HIP 2005 workshop proceedings also describe the status of CAPTCHA methods at that time [5]. Another survey of CAPTCHA methods is [47]. All of these surveys are not broad and mention a small number of methods. So we think that a comprehensive survey on CAPTCHA methods is required.

2.1. OCR-Based Methods

Pessimal Print [4] is one of the first OCR-Based methods. Another early work on OCR-Based CAPTCHA methods is [83]. BaffleText [20] is another OCR-Based method which generate meaning less pronounceable words. ScatterType [6] is another method created by authors of BaffleText method. The authors of [9] discuss how to generate random words which are easier for human users. Another similar paper is [81]. The method which is currently used by Microsoft web services is described in [17, 16, 18, 19].

A special method for using in console applications is presented in [23]. Method [38] uses visual patterns as foreground and background for displaying the text which the user must type. Rusu proposed Handwritten CAPTCHA, which uses scanned handwritten words for generating CAPTCHA images [49]. The majority of works done on CAPTCHA are for English CAPTCHA methods. There are a few CAPTCHA methods for other languages such as [62, 85, 66, 65, 63].

2.2. Visual Non-OCR-Based Methods

In addition to OCR-Based methods, there are another visual methods which do not use OCR software weaknesses. These methods usually uses the drawbacks of computer vision systems such as their difficulties in identifying the type of a object in an image. PIX method is one of the first Non-OCR-Based methods. More information about PIX and EPS-Game which is used for creating the required image database can be found in [77]. Bongo which is another Non-OCR-Based method which is created in the CMU CAPTCHA project is described in [12] in 2001.

The authors of [24], who are working on Content Based Image Retrieval (CBIR) systems, proposed a method which uses the problems of CBIR methods. Another examples of Non-OCR-Based methods which are based on object recognition are [26, 57].

The method presented in [31] uses the idea of rendering 3D scenes for creating CAPTCHA images instead of using a bank of images. The idea of method [39] is to exchange a number of blocks in an image and ask the user to click on that blocks. ARTiFACIAL is a method developed at Microsoft research and ask the user to found the complete human face among a number of imperfect faces [48]. A number of Non-OCR-Based methods are described in [3] such as the method which asks the user to click on a certain object in an image. Similar methods are proposed in [21].

Most of visual Non-OCR-Based methods require a database of labeled images. Creating a database of labeled images is costly and time consuming. An approach for solving this problem is creating games such as EPS-Game [77]. Another idea is using image search engines for this purpose [58, 53].

Movies can also be used instead of images in the CAPTCHA methods. In [1] an animated CAPTCHA method is proposed. Another method which uses small movies is [61]. The face recognition method proposed in [41] asked the user to match the two face images which are similar in a set of images.

A hybrid method which has both OCR-Based and Non-OCR-Based parts is described in [40]. CAPTCHA methods are usually designed for using with computers and are not suitable for other devices such as mobile phones and PDAs. A number of methods are designed especially for devices such as mobile phones [52, 54].

2.3. Non Visual Methods

One of the main categories of non visual methods are sound based CAPTCHA methods such as [35, 14]. In these methods, a word is said and the user must type the word. These systems are usually used beside other CAPTCHA methods, especially OCR-Based methods, for disabled people.

CAPTCHA in text domain was desired from the beginning, but there are few works done in this field including [10, 82]. As the authors of these paper said, it seems that designing a Text Domain CAPTCHA is very difficult. A new type of CAPTCHA methods are proposed in [22] in which there is no specific answer to the question asked from the user.

Disabled people usually have problems with CAPTCHA methods, because most of CAPTCHA methods are designed for and tested by normal persons

(e.g. see the test group description in [18]). So special methods can be designed for disabled persons or persons with special needs such as [56, 64, 69, 70].

Another group of methods uses questions which need reasoning to be answered such as [60]. This idea can be extended to create HIP systems which can distinguish between different groups of people, such as method explained in [72].

3. Applications

CAPTCHA methods were originally designed to prevent spammers from registering free accounts in the free email services [7]. But they are used in a number of methods to prevent email spam sending or identifying spammers such as [34, 68]. In addition to email spam problem, CAPTCHA methods are used for other types of spams such as [30, 51].

Another main application of CAPTCHA methods is in bot detection. Bots are computer programs which simulate human behaviours. CAPTCHA methods are used in different applications to identify bots. These methods identify bots to ban them from using services such as [28, 86] or to block them in automated attacks such as Denial of Service (DoS) attacks [32, 33].

Spammers are also using CAPTCHA techniques for sending undetectable spams [37]. A method is proposed for filtering this type of spams in [11]. CAPTCHA methods are widely used to block brute-force attacks in different applications such as [13, 71, 55, 45, 74, 84]. They are also used for detecting Phishing attacks [15, 25, 50]. Other special applications are [73, 27, 67, 59]. Most of these applications try to improve the security.

4. Attacks and Analysis

One of the first and well known attacks to CAPTCHA methods (Gimpy method) is [43]. Another attacks on Gimpy method are [44, 75, 42]. In [46] authors described two attacks on two OCR-Based CAPTCHA methods and discuss about the security which CAPTCHA methods can provide. A more recent attacks on OCR-Based CAPTCHA methods are reported in [87]. A series of in depth works on analysis of CAPTCHA methods are done in Microsoft Research labs. In [16] they show that computers are more successful in some parts of solving OCR-Based CAPTCHA methods. They also report their result on attacking a number of OCR-Based methods which are used in websites such as Yahoo and Google in [19].

Reference [78] have a formal definition of CAPTCHA methods and further analysis. Another paper which analyses the limits and security of

CAPTCHA method is [8]. There are another papers which analyse the CAPTCHA systems and their efficiency such as [36, 80]. There is a detailed discussion on the spam problem and using CAPTCHA methods to stop spams in [29].

5. Conclusion

CAPTCHA systems are used to distinguish between human users and computer programs. Today they are used widely in web servcies to offer better services to human users. In this paper we collect a great part of the works done on CAPTCHA during last year. It includes different methods designed, applications of CAPTCHA methods and analysis done on robustness of CAPTCHA methods to attacks. We hope that this paper can assist the researchers who works on the CAPTCHA methods to find previous works done in this field.

Most of the works which done in design and analysis of HIP was focused on CAPTCHA systems, which aim at distinguishing between human users and computers programs. But other fields of HIP have potential uses. A few works have been done in proofing membership in a special group [72]. But we did not find any work on distinguishing children from adults, which is needed in sites which are for adults only. We think that other areas of HIP systems are open fields for further researches and during next years, we will see practical systems for them, such as systems which can distinguish between child users and adults.

References

- [1] E. Athanasopoulos and S. Antonatos. Enhanced CAPTCHAs: Using animation to tell humans and computers apart. *Proc. of 10th Int. Conf. on Communications and Multimedia Security (CMS 2006)*, vol. 4237 of LNCS, pp. 97–108, October 2006.
- [2] H. S. Baird. *Data Complexity in Pattern Recognition*, chapter in Complex Image Recognition and Web Security. Springer, 2006.
- [3] H. S. Baird and J. L. Bentley. Implicit CAPTCHAs. *Proc. of SPIE-IS&T Electronic Imaging, Document Recognition and Retrieval XII*, vol. 5676 of SPIE Proceedings, pp. 191–196, January 2005.
- [4] H. S. Baird, A. L. Coates, and R. J. Fateman. Pessimprint: a reverse turing test. *International Journal on Document Analysis and Recognition (IJ DAR)*, 5(2–3):158–163, April 2003.
- [5] H. S. Baird and D. P. Lopresti. Second international workshop on human interactive proofs - preface. *Proc. of 2nd Int. Workshop on Human Interactive Proofs (HIP 2005)*, vol. 3517 of LNCS, May 2005.
- [6] H. S. Baird, M. A. Moll, and S.-Y. Wang. Scattertype: A legible but hard-to-segment CAPTCHA. *Proc. of 8th Int. Conf. on Document Analysis and Recognition (ICDAR 05)*, vol. 2, pp. 935–939, August–September 2005.
- [7] H. S. Baird and K. Popat. Human interactive proofs and document image analysis. *Proc. of 5th IAPR Int. Workshop on Document Analysis Systems (DAS 2002)*, vol. 2423 of LNCS, pp. 507–518, 2002.
- [8] J. Bentley and C. Mallows. How much assurance does a PIN provide? *Proc. of 2nd Int. Workshop on Human Interactive Proofs (HIP 2005)*, vol. 3517 of LNCS, pp. 111–126, May 2005.
- [9] J. Bentley and C. Mallows. CAPTCHA challenge strings: problems and improvements. *Proceedings of 18th SPIE-IS&T Electronic Imaging, Document Recognition and Retrieval XIII*, vol. 6067 of SPIE Proceedings, January 2006.
- [10] R. Bergmair and S. Katzenbeisser. Towards human interactive proofs in the text-domain: Using the problem of sense-ambiguity for security. *Proc. of 7th Int. Information Security Conference (ISC 2004)*, vol. 3225 of LNCS, pp. 257–267, September 2004.
- [11] B. Biggio, G. Fumera, I. Pillai, and F. Roli. Image spam filtering using visual information. *Proc. of 14th Int. Conf. on Image Analysis and Processing (ICIAP 2007)*, pp. 105–110, September 2007.
- [12] D. Blank. A practical turing test for detecting adbots. *Intelligence*, 12(4):6, October 2001.
- [13] S. Chakrabarti and M. Singhal. Password-based authentication: Preventing dictionary attacks. *Computer*, 40(6):68–74, June 2007.
- [14] T.-Y. Chan. Using a text-to-speech synthesizer to generate a reverse Turing test. *Proc. of 15th IEEE Int. Conf. on Tools with Artificial Intelligence (ICTAI 03)*, pp. 226–232, November 2003.
- [15] M. Chandrasekaran, R. Chinchani, and S. Upadhyaya. PHONEY: Mimicking user response to detect phishing attacks. *Proc. of 2006 Int. Symposium on on World of Wireless, Mobile and Multimedia Networks (WOW-MOM '06)*, pp. 668–672, June 2006.
- [16] K. Chellapilla, K. Larson, P. Simard, and M. Czerwinski. Computers beat humans at single character recognition in reading based human interaction proofs (HIPs). *Proc. of 2nd Conf. on Email and Anti-Spam*, July 2005.
- [17] K. Chellapilla, K. Larson, P. Simard, and M. Czerwinski. Designing human friendly human interaction proofs (HIPs). *Proc. of SIGCHI Conf. on Human factors in computing systems (CHI 05)*, pp. 711–720, April 2005.
- [18] K. Chellapilla, K. Larson, P. Y. Simard, and M. Czerwinski. Building segmentation based human-friendly human interaction proofs (HIPs). *Proc. of 2nd Int. Workshop on Human Interactive Proofs (HIP 2005)*, vol. 3517 of LNCS, pp. 1–26, May 2005.
- [19] K. Chellapilla and P. Simard. Using machine learning to break visual human interaction proofs (HIPs). *Advances in Neural Information Processing Systems*, Dec. 2004.
- [20] M. Chew and H. S. Baird. Baffletext: A human interactive proof. *Proc. of SPIE-IS&T Electronic Imaging, Document Recognition and Retrieval X*, vol. 5010 of Proceedings of SPIE, pp. 305–316, January 2003.

- [21] M. Chew and J. Tygar. Image recognition CAPTCHAs. Technical Report UCB/CSD-04-1333, Computer Science Division, UC Berkeley, USA, June 2004.
- [22] M. Chew and J. Tygar. Collaborative filtering CAPTCHAs. *Proc. of 2nd Int. Workshop on Human Interactive Proofs (HIP 2005)*, vol. 3517 of *Lecture Notes in Computer Science*, pp. 66–81, May 2005.
- [23] M. Dailey and C. Namprempre. A text-graphics character CAPTCHA for password authentication. *Proc. of 2004 IEEE Region 10 Conference (TENCON 2004)*, vol. 2, pp. 45–48, November 2004.
- [24] R. Datta, J. Li, and J. Z. Wang. IMAGINATION: a robust image-based CAPTCHA generation system. *Proc. of 13th ACM Int. Conf. on Multimedia (MULTIMEDIA 05)*, pp. 331–334, November 2005.
- [25] R. Dhamija and J. D. Tygar. Phish and HIPs : Human interactive proofs to detect phishing attacks. *Proc. of 2nd Int. Workshop on Human Interactive Proofs (HIP 2005)*, vol. 3517 of *LNCS*, pp. 127–141, May 2005.
- [26] J. Elson, J. R. Douceur, J. Howell, and J. Saul. ASIRRA: a CAPTCHA that exploits interest-aligned manual image categorization. *Proc. of 14th ACM Conf. on Computer and Communications Security (CCS 2007)*, pp. 366–374, October – November 2007.
- [27] I. Fischer and T. Herfet. Visual CAPTCHAs for document authentication. *Proc. of 8th Workshop on Multimedia Signal Processing*, pp. 471–474, October 2006.
- [28] P. Golle and N. Ducheneaut. Preventing bots from playing online games. *Comput. Entertain.*, 3(3):3, 2005.
- [29] J. Goodman and R. Rounthwaite. Stopping outgoing spam. *Proc. of 5th ACM Conf. on Electronic commerce (EC '04)*, pp. 30–39, May 2004.
- [30] P. He, Y. Sun, W. Zheng, and X. Wen. Filtering short message spam of group sending using captcha. *Proc. of Int. Workshop on Knowledge Discovery and Data Mining (WKDD 2008)*, pp. 558–561, January 2008.
- [31] M. E. Hoque, D. J. Russomanno, and M. Yeasin. 2d captchas from 3d models. *Proc. of IEEE SoutheastCon 2006*, pp. 165–170, March–April 2006.
- [32] S. Kandula, D. Katabi, M. Jacob, and A. Berger. Botz-4-sale: surviving organized ddos attacks that mimic flash crowds. *Proc. of 2nd Symposium on Networked Systems Design & Implementation*, pp. 287–300, May 2005.
- [33] R. P. Karrer. Ec: an edge-based architecture against ddos attacks and malware spread. *Proc. of 20th Int. Conf. on Advanced Information Networking and Applications (AINA'06)*, pp. 49–56, April 2006.
- [34] E. J. Kartaltepe and S. Xu. Towards blocking outgoing malicious impostor emails. *Proc. of 2006 International Symposium on World of Wireless, Mobile and Multimedia Networks (WOWMOM 06)*, pp. 657–661, June 2006.
- [35] G. Kochanski, D. Lopresti, and C. Shih. A reverse turing test using speech. *Proc. of 7th Int. Conf. on Spoken Language Processing*, pp. 1357–1360, September 2002.
- [36] A. Kolupaev and J. Ogijenko. CAPTCHAs: Humans vs. bots. *IEEE Security & Privacy*, 6(1):68–70, Jan. 2008.
- [37] N. Leavitt. Vendors fight spam's sudden rise. *Computer*, 40(3):16–19, March 2007.
- [38] W. Liao and C. Chang. Embedding information within dynamic visual patterns. *Proc. of 2004 Int. Conf. on Multimedia and Expo*, vol. 2, pp. 895–898, June 2004.
- [39] W.-H. Liao. A CAPTCHA mechanism by exchange image blocks. *Proc. of 18th Int. Conf. on Pattern Recognition (ICPR 06)*, pp. 1179–1183, August 2006.
- [40] D. Lopresti. Leveraging the CAPTCHA problem. *Proc. of 2nd Int. Workshop on Human Interactive Proofs (HIP 2005)*, vol. 3517 of *Lecture Notes in Computer Science*, pp. 97–110, May 2005.
- [41] D. Misra and K. Gaj. Face recognition CAPTCHAs. *Proc. of Advanced Int. Conf. on Telecommunications and Int. Conf. on Internet and Web Applications and Services (AICT-ICIW 06)*, p. 122, 2006.
- [42] G. Mori, S. Belongie, and J. Malik. Efficient shape matching using shape contexts. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 27(11):1832–1837, November 2005.
- [43] G. Mori and J. Malik. Recognizing objects in adversarial clutter: Breaking a visual CAPTCHA. *Proc. of 2003 IEEE Conf. on Computer Vision and Pattern Recognition (CVPR 03)*, vol. 1, pp. 134–141, June 2003.
- [44] G. Moy, N. Jones, C. Harkless, and R. Potter. Distortion estimation techniques in solving visual CAPTCHAs. *Proc. of 2004 IEEE Conf. on Computer Vision and Pattern Recognition*, vol. 2, pp. 23–28, June–July 2004.
- [45] B. Pinkas and T. Sander. Securing passwords against dictionary attacks. *Proc. of 9th Conf. on Computer and Communications Security*, pp. 161–170, Nov. 2002.
- [46] M. Ponc. Visual reverse turing tests: A false sense of security. *Proc. of 2006 IEEE Workshop on Information Assurance*, pp. 305–311, June 2006.
- [47] C. Pope and K. Kaur. Is it human or computer? defending e-commerce with captchas. *IT Professional*, 7(2):43–49, March 2005.
- [48] Y. Rui and Z. Liu. ARTIFACIAL: Automated reverse turing test using facial features. Technical Report MSR-TR-2003-48, Microsoft, April 2003.
- [49] A. Rusu. *Exploiting the Gap in Human and Machine Abilities in Handwriting Recognition for Web Security Applications*. PhD thesis, Dept. of Comp. Sci. and Eng., University of New York at Buffalo, USA, August 2006.
- [50] S. Saklikar and S. Saha. Public key-embedded graphic CAPTCHAs. *Proc. of 5th Consumer Communications and Networking Conference*, pp. 262–266, Jan. 2008.
- [51] M. Shirali-Shahreza. Verifying spam SMS by Arabic CAPTCHA. *Proc. of 2nd IEEE Int. Conf. on Information and Communication Technologies: From Theory to Applications (ICTTA 06)*, vol. 1, pp. 78–83, April 2006.
- [52] M. Shirali-Shahreza. Highlighting CAPTCHA. *Proc. of the Conf. on Human System Interaction (HSI 2008)*, pp. 247–250, May 2008.
- [53] M. Shirali-Shahreza and M. H. Shirali-Shahreza. Online PIX CAPTCHA. *Proc. of IEEE Int. Conf. on Signal Processing, Communications and Networking (IC-SCN 2008)*, pp. 582–585, January 2008.
- [54] M. Shirali-Shahreza and S. Shirali-Shahreza. Drawing CAPTCHA. *Proc. of 28th Int. Conf. Information Technology Interfaces (ITI 2006)*, pp. 475–480, June 2006.

- [55] M. Shirali-Shahreza and S. Shirali-Shahreza. Preventing mobile software cracking using CAPTCHA. *Proc. of IEEE Int. Conf. on Innovations in Information Technology 2006 (IIT 2006)*, p. 128, November 2006.
- [56] M. Shirali-Shahreza and S. Shirali-Shahreza. CAPTCHA for blind people. *Proc. of 7th IEEE Int. Symposium on Signal Processing and Information Technology (ISSPIT 2007)*, pp. 995–998, Dec. 2007.
- [57] M. Shirali-Shahreza and S. Shirali-Shahreza. Collage CAPTCHA. *Proc. of 20th IEEE Int. Symposium Signal Processing and Application (ISSPA 2007)*, Feb. 2007.
- [58] M. Shirali-Shahreza and S. Shirali-Shahreza. Online collage CAPTCHA. *Proc. of 8th Int. Workshop on Image Analysis for Multimedia Interactive Services (WIAMIS 2007)*, p. 58, June 2007.
- [59] M. Shirali-Shahreza and S. Shirali-Shahreza. Passwordless login system for mobile phones using CAPTCHA. *Proc. of 49th Int. Symposium ELMAR-2007*, pp. 243–246, September 2007.
- [60] M. Shirali-Shahreza and S. Shirali-Shahreza. Question-based CAPTCHA. *Proc. of Int. Conf. on Computational Intelligence and Multimedia Applications (IC-CIMA 2007)*, vol. 4, pp. 54–58, December 2007.
- [61] M. Shirali-Shahreza and S. Shirali-Shahreza. Motion CAPTCHA. *Proc. of Conf. on Human System Interaction (HSI 2008)*, pp. 1042–1044, May 2008.
- [62] M. H. Shirali-Shahreza and M. Shirali-Shahreza. Persian/Arabic Baffletext CAPTCHA. *Journal of Universal Computer Science*, 12(12):1783–1796, Dec. 2006.
- [63] M. H. Shirali-shahreza and M. Shirali-shahreza. Persian/Arabic CAPTCHA. *IADIS International Journal on Computer Science and Information Systems (IJCSIS)*, 1(2):63–75, October 2006.
- [64] M. H. Shirali-Shahreza and M. Shirali-Shahreza. Localized CAPTCHA for illiterate people. *Proc. of Int. Conf. on Intelligent & Advanced Systems*, November 2007.
- [65] M. H. Shirali-Shahreza and M. Shirali-Shahreza. Multilingual CAPTCHA. *Proc. of 5th Int. Conf. on Computational Cybernetics*, pp. 135–139, October 2007.
- [66] M. H. Shirali-Shahreza and M. Shirali-Shahreza. Nastaliq CAPTCHA. *Iranian Journal of Electrical and Computer Engineering (IJECE)*, 5(2):109–114, 2007.
- [67] M. H. Shirali-Shahreza and M. Shirali-Shahreza. New solution for password key transferring in steganography methods. *Proc. of Int. Conf. on Computational Intelligence and Multimedia Applications (ICCIMA 2007)*, vol. 4, pp. 123–125, December 2007.
- [68] S. Shirali-Shahreza and A. Movaghar. A new anti-spam protocol using CAPTCHA. *Proc. of 2007 Int. Conf. Networking, Sensing and Control*, pp. 234–238, Apr. 2007.
- [69] S. Shirali-Shahreza and M. Shirali-Shahreza. CAPTCHA for children. *Proc. of 3rd Int. Conf. on System of Systems Engineering*, June 2008.
- [70] S. Shirali-Shahreza and M. Shirali-Shahreza. A new human interactive proofs system for deaf persons. *Proc. of 5th Int. Conf. on Information Technology: New Generations (ITNG 2008)*, pp. 807–810, April 2008.
- [71] S. Shirali-Shahreza, M. Shirali-Shahreza, and M. T. Manzuri-Shalmani. Easy and secure login by CAPTCHA. *International Reviews on Computers and Software (IReCoS)*, 2(4):393–400, July 2007.
- [72] S. Shirali-Shahreza, M. Shirali-Shahreza, and A. Movaghar. Exam HIP. *Proc. of 2007 IEEE Int. Workshop on Anti-counterfeiting, Security, Identification (ASID 2007)*, pp. 415–418, April 2007.
- [73] S. Shirali-Shahreza, M. Shirali-Shahreza, and A. Movaghar. Restricted access to exam grades on the web by HIP. *Proc. of 1st IEEE Int. Workshop on e-Activity (IEEE-IWEA2007)*, pp. 967–971, July 2007.
- [74] M. Szydłowski, C. Kruegel, and E. Kirda. Secure input for web applications. *Proc. of 23rd Annual Computer Security Applications Conference (ACSAC 2007)*, pp. 375–384, December 2007.
- [75] A. Thayananthan, B. Stenger, P. Torr, and R. Cipolla. Shape context and chamfer matching in cluttered scenes. *Proc. of 2003 Conf. on Computer Vision and Pattern Recognition*, vol. 1, pp. 127–133, June 2003.
- [76] A. M. Turing. Computing machinery and intelligence. *Mind*, 59(236):433–460, 1950.
- [77] L. von Ahn. *Human Computation*. PhD thesis, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA, USA, December 2005.
- [78] L. von Ahn, M. Blum, N. J. Hopper, and J. Langford. CAPTCHA: Using hard AI problems for security. *Proc. of Int. Conf. on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2003)*, vol. 2656 of LNCS, pp. 294–311, May 2003.
- [79] L. von Ahn, M. Blum, and J. Langford. Telling humans and computers apart automatically. *Communications of the ACM*, 47(2):56–60, February 2004.
- [80] D. Voth. The paradox of CAPTCHAs. *IEEE Intelligent Systems*, 18(2):6–7, March–April 2003.
- [81] S.-Y. Wang and J. L. Bentley. CAPTCHA challenge tradeoffs: Familiarity of strings versus degradation of images. *Proc. of 18th Int. Conf. on Pattern Recognition (ICPR 06)*, pp. 164–167, August 2006.
- [82] P. Ximenes, A. dos Santos, M. Fernandez, and J. Celestino. A CAPTCHA in the text domain. *Proc. of Workshops On the Move to Meaningful Internet Systems 2006 (OTM 2006)*, vol. 4277 of LNCS, pp. 605–615, October–November 2006.
- [83] J. Xu, I. A. Essa, and R. J. Lipton. Hello, are you human? Technical Report GIT-CC-00-28, Georgia Institute of Technology, November 2000.
- [84] J. Xu, R. Lipton, I. Essa, M. Sung, and Y. Zhu. Mandatory human participation: a new authentication scheme for building secure systems. *Proc. of 12th Int. Conf. on Computer Communications and Networks (ICCCN 2003)*, pp. 547–552, October 2003.
- [85] S. Xu, F. C. M. Lau, W. K. Cheung, and Y. Pan. Automatic generation of artistic chinese calligraphy. *IEEE Intelligent Systems*, 20(3):32–39, May 2005.
- [86] R. V. Yampolskiy. Detecting and controlling cheating in online poker. *Proc. of 5th Consumer Communications and Networking Conference*, pp. 848–853, Jan. 2008.
- [87] J. Yan and A. S. E. Ahmad. Breaking visual CAPTCHAs with naive pattern recognition algorithms. *Proc. of 23rd Annual Computer Security Applications Conference (ACSAC 2007)*, pp. 279–291, Dec. 2007.

ATTACHMENT 7

```

leader 00955cam a2200277 a 4500
001 991000901079704436
008 061020s2005      paau      bm      000 0 eng d
035 ##$a1025961-olcmu_inst
100 1#$aVon Ahn, Luis.
245 10$aHuman Computation / $cLuis von Ahn.
260 ##$aPittsburgh, PA : $b Carnegie Mellon University, $c2005.
300 ##$a87 p. : $bill. ; $c 29cm.
502 ##$aThesis (Ph.D.) -- Carnegie Mellon University, 2005.
504 ##$aIncludes bibliographical references (p. 83-87).
596 ##$a9
610 20$aCarnegie Mellon University $xDissertations.
700 1#$aBlum, Manuel, $eadvisor.
710 2$aCarnegie Mellon University. $b Dept. of Computer Science.
902 ##$a1025961
903 ##$aa1025961
916 ##$a20061020
917 ##$a20061020
918 ##$aCATALOGER
919 ##$a20170314
920 ##$aCATALOGER
927 ##$aNone
999 ##$aTHESIS VON,HUMA PH.D $wALPHANUM $cl $iF097061 $dd10/8/2009 $e9/27/2009 $lBY-REQUEST $mOFFSITE $n1 $rY $sY $tTHESIS $u10/20/2006 FORM=MARC

```

ATTACHMENT 8

ProQuest Dissertations & Theses A&I

Preview Available | Dissertations & Theses

Human computation

von Ahn, Luis.Carnegie Mellon University, ProQuest Dissertations Publishing, 2005. 3205378.


PDF


Order a copy


Cite


Email


All Options

Abstract

Tasks like image recognition are trivial for humans, but continue to challenge even the most sophisticated computer programs. This thesis introduces a paradigm for utilizing human processing power to solve problems that computers cannot yet solve. Traditional approaches to solving such problems focus on improving software. I advocate a novel approach: constructively channel human brainpower using computer games. For example, the ESP Game, introduced in this thesis, is an enjoyable online game—many people play over 40 hours a week—and when people play, they help label images on the Web with descriptive keywords. These keywords can be used to significantly improve the accuracy of image search. People play the game not because they want to help, but because they enjoy it.

I introduce three other examples of "games with a purpose": Peekaboom, which helps determine the location
More

Details

Subject	Computer science; Artificial intelligence
Classification	0984: Computer science 0800: Artificial intelligence
Identifier / keyword	Applied sciences; CAPTCHA; ESP game; Human computation; Peekaboom
Title	Human computation
Author	von Ahn, Luis
Number of pages	87
Publication year	2005
	2005

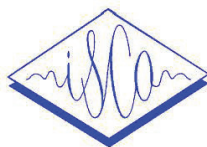
Degree date	
School code	0041
Source	DAI-B 67/02, Dissertation Abstracts International
Place of publication	Ann Arbor
Country of publication	United States
ISBN	978-0-542-54148-3
Advisor	Blum, Manuel
University/institution	Carnegie Mellon University
University location	United States -- Pennsylvania
Degree	Ph.D.
Source type	Dissertations & Theses
Language	English
Document type	Dissertation/Thesis
Dissertation/thesis number	3205378
ProQuest document ID	305006687
Document URL	http://libproxy.unl.edu/login?url=https://www-proquest-com.libproxy.unl.edu/docview/305006687?accountid=8116
Copyright	Database copyright ProQuest LLC; ProQuest does not claim copyright in the individual underlying works.
Database	ProQuest Dissertations & Theses A&I



Ask a Question

The University of Nebraska-Lincoln

ATTACHMENT 9



A REVERSE TURING TEST USING SPEECH

Greg Kochanski, Daniel Lopresti, and Chilin Shih

Bell Laboratories, Lucent Technologies
{gpk,dpl,cls}@research.bell-labs.com, 600 Mountain Ave, Murray Hill, NJ 07974

ABSTRACT

“Hackers” have written malicious programs to exploit on-line services intended for human users. As a result, service providers need a method to tell whether a web site is being accessed by a human or a machine. We expect a parallel scenario as spoken language interfaces become common.

In this paper, we describe a *Reverse Turing Test* (i.e., an algorithm that can distinguish between humans and computers) using speech. We present a test that depends on the fact that human recognition of distorted speech is far more robust than automatic speech recognition techniques.

Our analysis of 18 different sets of distortions demonstrates that there are a variety of ways to make the problem hard for machines. In addition, humans and speech recognition systems make different kinds of mistakes, and this difference can be employed to improve discrimination.

1. INTRODUCTION

The use of the Internet as a means for distributing valuable information and content have also made it an attractive target for “hackers.” Attacks involving malicious programs (“bots”) that attempt to exploit online services intended for human users are already common. These programs consume resources, harass users, make attempts to guess passwords, steal and re-purpose copyrighted content, and invade privacy by reconstructing sensitive data from public views.

As a result, there is a need for automatic methods to tell whether the entity attempting to access a service is a human or a machine. This has come to be known as a *Reverse Turing Test*, or *RTT* (or sometimes a *Human Interactive Proof*). Unlike the test originally proposed by Alan Turing [1], a Reverse Turing Test is administered by a computer, not a human. For the test to be considered effective, humans should be able to pass it with ease, but machines should have a low probability of passing.

While it may seem that passwords and/or biometrics could provide a solution, one must keep in mind that these approaches require pre-registration. An RTT will work even if the user is anonymous and has never used the service before. The RTT problem is fundamentally different from validating a known user. Indeed, a Reverse Turing Test should

be applied before authentication to prevent automated attacks on passwords.

Coates, Baird, and Fateman [2], and von Ahn *et al.* [3] have developed such a test based on a visual perception task. Their ideas are based on the observation that optical character recognition (OCR) systems are not as adept at reading degraded word images as humans are. That RTT is now used commercially to protect a free email service [4].

Speech-based services are proliferating because of their ease-of-use, portability, and potential for hands-free operation. Building a “bot” to navigate a spoken language interface is a tractable problem, especially if there is a fixed sequence of predefined prompts. Hence, we anticipate attacks on such systems and a similar need to prevent machines from abusing speech-based resources intended for human users. Previous work on speech RTTs can be found in [5, 6].

As in the vision RTTs, we exploit the fact that certain pattern recognition tasks are significantly harder for machines than they are for humans. We will use text-to-speech synthesis (TTS) to generate tests, and make use of the limitations of state-of-the-art automatic speech recognition (ASR) technology. (We require only that RTTs cannot be broken cheaply or rapidly. Clearly, any RTT can be broken by hiring a human.)

In this paper, we present the core of a spoken language RTT. We assume a user with a cell phone; the test may consist of having the system speak: “Please enter the following digits on your keypad: ...” followed by a short, random digit string. The speech would be synthesized in a way that ASR is likely to fail the test, e.g., by distorting the signal or adding “difficult” background noise to it after synthesis.

2. PROCEDURES

We designed a set of 18 RTTs based on different distortions of a speech signal (Table 2) to explore a broad range of possibilities. To test our RTTs, we synthesized 200 random 5-digit sequences using the Bell Labs English text-to-speech system [7], with the default male voice. We next distorted the signals and ran the Bell Labs speech recognition system [8] on them, with a grammar that allowed any digit se-

Name	Description	Error Ratio
<i>white</i>	• White Gaussian noise, 4000 Hz bandwidth.	15
<i>buzz</i>	• Sine waves at 700 Hz, 2100 Hz, 3500 Hz.	≥ 20
<i>song</i>	• Bell Labs Song (pop/rock).	> 15
<i>chopin</i>	• Chopin Polonaise for Piano No. 6, Op. 53.	> 20
<i>chant</i>	• Gregorian chant.	> 20
<i>female</i>	• Three overlapping instances of a female voice reading numbers.	> 20
<i>pow</i>	• 10 ms bursts of white Gaussian noise, repeated every 100 ms.	> 20
<i>rnoise</i>	• Every 100 ms, a section of the signal is replaced by white noise of the same RMS amplitude.	> 20
<i>cell</i>	• For each 30 ms window, decide if the data was lost. If so, and previous not lost, duplicate previous. If so, and previous is lost, set to zero. Simulates a bad cell phone channel.	> 10
<i>echo</i>	• Three echoes.	> 20
<i>filter</i>	• A random zero-phase filter.	> 5
<i>distort</i>	• Apply AGC on a 60 ms window, raise to a power, multiply by original amplitude.	≥ 20
<i>mx</i>	• <i>rnoise</i> + <i>chopin</i>	> 20
<i>mb</i>	• <i>song</i> + <i>echo</i>	> 20
<i>mc</i>	• <i>white</i> + <i>pow</i>	≥ 20
<i>md</i>	• <i>female</i> + <i>buzz</i>	≥ 5
<i>me</i>	• <i>rnoise</i> + <i>distort</i>	≥ 20
<i>mf</i>	• <i>filter</i> + <i>distort</i>	3

Table 1. Tested RTTs. The error ratio is an estimate of the largest ratio of the ASR to human utterance error rates. The components of all mixtures were chosen to cause equal error rates for ASR utterance error rates near 85%.

quence.

The recognition results were compared to the original digit sequences using approximate string matching ([9] and references therein) to identify added, missing, and substituted digits. From this we obtained, for each distortion, per-digit and per-utterance error rates, as well as a confusion matrix showing the frequency of each type of error.

A similar procedure was followed to test how well humans could recognize the signals. The authors each listened to 10 randomly-chosen digit sequences for each type of distortion. In these tests, the audio signals were presented twice with a one second pause in between. The subject then typed his/her interpretation and pressed return to listen to the next signal. The tests began at the most severe distortion of each type, and terminated when the subject correctly identified all 10 sequences. One set (*white*) received 67 repetitions per person for a more accurate confusion matrix.

The confusion matrices are scaled to make all diagonal confusion matrices identical. This step is necessary because the distance between raw confusion matrices is generally nonzero, even if there are no errors (*i.e.* the matrices are diagonal). This happens because we do not explicitly balance

the frequencies of each digit, so that one test may see more instances of, say, “3” than another. Hence, we use a scaled confusion matrix, $S = P \cdot C \cdot Q$, where P and Q are diagonal matrices chosen so that the row- and column-sums of S are unity. While deletions and insertions are conventionally placed in the same matrix as substitutions they are actually a fundamentally different kind of error. Specifically, $C_{del,ins}$ is on the diagonal and is missing (zero). Thus, insertions and deletions must be treated differently in the scaling. We make an ad-hoc modification to C before scaling: we set $C_{del,ins} = \sum_{i,j} C_{i,j}/N$ (where $N = 11$ is the number of rows and columns in C), and then set $S_{del,ins} = 0$.

3. ANALYSIS: IS IT POSSIBLE TO DISTINGUISH HUMANS FROM MACHINES?

Human perception of speech in noisy environments is fairly robust. Normal-hearing listeners need a signal-to-noise ratio (SNR) of approximately 1.5 dB to recognize speech [10], while ASR systems require a much more favorable SNR of 5 to 15 dB [11]. Our test results show an even wider gap between human and ASR performance.

Figures 1-4 plot the error rates we measured in four experiments; these correspond to four distinct types of distortion: additive noise, deleting segments of the speech, adding echoes and filtering the signal. The four curves in each chart represent the error rates for ASR on a per-utterance (square) and per-symbol (diamond) basis along with per-utterance (X) and per-symbol (triangle) rates for humans.

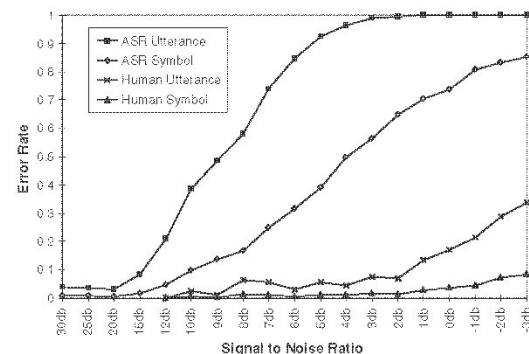


Fig. 1. Results for white noise experiment (*white*).

In figure 1, *white* is simply additive white noise. The x-axis shows SNR, and the y-axis represents the rate of recognition errors. In the ASR curves, each datum represents scores from 200 utterances or 1,000 digits, while in the human curves, each datum represents 201 utterances or 1,005 digits as pooled from the three listeners. ASR performance starts deteriorating when the SNR reaches 15 dB, and breaks down completely by 3 dB. Human performance is only starting to deteriorate at 0 dB SNR.

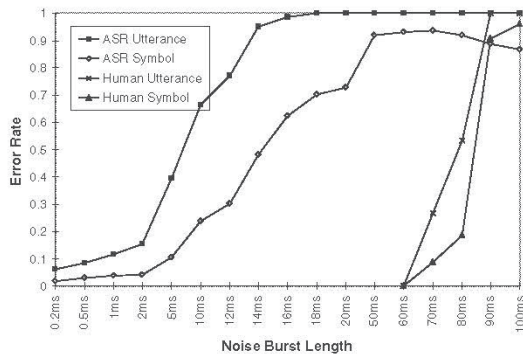


Fig. 2. Results for replacement noise experiment (*noise*).

Figure 2 shows the results for *noise*, which replaces a segment of speech with white noise every 100 ms, as we vary the length of the replaced segment. Human scores in this figure and in Figures 3-4 are based on 30 utterances (150 digits) per datum. As can be seen, ASR starts having problems when 2 ms (2%) of the speech is replaced. Amazingly, human recognition remains perfect at 60 ms (60% replacement), and 80% of the symbols are still correct even when 80% of the speech is missing.

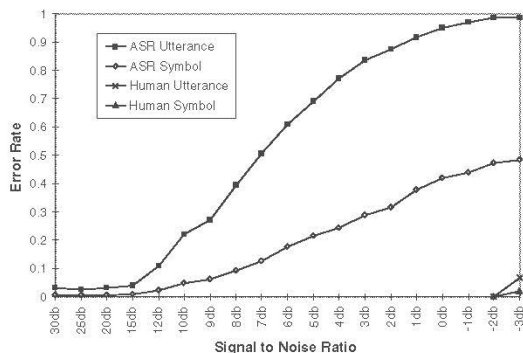


Fig. 3. Results for echo experiment (*echo*).

Our results for *echo*, which adds three echoes to the speech with delays of 60, 132, and 192 ms, are presented in Figure 3. The horizontal axis shows the relative amplitude of the first echo to the speech, while later echoes are 5 dB and 10 dB quieter. ASR performance starts declining when the SNR is 12 dB, while human performance is perfect until -3 dB. This behavior is typical of many of the other tests we performed.

Among our tests, *filter* (Figure 4) showed the smallest difference between ASR and humans. This is a zero-phase frequency domain filter, with a frequency response chosen randomly every 30 Hz. The control parameter sets the standard deviation of the gain, expressed in dB.

Our findings are that the gap between ASR and human

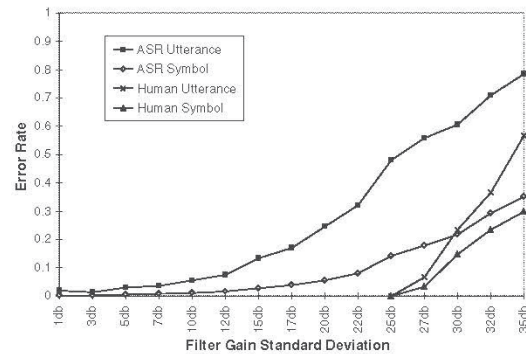


Fig. 4. Results for random filter experiment (*filter*).

performance appears to be wide enough to administer a robust Reverse Turing Test. In general, our tests show that humans can handle noise levels about 15 dB higher than ASR can. Likewise, humans can understand digit strings when more than half of the signal is missing, a point at which the machine already has a 100% error rate for utterances.

4. ANALYSIS: DO HUMANS MAKE THE SAME KINDS OF ERRORS AS MACHINES?

Not only is the error rate larger for an ASR system than for humans, but the pattern of errors is significantly different as well. Figure 5 shows a gray-scale plot of errors made by the machine and humans on the *white* data set. The figures represent noise levels chosen to give matching error rates.

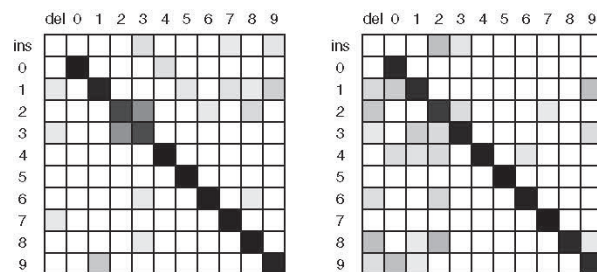


Fig. 5. Scaled confusion matrices at 35% error rate for humans (-3db SNR, left) and machine (+10db SNR, right).

Based on this observation, we could improve an RTT by looking at the kinds of errors that are made. For instance, humans readily confuse the digits “2” and “3” in the presence of white noise, so such an error should not be considered evidence that a machine is attempting to access the system. On the other hand, an “8” is never misunderstood as a “2” by humans but is sometimes by ASR, so such an error would suggest a machine’s presence.

5. ANALYSIS: HOW MANY DISTINCT KINDS OF DISTORTION ARE THERE?

One obvious attack on this kind of RTT is to build a classifier that, working from the input signal, attempts to identify the distortion that was applied, and then sends the input to an ASR system trained specifically for that distortion. ASR can be tuned to work well in the presence of noise [12], but it first needs to be trained with a large representative corpus collected from the environment in question.

Assuming that it is possible to build the necessary classifier, the question then arises “How many different ASR systems would one need to train in order to break the RTT?” To make this question tractable, we approach it by examining the confusion matrices derived from the experiments we have performed; these will serve as a proxy for training and testing a large number of ASR systems.

To do this, we follow logic presented elsewhere in the context of OCR systems [13]. We assume that if the ASR confusion matrices corresponding to two distorted signals are different enough, then separate recognizers will be needed because the two signals are fundamentally different. To make a quantitative comparison, we need to define a distance measure: we use the 2-norm of the difference of the scaled confusion matrices, $D(\alpha, \beta)^2 = \sum_{i,j} (S_{i,j}(\alpha) - S_{i,j}(\beta))^2$, where α and β refer to two different distortions, and S is a function of how the speech is distorted.

We can calibrate our notion of “different enough” by picking an error rate at which the ASR system fails and measuring $D(\alpha, \text{perfect})$ for various types of distortion at that rate. We choose noise levels that yield an utterance error rate of $85\% \pm 6\%$, with a symbol error rate of $34\% \pm 5\%$. The confusion matrices at these levels were found to be distance $D_{85} = 2.1 \pm 0.1$ from the perfect, error-free case. We assume that if the confusion matrices for any two distortions differ by this amount or more, an ASR system trained for one distortion will not be able to function on the other.

In our experiments, the average distance between a pair of distortions (excluding the mixtures) is 2.0 ± 0.9 , quite close to D_{85} , so we would expect that, in general, an ASR system could not be trained to handle two different types of distortions simultaneously. The mixtures tend to be closer to their components, a distance of 1.8 ± 0.6 away, but this is still far enough to conclude that an ASR system trained on either component of the mixture would probably not perform well on the mixture itself. Consequently, it appears there are enough ways of generating fundamentally distinct distortions that the RTTs we have described would resist an attack using any single, well-trained ASR system.

6. CONCLUSIONS

In this paper, we have described our work towards building a speech-based Reverse Turing Test. We show that the gap between ASR and human performance is wide for a variety of noise effects, and that there are opportunities to exploit differences between the patterns of errors that humans and machines make. The RTT is a fundamentally new way of using speech synthesis and recognition technologies.

The authors thank Olivier Siohan for assistance.

7. REFERENCES

- [1] A. Turing, “Computing machinery and intelligence,” *Mind*, vol. 59, no. 236, pp. 433–460, 1950.
- [2] A. L. Coates, H. S. Baird, and R. J. Fatahan, “Pessimistic print: A Reverse Turing Test,” in *Proc. of the Sixth Intl. Conf. on Document Analysis and Recognition*, Seattle, WA, September 2001, pp. 1154–1158.
- [3] L. von Ahn, M. Blum, J. Langford, and U. Manber, “The CAPTCHA project: Telling humans and computers apart (automatically),” October 2001, <http://www.captcha.net/>.
- [4] Yahoo! Inc., March 2002, <http://mail.yahoo.com>.
- [5] D. Lopresti, C. Shih, and G. Kochanski, “Human interactive proofs for spoken language interfaces,” in *Proc. of the Workshop on Human Interactive Proofs*, Palo Alto, CA, January 2002, pp. 30–34.
- [6] N. Chan, “Abstract of sound oriented CAPTCHA,” in *Proc. of the Workshop on Human Interactive Proofs*, Palo Alto, CA, January 2002, p. 35.
- [7] R. W. Sproat, Ed., *Multilingual Text-to-Speech Synthesis: The Bell Labs Approach*, Kluwer, 1998.
- [8] Q. Zhou and W. Chou, “An approach to continuous speech recognition based on layered self-adjusting decoding graph,” in *Proc. of the Intl. Conf. on Acoustics, Speech, and Signal Processing*, Munich, Germany, April 1997, pp. 1779–1782.
- [9] D. Sankoff and B. Kruskal, Joseph, *Time Warps, String Edits and Macromolecules: the Theory and Practice of Sequence Comparison*, CSLI Publications, 2 edition, 1999, ISBN 1-57586-217-4. Originally Addison-Wesley, 1993.
- [10] A. Stuart and D. P. Phillips, “Word recognition in continuous and interrupted broadband noise by young normal-hearing, older normal-hearing, and presbycusis listeners,” *Ear & Hearing*, vol. 17, pp. 478–489, 1996.
- [11] E. Woudenberg, F. K. Soong, and J. E. West, “Acoustic echo cancellation for hands-free ASR applications in noise,” in *Proc. of the Workshop on Acoustic Echo and Noise Control*, 1999, pp. 160–163.
- [12] P. J. Moreno, B. Raj, and R. M. Stern, “Data-driven environmental compensation for speech recognition: A unified approach,” *Speech Communication*, vol. 24, pp. 267–285, 1998.
- [13] Y. Li, D. Lopresti, G. Nagy, and A. Tomkins, “Validation of image defect models for optical character recognition,” *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. 18, no. 2, pp. 99–108, 1996.

ATTACHMENT 10

A REVERSE TURING TEST USING SPEECH

Greg Kochanski, Daniel Lopresti, and Chilin Shih

Bell Laboratories, Lucent Technologies
{gpk,dpl,cls}@research.bell-labs.com, 600 Mountain Ave, Murray Hill, NJ 07974

ABSTRACT

“Hackers” have written malicious programs to exploit on-line services intended for human users. As a result, service providers need a method to tell whether a web site is being accessed by a human or a machine. We expect a parallel scenario as spoken language interfaces become common.

In this paper, we describe a *Reverse Turing Test* (*i.e.*, an algorithm that can distinguish between humans and computers) using speech. We present a test that depends on the fact that human recognition of distorted speech is far more robust than automatic speech recognition techniques.

Our analysis of 18 different sets of distortions demonstrates that there are a variety of ways to make the problem hard for machines. In addition, humans and speech recognition systems make different kinds of mistakes, and this difference can be employed to improve discrimination.

1. INTRODUCTION

The use of the Internet as a means for distributing valuable information and content have also made it an attractive target for “hackers.” Attacks involving malicious programs (“bots”) that attempt to exploit online services intended for human users are already common. These programs consume resources, harass users, make attempts to guess passwords, steal and re-purpose copyrighted content, and invade privacy by reconstructing sensitive data from public views.

As a result, there is a need for automatic methods to tell whether the entity attempting to access a service is a human or a machine. This has come to be known as a *Reverse Turing Test*, or *RTT* (or sometimes a *Human Interactive Proof*). Unlike the test originally proposed by Alan Turing [1], a Reverse Turing Test is administered by a computer, not a human. For the test to be considered effective, humans should be able to pass it with ease, but machines should have a low probability of passing.

While it may seem that passwords and/or biometrics could provide a solution, one must keep in mind that these approaches require pre-registration. An RTT will work even if the user is anonymous and has never used the service before. The RTT problem is fundamentally different from validating a known user. Indeed, a Reverse Turing Test should

be applied before authentication to prevent automated attacks on passwords.

Coates, Baird, and Fateman [2], and von Ahn *et al.* [3] have developed such a test based on a visual perception task. Their ideas are based on the observation that optical character recognition (OCR) systems are not as adept at reading degraded word images as humans are. That RTT is now used commercially to protect a free email service [4].

Speech-based services are proliferating because of their ease-of-use, portability, and potential for hands-free operation. Building a “bot” to navigate a spoken language interface is a tractable problem, especially if there is a fixed sequence of predefined prompts. Hence, we anticipate attacks on such systems and a similar need to prevent machines from abusing speech-based resources intended for human users. Previous work on speech RTTs can be found in [5, 6].

As in the vision RTTs, we exploit the fact that certain pattern recognition tasks are significantly harder for machines than they are for humans. We will use text-to-speech synthesis (TTS) to generate tests, and make use of the limitations of state-of-the-art automatic speech recognition (ASR) technology. (We require only that RTTs cannot be broken cheaply or rapidly. Clearly, any RTT can be broken by hiring a human.)

In this paper, we present the core of a spoken language RTT. We assume a user with a cell phone; the test may consist of having the system speak: “Please enter the following digits on your keypad: ...” followed by a short, random digit string. The speech would be synthesized in a way that ASR is likely to fail the test, *e.g.*, by distorting the signal or adding “difficult” background noise to it after synthesis.

2. PROCEDURES

We designed a set of 18 RTTs based on different distortions of a speech signal (Table 2) to explore a broad range of possibilities. To test our RTTs, we synthesized 200 random 5-digit sequences using the Bell Labs English text-to-speech system [7], with the default male voice. We next distorted the signals and ran the Bell Labs speech recognition system [8] on them, with a grammar that allowed any digit se-

Name	Description	Error Ratio
<i>white</i>	• White Gaussian noise, 4000 Hz bandwidth.	15
<i>buzz</i>	• Sine waves at 700 Hz, 2100 Hz, 3500 Hz.	≥ 20
<i>song</i>	• Bell Labs Song (pop/rock).	> 15
<i>chopin</i>	• Chopin Polonaise for Piano No. 6, Op. 53.	> 20
<i>chant</i>	• Gregorian chant.	> 20
<i>female</i>	• Three overlapping instances of a female voice reading numbers.	> 20
<i>pow</i>	• 10 ms bursts of white Gaussian noise, repeated every 100 ms.	> 20
<i>rnoise</i>	• Every 100 ms, a section of the signal is replaced by white noise of the same RMS amplitude.	> 20
<i>cell</i>	• For each 30 ms window, decide if the data was lost. If so, and previous not lost, duplicate previous. If so, and previous is lost, set to zero. Simulates a bad cell phone channel.	> 10
<i>echo</i>	• Three echoes.	> 20
<i>filter</i>	• A random zero-phase filter.	> 5
<i>distort</i>	• Apply AGC on a 60 ms window, raise to a power, multiply by original amplitude.	≥ 20
<i>mxa</i>	• <i>rnoise</i> + <i>chopin</i>	> 20
<i>mxh</i>	• <i>song</i> + <i>echo</i>	> 20
<i>mxg</i>	• <i>white</i> + <i>pow</i>	≥ 20
<i>mxj</i>	• <i>female</i> + <i>buzz</i>	≥ 5
<i>mxk</i>	• <i>rnoise</i> + <i>distort</i>	≥ 20
<i>mxl</i>	• <i>filter</i> + <i>distort</i>	3

Table 1. Tested RTTs. The error ratio is an estimate of the largest ratio of the ASR to human utterance error rates. The components of all mixtures were chosen to cause equal error rates for ASR utterance error rates near 85%.

quence.

The recognition results were compared to the original digit sequences using approximate string matching ([9] and references therein) to identify added, missing, and substituted digits. From this we obtained, for each distortion, per-digit and per-utterance error rates, as well as a confusion matrix showing the frequency of each type of error.

A similar procedure was followed to test how well humans could recognize the signals. The authors each listened to 10 randomly-chosen digit sequences for each type of distortion. In these tests, the audio signals were presented twice with a one second pause in between. The subject then typed his/her interpretation and pressed return to listen to the next signal. The tests began at the most severe distortion of each type, and terminated when the subject correctly identified all 10 sequences. One set (*white*) received 67 repetitions per person for a more accurate confusion matrix.

The confusion matrices are scaled to make all diagonal confusion matrices identical. This step is necessary because the distance between raw confusion matrices is generally nonzero, even if there are no errors (*i.e.* the matrices are diagonal). This happens because we do not explicitly balance

the frequencies of each digit, so that one test may see more instances of, say, “3” than another. Hence, we use a scaled confusion matrix, $S = P \cdot C \cdot Q$, where P and Q are diagonal matrices chosen so that the row- and column-sums of S are unity. While deletions and insertions are conventionally placed in the same matrix as substitutions they are actually a fundamentally different kind of error. Specifically, $C_{del,ins}$ is on the diagonal and is missing (zero). Thus, insertions and deletions must be treated differently in the scaling. We make an ad-hoc modification to C before scaling: we set $C_{del,ins} \leftarrow \sum_{i,j} C_{i,j}/N$ (where $N = 11$ is the number of rows and columns in C), and then set $S_{del,ins} \leftarrow 0$.

3. ANALYSIS: IS IT POSSIBLE TO DISTINGUISH HUMANS FROM MACHINES?

Human perception of speech in noisy environments is fairly robust. Normal-hearing listeners need a signal-to-noise ratio (SNR) of approximately 1.5 dB to recognize speech [10], while ASR systems require a much more favorable SNR of 5 to 15 dB [11]. Our test results show an even wider gap between human and ASR performance.

Figures 1-4 plot the error rates we measured in four experiments; these correspond to four distinct types of distortion: additive noise, deleting segments of the speech, adding echoes and filtering the signal. The four curves in each chart represent the error rates for ASR on a per-utterance (square) and per-symbol (diamond) basis along with per-utterance (X) and per-symbol (triangle) rates for humans.

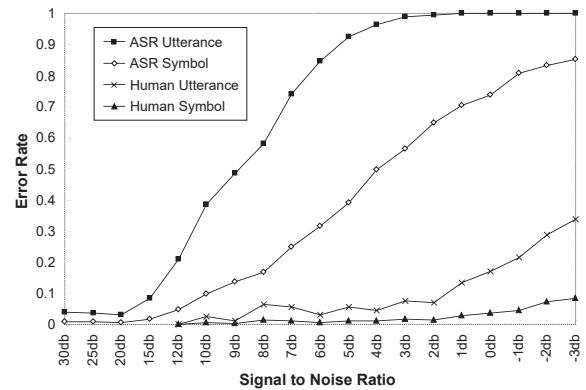


Fig. 1. Results for white noise experiment (*white*).

In figure 1, *white* is simply additive white noise. The x-axis shows SNR, and the y-axis represents the rate of recognition errors. In the ASR curves, each datum represents scores from 200 utterances or 1,000 digits, while in the human curves, each datum represents 201 utterances or 1,005 digits as pooled from the three listeners. ASR performance starts deteriorating when the SNR reaches 15 dB, and breaks down completely by 3 dB. Human performance is only starting to deteriorate at 0 dB SNR.

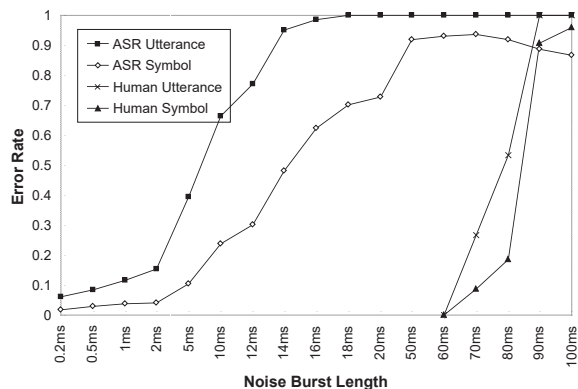


Fig. 2. Results for replacement noise experiment (*rnoise*).

Figure 2 shows the results for *rnoise*, which replaces a segment of speech with white noise every 100 ms, as we vary the length of the replaced segment. Human scores in this figure and in Figures 3-4 are based on 30 utterances (150 digits) per datum. As can be seen, ASR starts having problems when 2 ms (2%) of the speech is replaced. Amazingly, human recognition remains perfect at 60 ms (60% replacement), and 80% of the symbols are still correct even when 80% of the speech is missing.

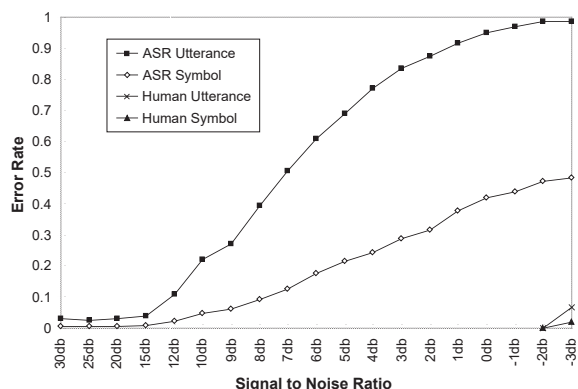


Fig. 3. Results for echo experiment (*echo*).

Our results for *echo*, which adds three echoes to the speech with delays of 60, 132, and 192 ms, are presented in Figure 3. The horizontal axis shows the relative amplitude of the first echo to the speech, while later echoes are 5 dB and 10 dB quieter. ASR performance starts declining when the SNR is 12 dB, while human performance is perfect until -3 dB. This behavior is typical of many of the other tests we performed.

Among our tests, *filter* (Figure 4) showed the smallest difference between ASR and humans. This is a zero-phase frequency domain filter, with a frequency response chosen randomly every 30 Hz. The control parameter sets the standard deviation of the gain, expressed in dB.

Our findings are that the gap between ASR and human

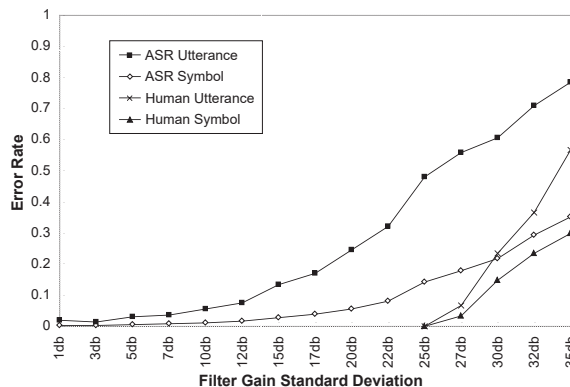


Fig. 4. Results for random filter experiment (*filter*).

performance appears to be wide enough to administer a robust Reverse Turing Test. In general, our tests show that humans can handle noise levels about 15 dB higher than ASR can. Likewise, humans can understand digit strings when more than half of the signal is missing, a point at which the machine already has a 100% error rate for utterances.

4. ANALYSIS: DO HUMANS MAKE THE SAME KINDS OF ERRORS AS MACHINES?

Not only is the error rate larger for an ASR system than for humans, but the pattern of errors is significantly different as well. Figure 5 shows a gray-scale plot of errors made by the machine and humans on the *white* data set. The figures represent noise levels chosen to give matching error rates.

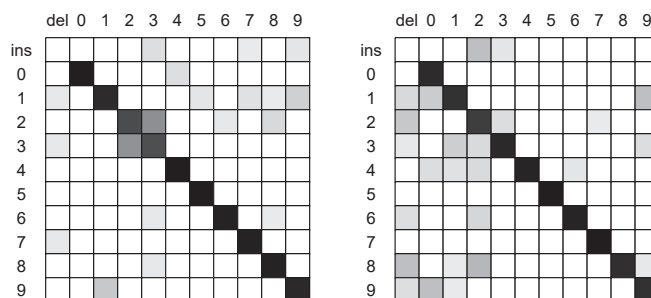


Fig. 5. Scaled confusion matrices at 35% error rate for humans (-3dB SNR, left) and machine (+10dB SNR, right).

Based on this observation, we could improve an RTT by looking at the kinds of errors that are made. For instance, humans readily confuse the digits “2” and “3” in the presence of white noise, so such an error should not be considered evidence that a machine is attempting to access the system. On the other hand, an “8” is never misunderstood as a “2” by humans but is sometimes by ASR, so such an error would suggest a machine’s presence.

5. ANALYSIS: HOW MANY DISTINCT KINDS OF DISTORTION ARE THERE?

One obvious attack on this kind of RTT is to build a classifier that, working from the input signal, attempts to identify the distortion that was applied, and then sends the input to an ASR system trained specifically for that distortion. ASR can be tuned to work well in the presence of noise [12], but it first needs to be trained with a large representative corpus collected from the environment in question.

Assuming that it is possible to build the necessary classifier, the question then arises “How many different ASR systems would one need to train in order to break the RTT?” To make this question tractable, we approach it by examining the confusion matrices derived from the experiments we have performed; these will serve as a proxy for training and testing a large number of ASR systems.

To do this, we follow logic presented elsewhere in the context of OCR systems [13]. We assume that if the ASR confusion matrices corresponding to two distorted signals are different enough, then separate recognizers will be needed because the two signals are fundamentally different. To make a quantitative comparison, we need to define a distance measure: we use the 2-norm of the difference of the scaled confusion matrices, $D(\alpha, \beta)^2 = \sum_{i,j} (S_{i,j}(\alpha) - S_{i,j}(\beta))^2$, where α and β refer to two different distortions, and S is a function of how the speech is distorted.

We can calibrate our notion of “different enough” by picking an error rate at which the ASR system fails and measuring $D(\alpha, \text{perfect})$ for various types of distortion at that rate. We choose noise levels that yield an utterance error rate of $85\% \pm 6\%$, with a symbol error rate of $34\% \pm 5\%$. The confusion matrices at these levels were found to be distance $D_{85} = 2.1 \pm 0.1$ from the perfect, error-free case. We assume that if the confusion matrices for any two distortions differ by this amount or more, an ASR system trained for one distortion will not be able to function on the other.

In our experiments, the average distance between a pair of distortions (excluding the mixtures) is 2.0 ± 0.9 , quite close to D_{85} , so we would expect that, in general, an ASR system could not be trained to handle two different types of distortions simultaneously. The mixtures tend to be closer to their components, a distance of 1.8 ± 0.6 away, but this is still far enough to conclude that an ASR system trained on either component of the mixture would probably not perform well on the mixture itself. Consequently, it appears there are enough ways of generating fundamentally distinct distortions that the RTTs we have described would resist an attack using any single, well-trained ASR system.

6. CONCLUSIONS

In this paper, we have described our work towards building a speech-based Reverse Turing Test. We show that the gap between ASR and human performance is wide for a variety of noise effects, and that there are opportunities to exploit differences between the patterns of errors that humans and machines make. The RTT is a fundamentally new way of using speech synthesis and recognition technologies.

The authors thank Olivier Siohan for assistance.

7. REFERENCES

- [1] A. Turing, “Computing machinery and intelligence,” *Mind*, vol. 59, no. 236, pp. 433–460, 1950.
- [2] A. L. Coates, H. S. Baird, and R. J. Fateman, “Pessimistic print: A Reverse Turing Test,” in *Proc. of the Sixth Intl. Conf. on Document Analysis and Recognition*, Seattle, WA, September 2001, pp. 1154–1158.
- [3] L. von Ahn, M. Blum, J. Langford, and U. Manber, “The CAPTCHA project: Telling humans and computers apart (automatically),” October 2001, <http://www.captcha.net/>.
- [4] Yahoo! Inc., “,” March 2002, <http://mail.yahoo.com>.
- [5] D. Lopresti, C. Shih, and G. Kochanski, “Human interactive proofs for spoken language interfaces,” in *Proc. of the Workshop on Human Interactive Proofs*, Palo Alto, CA, January 2002, pp. 30–34.
- [6] N. Chan, “Abstract of sound oriented CAPTCHA,” in *Proc. of the Workshop on Human Interactive Proofs*, Palo Alto, CA, January 2002, p. 35.
- [7] R. W. Sproat, Ed., *Multilingual Text-to-Speech Synthesis: The Bell Labs Approach*, Kluwer, 1998.
- [8] Q. Zhou and W. Chou, “An approach to continuous speech recognition based on layered self-adjusting decoding graph,” in *Proc. of the Intl. Conf. on Acoustics, Speech, and Signal Processing*, Munich, Germany, April 1997, pp. 1779–1782.
- [9] D. Sankoff and B. Kruskal, Joseph, *Time Warps, String Edits and Macromolecules: the Theory and Practice of Sequence Comparison*, CSLI Publications, 2 edition, 1999, ISBN 1-57586-217-4. Originally Addison-Wesley, 1993.
- [10] A. Stuart and D. P. Phillips, “Word recognition in continuous and interrupted broadband noise by young normal-hearing, older normal-hearing, and presbycusis listeners,” *Ear & Hearing*, vol. 17, pp. 478–489, 1996.
- [11] E. Woudenbergh, F. K. Soong, and J. E. West, “Acoustic echo cancellation for hands-free ASR applications in noise,” in *Proc. of the Workshop on Acoustic Echo and Noise Control*, 1999, pp. 160–163.
- [12] P. J. Moreno, B. Raj, and R. M. Stern, “Data-driven environmental compensation for speech recognition: A unified approach,” *Speech Communication*, vol. 24, pp. 267–285, 1998.
- [13] Y. Li, D. Lopresti, G. Nagy, and A. Tomkins, “Validation of image defect models for optical character recognition,” *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. 18, no. 2, pp. 99–108, 1996.

ATTACHMENT 11

ATTACHMENT 12

ome

Tools

CAPTCHA-ATTAC...

CAPTCHA-ATTAC...

☆

📄

🔍

📶

📱

📺

1 / 4

124%

🔍

🖨

🔗

Document Properties

Description

File: CAPTCHA-ATTACHMENT10.pdf

Title: rtt.dvi

Author:

Subject:

Keywords:

Additional Metadata...

Advanced

Created: 4/1/02, 12:25:09 PM

Modified: 9/10/20, 12:27:35 PM

Application: dvipsk 5.58c Copyright 1986, 1994 Radical Eye Software

Advanced

PDF Producer: Acrobat Distiller 3.01 for Windows

PDF Version: 1.6 (Acrobat 7.x)

Location: /Users/Mary/Documents/consult/

File Size: 80,96 KB (82,906 Bytes)

Page Size: 8.50 x 11.00 in

Number of Pages: 4

Tagged PDF: No

Fast Web View: Yes

Help

Cancel

Scan & OCR

Protect

Your current plan is Creative Cloud

Learn More

A REVERSE TURING TEST USING SPEECH

Greg Kochanski, Daniel Lopresti, and Chilin Shih

Bell Laboratories, Lucent Technologies
{gpk,dpl,cls}@research.bell-labs.com, 600 Mountain Ave, Murray Hill, NJ

be applied before authentication to attacks on passwords.

Coates, Baird, and Fateman [2], have developed such a test based on an actor recognition (OCR) systems are not as adept at reading degraded word images as humans are. That RTT is now used commercially to protect a free email service [4].

Speech-based services are proliferating because of their ease-of-use, portability, and potential for hands-free operation. Building a “bot” to navigate a spoken language interface is a tractable problem, especially if there is a fixed sequence of predefined prompts. Hence, we anticipate at-

ATTACHMENT 13

Search 189,434,870 papers from all ...

Search

[FAQ](#)[About](#)[Contact](#)[Sign In](#)

Create Free Account

Share This Paper

[Twitter](#)[Facebook](#)[LinkedIn](#)[Email](#)

Corpus ID: 63634578

Proceedings of the 7th International Conference on Spoken Language Processing (ICSLP'2002), Denver-Colorado, USA, September 2002

[Z. Tan](#), [P. Dalsgaard](#) · Published 2002 · Computer Science

[Save To Library](#)[Create Alert](#)[Cite](#)[Launch Research Feed](#)

Top 3 of 9 Citations

[View All](#)

Affective Dialogue Management Using Factored POMDPs

Trung H. Bui, J. Zwiers, ... A. Nijholt · Interactive Collaborative Information Systems · 2010

14

Beyond multi-class : structured learning for machine translation

Yizhao Ni · 2010

2

Confidence Measures in Automatic Speech Recognition Systems for Err...

Julia Olcoz, A. Ortega, ... E. Lleida · IberSPEECH · 2014

[ABSTRACT](#)

[9 CITATIONS](#)

[RELATED PAPERS](#)

9 Citations

Q

Fields Of Study

Citation Type

Has PDF

More Filters

More Filters

Filters

Sort by Relevance

Testing the performance of spoken dialogue systems by means of an artificially simulated user

[R. López-Cózar](#), [Zoraida Callejas Carrión](#), [M. McTear](#) · Computer Science · 2007

39 Save Alert Feed

Affective Dialogue Management Using Factored POMDPs

[Trung H. Bui](#), [J. Zwiers](#), [M. Poel](#), [A. Nijholt](#) · Computer Science · 2010

14 Save Alert Feed

Confidence Measures in Automatic Speech Recognition Systems for Error Detection in Restricted Domains

[Julia Olcoz](#), [A. Ortega](#), [A. Miguel](#), [E. Lleida](#) · Computer Science · 2014

Save Alert Feed

Venetan to English machine translation: issues and possible solutions

[Suhel Jaber](#), [Sara Tonelli](#), [Rodolfo Delmonte](#) · Computer Science · 2011

“1” Save Alert Feed

Voice conversion by mapping the speaker-specific features using pitch synchronous approach

K. Rao · Computer Science · 2010

67 Save Alert Feed

Czech-Sign Speech Corpus for Semantic Based Machine Translation

J. Kanis, J. Zahradil, Filip Jurcicek, L. Müller • Computer Science • 2006

14 Save Alert Feed

Beyond multi-class : structured learning for machine translation

Yizhao Ni · Computer Science · 2010

“2” Save Alert Feed

Exploitation of Machine Learning Techniques in Modelling Phrase Movements for Machine Translation

Yizhao Ni, C. Saunders, S. Szedmák, M. Niranjan • Computer Science • 2011

14 Save Alert Feed

SmartKom: adaptive and flexible multimodal access to multiple applications

Norbert Reithinger, J. Alexandersson, +8 authors Valentin Tschernomas · Computer Science · 2003

78 Save Alert Feed

Related Papers

▼ Show More

2/0

Proudly built by [AI2](#) with the help of our [Collaborators](#) using these [Sources](#).
[Research](#) • [Publisher Partnerships](#) • [Data Partnerships](#) • [API and Open Corpus](#)
[Terms of Service](#) • [Privacy Policy](#)

ATTACHMENT 14

A REVERSE TURING TEST USING SPEECH

Greg Kochanski, Daniel Lopresti, and Chilin Shih

Bell Laboratories, Lucent Technologies

{gpk,dpl,cls}@research.bell-labs.com, 600 Mountain Ave, Murray Hill, NJ 07974

ABSTRACT

"Hackers" have written malicious programs to exploit online services intended for human users. As a result, service providers need a method to tell whether a web site is being accessed by a human or a machine. We expect a parallel scenario as spoken language interfaces become common.

In this paper, we describe a *Reverse Turing Test* (i.e., an algorithm that can distinguish between humans and computers) using speech. We present a test that depends on the fact that human recognition of distorted speech is far more robust than automatic speech recognition techniques.

Our analysis of 18 different sets of distortions demonstrates that there are a variety of ways to make the problem hard for machines. In addition, humans and speech recognition systems make different kinds of mistakes, and this difference can be used to prove discrimination.

Lightshot Screenshots

be applied before authentication to prevent automated attacks on passwords.

Coates, Baird, and Fateman [2], and von Ahn *et al.* [3] have developed such a test based on a visual perception task. Their ideas are based on the observation that optical character recognition (OCR) systems are not as adept at reading degraded word images as humans are. That RTT is now used commercially to protect a free email service [4].

Speech-based services are proliferating because of their ease-of-use, portability, and potential for hands-free operation. Building a "bot" to navigate a spoken language interface is a tractable problem, especially if there is a fixed sequence of predefined prompts. Hence, we anticipate attacks on such systems and a similar need to prevent machines from abusing speech-based resources intended for human users. Previous work on speech RTTs can be found in [5, 6].

As in the vision RTTs, we exploit the fact that certain