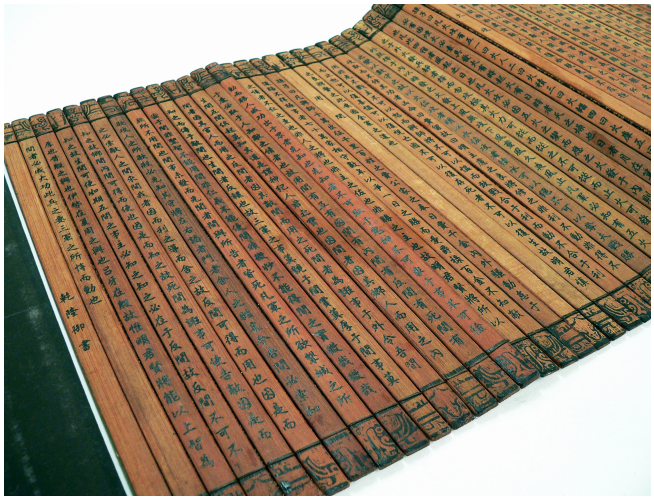
December 2020, Issue Code NL-2021-3-C

DDD (Digital Data Deception) Technology Watch Newsletter: Chinese Section

Table of Contents



Source: `https://www.flickr.com/photos/bluefootedbooby/370460130/`

“兵者，诡道也。故能而示之不能，用而示之不用，近而示之远，远而示之近。利而诱之，乱而取之，实而备之，强而避之，怒而挠之，卑而骄之，佚而劳之，亲而离之。攻其无备，出其不意。此兵家之胜，不可先传也。”

— 孙武：《孙子兵法·始计篇》

(The above is the original Chinese version of the English quotation included on the cover page of the newsletter's main issue NL-2021-3; quote by Sun Tzu, *The Art of War*.)

Editors: Li Qin, Shujun Li, Enes Altuncu, Virginia Franqueira, and Sanjay Bhattacherjee
Affiliation: Kent Interdisciplinary Research Centre in Cyber Security (KirCCS), University of Kent, UK
Contact Us: `ddd-newsletter@kent.ac.uk`

Editorial

In this third issue of the Digital Data Deception (DDD) newsletter, we also include a Chinese section covering some general background information and five selected Chinese research papers on AI-related DDD topics. In future issues, we will cover more research papers on other DDD-related topics.

For the general information sections, since most sources of information are not research papers, we include main references immediately below the relevant text. A lot of information included in those sections is common knowledge, so we also use English Wikipedia and Encyclopaedia Britannica as information sources. For some subsections we will not explicitly list any references, if the text is mainly based on our personal knowledge and understanding (note that two editors of this newsletter, Li Qin and Shujun Li, are native Chinese speakers).

We hope you enjoy reading the Chinese section of this issue. Feedback is always welcome, and should be directed to `ddd-newsletter@kent.ac.uk`.

List of Acronyms

- AI: Artificial Intelligence
- AR: Autoregressive Model
- ASV: Automatic Speaker Verification
- CNKI: China National Knowledge Infrastructure
- CNN: Convolution Neural Network
- DAE: Denoising Autoencoder
- DDD: Digital Data Deception
- DNN: Deep Neural Network
- FC: Fully Connected
- FGSM: Fast Gradient Sign Method
- GAN: Generative Adversarial Network
- GAP: Global Aver-age Pooling
- GMM: Gaussian Mixture Model
- HMM: Hidden Markov Model
- HE: Higher Education
- HEI: Higher Education Institutions
- LSTM: Long Short Term Memory
- PLDA: Probabilistic Linear Discriminant Analysis
- RNN: Recurrent Neural Network
- SVM: Support Vector Machine
- TDNN: Time Delay Neural Network
- TTS: Text-to-speech

General Background Information about Greater China and Chinese

Introduction

This section is included in this newsletter to give readers an overview of some important background information about Greater China as a region, people living in that region, and Chinese as a spoken language and a writing system.

Greater China and People Living There

The term "Greater China" is commonly used to refer to four main Chinese-dominating regions in Eastern Asia: Mainland China (中国大陆), Taiwan (台湾 / 臺灣), Hong Kong (香港), and Macao/-Macau (澳门 / 澳門). Between the two different spellings of Macau/Macao, we will mainly use "Macao" following the official name of the region in official governmental documents and the common practice of the UK Government, however, note that "Macau" is still recognised by the Macao government as an acceptable spelling and it is still widely used in Macao including for naming higher education institutions such as the University of Macau / Universidade de Macau (澳門大學 / 澳门大学, `https://www.um.edu.mo/`).

References

[1] Wikipedia, "Greater China," `https://en.wikipedia.org/wiki/Greater_China`

[2] Macao Government Tourism Office, "Is it Macau or Macao?" `https://www.visitmacao.com.au/macao-tourism-blog/faq/is-it-macau-or-macao/`

[3] UK Government, "Foreign travel advice: Macao," `https://www.gov.uk/foreign-travel-advice/macao`

The biggest ethnic group in Greater China is Han Chinese (汉族 / 汉人), which is also the largest ethnic group in the world. There are also many other minority ethnic groups in Greater China, e.g., the 55 recognised ethnic minorities in Mainland China such as the following with a population of over one million people: Zhuang (壮族), Hui (回族), Manchu (满族), Uyghur (维吾尔族), Miao (苗族), Yi (彝族), Tujia (土家族), Tibetan (藏族), Mongol (蒙古族), Dong (侗族), Buyei (布依族), Yao (瑶族), Bai (白族), Korean (朝鲜族), Hani (哈尼族), Li (黎族), Kazakh (哈萨克族) and Dai (傣族).

References

[1] Wikipedia, "Ethnic minorities in China," `https://en.wikipedia.org/wiki/Ethnic_minorities_in_China`

[2] Wikipedia, "List of ethnic groups in China," `https://en.wikipedia.org/wiki/List_of_ethnic_groups_in_China`

The Chinese Language

The Chinese language (汉语 / 漢語) is a language or a group of language varieties spoken by ethnic Han Chinese and many other ethnic groups such as Hui people (who are Chinese-speaking Muslims). Chinese-speaking people and linguists have different opinions on if Chinese should be considered a single language with different dialects or a group of different languages of their own rights (although they were all originated from ancient Chinese). This is mainly because all Chinese-speaking people share the same writing system (or two, to be detailed below) and the lack of mutual intelligibility between different language varieties of Chinese. Among all the varieties of Chinese, Mandarin (官话 / 官話) is the most-spoken one, followed by other varieties such as Min (閩語 / 闽语), Wu (吴语 / 吳語), Yue (粵语 / 粵語), Jin (晋语 / 晉語), Gan (赣语 / 贛語), Hakka (客家话 / 客家話), Xiang (湘语 / 湘語), Pinghua (平话 / 平話), and Huizhu Chinese (徽州话 / 徽州話).

References

[1] 中国社会科学院 / Chinese Academy of Social Sciences,《中国语言地图集》/ *Language Atlas of China*, 第二版 (2nd Edition), 商务印书馆 (The Commercial Press), 2012

[2] Wikipedia, "List of varieties of Chinese," `https://en.wikipedia.org/wiki/List_of_varieties_of_Chinese`

The writing system of the Chinese language is not based on an alphabet like in Western languages, but a logosyllabic system based on a large number of Chinese characters (汉字 / 漢字) each representing one syllable in spoken Chinese and often a word by itself. Currently, there are two standard writing systems of Chinese: Simplified Chinese (简体中文

/ 簡體中文) used in Mainland China and Traditional Chinese (繁体中文, also called 正体中文 in Taiwan) used in Taiwan, Hong Kong and Macao. Traditionally, there is only one writing system, but in the 1950s and 1960s the government of Mainland China decided to promote the use of Simplified Chinese characters (简化字 / 簡化字). Since then these have become the standard writing system in Mainland China and have also been accepted by some overseas Chinese populations such as those living in Southeastern Asia. Although the Chinese writing system was created for writing in Chinese only, it has been adopted by a number of other countries in the East Asian cultural sphere (东亚文化圈 / 東亞文化圈), also known as Chinese Character cultural sphere (汉字文化圈 / 漢字文化圈) or simply Sinosphere (中华文化圈 / 中華文化圈), including Japan, Korea and Vietnam. For instance, the Chinese writing system has been used for official documents and for the general literature in those countries, and even today many Chinese characters are still being used in Japan and Korea today – called Kanji in Japan and Hanja in Korea. The Chinese writing system also inspired Japanese, Korean and Vietnamese to create their own writing systems, including Japanese Kana (假名), Korean Hangul (韩字 / 韓字, 朝鲜字 / 朝鮮字, 谚文 / 諺文), and Vietnamese Chữ Nôm (喃字 / 字喃).

References

[1] Wikipedia, "Traditional Chinese characters,"https://en.wikipedia.org/wiki/Traditional_Chinese_characters

[2] Wikipedia, "Simplified Chinese characters," https://en.wikipedia.org/wiki/Simplified_Chinese_characters

[3] Wikipedia, "East Asian cultural sphere," https://en.wikipedia.org/wiki/East_Asian_cultural_sphere

Romanisation of Chinese

To facilitate communications between Chinese and Western people using Latin characters and to help people learn Chinese, a number of romanisation systems of Chinese characters have been developed. The Hanyu Pinyin (汉语拼音) system, normally abbreviated as Pinyin (拼音), is the official romanisation system used in Mainland China and to some extent in Taiwan. The Pinyin system was developed in the 1950s and has been adopted in 1982 as an international standard (ISO 7098:1982). The English name of the Chinese editor of this newsletter (Shujun Li, romanised from 李树钧) is spelt following the Pinyin system.

References

[1] Wikipedia, "Romanization of Chinese," https://en.wikipedia.org/wiki/Romanization_of_Chinese

[2] Encyclopaedia Britannica, "Pinyin romanization," https://www.britannica.com/topic/Pinyin-romanization

[3] ISO, "Information and documentation — Romanization of Chinese," ISO 7098:1982, https://www.iso.org/standard/13682.html

[4] ISO, "Information and documentation — Romanization of Chinese," ISO 7098:2015, https://www.iso.org/standard/61420.html

Another widely used romanisation system of Chinese is the Wade–Giles romanisation system (威妥瑪拼音 / 威翟式拼音 / 韋氏拼音 / 威妥玛拼音 / 韦氏拼音) initialised by Thomas Francis Wade in the 19th century and finalised by the University of Cambridge professor Herbert Allen Giles in his *A Chinese–English Dictionary* (1892; 2nd Edition 1912), which is currently widely used in Taiwan, Hong Kong, Macao and among many overseas Chinese. Nowadays many Chinese universities that had been established before Pinyin was introduced in the 1950s still keep their old names spelt in the Wade–Giles system, rather than switch to the Pinyin system, e.g., the name of Peking University (北京大学) would be "Beijing University" if the Pinyin system was used.

References

[1] Encyclopaedia Britannica, "Wade-Giles romanization," https://www.britannica.com/topic/Wade-Giles-romanization

[2] Herbert Allen Giles, *A Chinese–English Dictionary*, Kelly and Walsh, 1892, 2nd Edition 1912 (see also Wikipedia's entry https://en.wikipedia.org/wiki/A_Chinese%E2%80%93English_Dictionary)

Higher Education and Research in Greater China

Introduction

This section covers some general background information about the higher education (HE) sector and research activities in Greater China, which will be helpful for our readers to understand the general context of selected research papers published in Chinese.

Higher Education

Due to historical reasons, the higher education (HE) systems in the four regions in Greater China have followed very different paths.

The system in Mainland China has borrowed a lot from that of the former Soviet Union (USSR – Union of Soviet Socialist Republics), e.g., many higher educational institutions (HEIs) concentrate on research and education in one or more highly specialised subjects or areas, e.g., Beijing University of Posts and Telecommunications (BUPT, 北京邮电大学, https://www.bupt.edu.cn/) and University of Electronic Science and Technology of China (UESTC, 电子科技大学, https://www.uestc.edu.cn/), both of which have active research on DDD-related topics. However, recently many Chinese HEIs have started adopting elements in the North American system and expanding their research spectrum towards becoming more universal HEIs, e.g., the introduction of tenure-tracked Assistant Professorships in many top Chinese HEIs, and creation of academic schools covering social sciences and humanities at HEIs that had previously focused solely on physical sciences and engineering. The HE sector in Mainland China has always been dominated by publicly funded HEIs and degrees awarded by HEIs are tightly regulated by the Ministry of Education (MoE). In the past a few decades, many private universities have emerged and some have become very successful, such as Westlake University (西湖大学, https://www.westlake.edu.cn/), Cheung Kong Graduate School of Business (CKGSB, 长江商学院, http://www.ckgsb.edu.cn/), Jilin International Studies University (吉林外国语大学, http://www.jisu.edu.cn/), Wuchang Shouyi University (武昌首义学院, http://www.wsyu.edu.cn/), and Xi'an Eurasia University (西安欧亚学院, http://www.eurasia.edu/). In addition to Chinese HEIs, some overseas HEIs have set up campuses in Mainland China or have been working together with partner HEIs in China to run joint HEIs, including the Xi'an Jiaotong-Liverpool University (XJTLU, 西交利物浦大学, https://www.xjtlu.edu.cn/), University of Nottingham Ningbo China (宁波诺丁汉大学, https://www.nottingham.edu.cn/), Duke Kunshan University (中国昆山杜克大学, https://dukekunshan.edu.cn/), NYU Shanghai (上海纽约大学, https://shanghai.nyu.edu/), Guangdong Technion-Israel Institute of Technology (广东以色列理工学院, https://www.gtiit.edu.cn/), Wenzhou-Kean University (温州肯恩大学, https://wku.edu.cn/) and Shenzhen MSU-BIT University (深圳北理莫斯科大学, https://www.smbu.edu.cn/). Due to the huge population and the expansion of higher education in Mainland China, the number of HEIs is huge: 3,005 in total as of 30 June 2020, including 1,272 offering bachelor degrees and above, 1,468 offering only 2-year associate (college) degree, 1,986 public HEIs and 773 private ones.

References

[1] Wikipedia, "Higher education in China," https://en.wikipedia.org/wiki/Higher_education_in_China

[2] 中华人民共和国教育部 / Ministry of Education of People's Republic of China, "全国高等学校名单 / A list of higher educational institutions," http://www.moe.gov.cn/jyb_xxgk/s5743/s5744/202007/t20200709_470937.html

[3] 艾瑞深校友会 / Chinese Universities Alumni Association (CUAA), "校友会 2019 中国民办大学排名 150 强，武昌首义学院第一 / Top 150 private HEIs in China according to CUAA rankings for 2019: Wuchang Shouyi University tops the list," online article, 24 December 2018, http://www.cuaa.net/paihang/news/news.jsp?information_id=135468

[4] 《留学》杂志 / Studying Abroad Magazine, "浅析国内九所中外合办大学 / A short analysis of nine joint Sino-overseas universities in China," online article on Sina Zhuanlan (新浪专栏), 27 July 2018, http://edu.sina.com.cn/zl/2018-07-

27/doc-ihfvkitx6343154.shtml

The HE system in Taiwan largely continued its original path from the old Republic of China's system but also saw some major developments since the 1950s, particularly the 1994 "410 Demonstration for Education Reform" led to a significant expansion of the HE sector for the masses rather than for the elite. The system in Hong Kong has a root in the UK system and also the old system of the Qing Empire (the last imperial dynasty of China, which ruled China when Hong Kong became a British colony in the 1840s) especially for Chinese studies. There have been major changes the past several decades such as the process of Americanisation, which saw the academic ranks largely changed to the North American system. The higher education system in Macao is much younger as most HEIs were established in the past half a century, with its first university founded in 1981 (the former University of East Asia, which later led to two universities – University of Macau and the City University of Macau). Another major university – Macau University of Science and Technology – was founded in 2000.

References

[1] Yu-Lan Huang, Dian-Fu Chang and Chiung-Wen Liu, "Higher Education in Taiwan: An Analysis of Trends Using the Theory of Punctuated Equilibrium," *Journal of Literature and Art Studies*, 2018, 8(1):169-180, https://doi.org/10.17265/2159-5836/2018.01.018

[2] Education Bureau of the Hong Kong SAR Government, "Post-Secondary Education: Overview," https://www.edb.gov.hk/en/edu-system/postsecondary/index.html

[3] Higher Education Bureau of the Macao SAR Government, "Macao Higher Education Overview," https://www.dses.gov.mo/eng/overview/introduction

Since Hong Kong was returned to China in 1997, a stronger tie has been developed between higher education sectors of Hong Kong and Mainland China, e.g., many universities in Hong Kong have set up campuses or joint research and taught programmes in China, such as the Chinese University of Hong Kong, Shenzhen (CUHK-Shenzhen, 香港中文大学（深圳）, https://www.cuhk.edu.cn/) and the Beijing Normal University-Hong Kong Baptist University United International College (UIC, 北京师范大学-香港浸会大学联合国际学院, https://uic.edu.hk/). Higher education collaborations between Mainland China and Taiwan are much more limited because of the political situation between the two regions. Higher education collaborations between Mainland China and Macao are also relatively limited since the sector is still relatively young in Macao.

Reference

[1] 中华人民共和国教育部 / Ministry of Education of People's Republic of China, 中外合作办学机构与项目 (含内地与港台地区合作办学机构与项目) 名单 / A list of joint taught programmes between Chinese and overseas institutions (including those between institutions in Maindland China and those in Hong Kong and Macau), http://www.crs.jsj.edu.cn/aproval/orglists

Academic Disciplines and Subjects

The academic disciplines and subjects in Taiwan, Hong Kong and Macau are more similar to those in Western countries, but those in Mainland China have more unique features.

In the HE sector of Mainland China, academic subjects are officially defined by the Ministry of Education (MoE) as the authority regulating all (undergraduate, master's and doctoral) degrees awarded by publicly funded HEIs. There are three tiers of academic subjects: the top tier are larger discipline groups (学科门类), followed by Tier 1 and Tier 2 academic subjects (学科类 / 学科 or 一级学科 / 二级学科). According to the latest regulations released in April 2018, there are 13 discipline groups: Philosophy (哲学), Economics (经济学), Law (法学), Education (教育学), Literature (文学), History (历史学), Physical Sciences (理学), Engineering (工学), Agriculture (农学), Medicine (医学), Military Science (军事学), Management (管理学), Arts (艺术学). Before 2011, both Tier 1 and Tier 2 academic subjects were defined by the State Council Academic Degree Committee (SCADC), a body managed by the Ministry of Education but whose head was directly appointed by the State Council (counterpart of the Cabinet Office in the UK). Since 2011, HEIs have been given the permission to self-define Tier 2

subjects for their degree programmes, but they are required to report such self-defined Tier 2 subjects to the MoE. MoE also encourages HEIs to create interdisciplinary subjects, which are treated as special Tier 2 subjects across more than one Tier 1 subject. The following Tier-1 academic subjects are closely related to DDD:

- Education: Psychology (心理学)
- Physical Sciences: Mathematics (数学), Systems Science (系统科学), Statistics (统计学)
- Engineering: Electronic Science and Technology (电子科学与技术), Information and Communication Engineering (信息与通信工程), Control Science and Engineering (控制科学与工程), Computer Science and Technology (计算机科学与技术), Software Engineering (软件工程), Policing Technology (公安技术), Cyber Security (网络空间安全)

In the above list, it deserves mentioning that Cyber Security was added very recently in 2015, one of the most recent additions to the list of Tier 1 subjects. Some of the above Tier 1 subjects are allowed to award degrees in more than one Tier 1 subject depending on the Tier 2 subjects below them, e.g., a Electronic Science and Technology or Computer Science and Technology degree can be under either Engineering or Physical Science, and a Statistics degree can be under either Physical Sciences or Economics.

References

[1] 中华人民共和国教育部 / Ministry of Education of People's Republic of China, 学位授予和人才培养学科目录 (2018 年 4 月更新) / A list of academic subjects for degree certificates and talent training (updated in April 2018), 2018, http://www.moe.gov.cn/s78/A22/xwb_left/moe_833/201804/t20180419_333655.html

[2] 中华人民共和国教育部 / Ministry of Education of People's Republic of China, 国务院学位委员会教育部关于增设网络空间安全一级学科的通知 / Notice on adding "Cyber Security" as a new Tier-1 subject by the State Council Academic Degree Committee and Ministry of Education, 2015, http://www.moe.gov.cn/s78/A22/tongzhi/201511/t20151127_221423.html

[3] 中华人民共和国教育部 / Ministry of Education of People's Republic of China, 授予博士、硕士学位和培养研究生的二级学科自主设置实施细则 / Detailed regulations on self-defined Tier-2 academic subjects for awarding doctoral and master's degrees and for educating postgraduate research students, 24 December 2010, http://www.moe.gov.cn/srcsite/A22/s7065/201012/t20101224_113508.html

[4] 中华人民共和国教育部 / Ministry of Education of People's Republic of China, 学位授予单位（不含军队单位）自主设置二级学科和交叉学科名单 / Lists of Tier-2 academic subjects and interdisciplinary subjects self-defined by HEIs (excluding military organisations), 2020, http://www.moe.gov.cn/jyb_xxgk/s5743/s5744/A22/202008/t20200827_480690.html

In addition to the classification of academic subjects defined by the MoE, Mainland China also has a separate national standard GB/T 13745-2009 that defines a different three-tiered classification and coding system of academic disciplines. This is used more for non-academic purposes, so less relevant for this newsletter.

Reference

[1] 中国标准化研究院 / China National Institute of Standardization, 中华人民共和国学科分类与代码国家标准 / Classification and code disciplines (of People's Republic of China), GB/T 13745-2009, a copy can be downloaded from https://dar.cwnu.edu.cn/__local/D/67/2D/71E79C7A1FDE42DF9B93E9303A7_7518C48A_611CB.pdf

Research Activities

As in many other countries, academic and research staff and research students at a lot of HEIs in Greater China are actively conducting research. Some HEIs are more teaching-focused than others, and how research active an HEI is can be judged based on university ranking based more on research outputs, e.g., the Academic Ranking of World Universities (ARWU,

also known as "Shanghai Ranking", http://www.shanghairanking.com/). The ARWU also maintains a specific ranking of top universities in Greater Asia from 2011 and one for universities in Mainland China only from 2015. For DDD-related research, almost all research-active universities in Greater China have relevant research, so we will not list any specific ones here.

In addition to research activities conducted by HEIs, in Greater China there are also many research institutes. In Mainland China, the following two organisations are of particular importance for DDD-related research:

- China Academy of Sciences (CAS, 中国科学院, http://www.cas.ac.cn/): It is the counterpart of the Royal Society in the UK, and has 12 branches and over 110 affiliated research units (many of which are research institutes focusing on one or more special research disciplines or areas, see https://www.cas.cn/zz/jg/ys/yj/index.shtml for a complete list). Many CAS research institutes conduct DDD-related research, e.g., Institute of Information Engineering (信息工程研究所, http://www.iie.ac.cn/), Institute of Automation (自动化研究所, http://www.ia.cas.cn/), Institute of Software (软件研究所, http://www.iscas.ac.cn/), Institute Of Computing Technology (计算技术研究所, http://www.ict.ac.cn/), and Institute of Psychology (心理研究所, http://www.psych.ac.cn/). The CAS also runs two research-active universities – University of Science and Technology of China (USTC, 中国科学技术大学, https://www.ustc.edu.cn/), and another university focusing on postgraduate research only – University of Chinese Academy of Sciences (UCAS, 中国科学院大学, https://www.ucas.ac.cn/).

- Chinese Academy of Social Sciences (中国社会科学院, http://cass.cssn.cn/): It is Mainland China's national academy in social sciences, with a similar status to the CAS introduced above. It has over 40 affiliated research units, including a number of research institutes conducting DDD-related research – Institute of Linguistic (语言研究所, http://ling.cass.cn/), Institute of Journalism and Communications (新闻与传播研究所, http://xinwen.cssn.cn/) and Institute of Information Studies (信息情报研究院). It runs a university focusing on postgraduate research only – University of Chinese Academy of Social Sciences (中国社会科学院大学, https://www.ucass.edu.cn/).

In addition to CAS and CASS, there are also many other research organisations and centres in Mainland China, which can be classified into three large groups:

- Research organisations owned, managed or directly funded by national or local governments, such as the China Academy of Information Communications Technology (CAICT, 中国信息通信研究院, http://www.caict.ac.cn/) and China Center for Information Industry Development (CCID, 中国电子信息产业发展研究院(赛迪集团), https://www.ccidgroup.com/) managed by the Ministry of Industry and Information Technology (MIIT, 工业和信息化部, https://www.miit.gov.cn/), National Research Centre for Information Technology Security (NITSC, 国家信息技术安全研究中心, http://www.nitsc.cn/) managed by the Cyberspace Administration of China (国家互联网信息办公室, http://www.cac.gov.cn/), the First Research Institute of the Ministry of Public Security (公安部第一研究所, http://www.fri.com.cn/) and the Third Research Institute of the Ministry of Public Security (公安部第三研究所, https://hr.trimps.ac.cn/index.jhtml), Beijing Academy of Science and Technology (BJAST, 北京市科学技术研究院, http://www.bjast.ac.cn/), Shanghai Academy of Science & Technology (SAST, 上海科学院, https://www.sast.org.cn/) and Jiangsu Industrial Technology Research Institute (JITRI, 江苏省产业技术研究院, http://www.jitri.org/).

- Research organisations jointly operated and managed by a number of collaborative organisations including HEIs, commercial bodies and local governments, such as the Zhijiang Lab (之江实验室, https://www.zhejianglab.com/) in Hangzhou, Peng Cheng Laboratory (PCL, 鹏城实验室, http://szpclab.com/), Shenzhen Institute of Artificial Intelligence and Robotics for Society (AIRS, 深圳市人工智能与机器人研究院, https://airs.cuhk.edu.cn/), Shenzhen Institute of

Computing Sciences (SICS, 深圳计算科学研究院, https://www.sics.ac.cn/) and Shenzhen Research Institute of Big Data (SRIBD, 深圳市大数据研究院, http://www.sribd.cn/) in Shenzhen, Sino-Singapore International Joint Research Institute (SSIJRI, 中新国际联合研究院, https://www.ssijri.com/) in Guangzhou, Institute for Interdisciplinary Information Core Technology (IIISCT, 交叉信息核心技术研究院, http://www.iiisct.com/) in Xi'an.

- Research arms of commercial organisations, including those set up by multi-national companies such as Microsoft Research Asia (https://www.microsoft.com/en-us/research/lab/microsoft-research-asia/) and IBM Research –China (https://www.research.ibm.com/labs/china/) in Beijing, and those by Chinese firms such as Tencent Research Institute (腾讯研究院, https://www.tisi.org/), Ali Research (阿里研究院, http://www.aliresearch.com/), Baidu Research (百度研究院, http://research.baidu.com/), 360 Network Security Lab (360 网络安全研究院, https://www.netlab.360.com/), and ByteDance AI Lab (字节跳动人工智能实验室, https://ailab.bytedance.com/).

In Taiwan, the Academia Sinica (中央研究院, https://www.sinica.edu.tw/) is of particular importance. This is the counterpart of the CAS in Mainland China, and the name was originated from a similar body of the Republic of China before 1949. A number of Academia Sinica's research units conduct DDD-related research, including Institute of Information Science (資訊科學研究所, https://www.iis.sinica.edu.tw/), Research Center for Information Technology (資訊科技創新研究中心, https://www.citi.sinica.edu.tw/), and Institute of Linguistics (語言學研究所, http://www.ling.sinica.edu.tw/). Another important research organisation in Taiwan is the Industrial Technology Research Institute (ITRI, 工業技術研究院, https://www.itri.org.tw/), one of the largest research organisations in Taiwan with relevant research activities. Other relevant research organisations include the Institute for National Defense and Security Research (INDSR, 國防安全研究院, https://indsr.org.tw/), National Chung-Shan Institute of Science and Technology (NCSIST, 國家中山科學研究院, https://www.ncsist.org.tw/), and Cybersecurity Technology Institute (CSTI, 資安科技研究所) of the Institute for Information Industry (III, 資訊工業策進會, https://www.iii.org.tw/).

In Hong Kong, in addition to research conducted at HEIs, the Hong Kong Applied Science and Technology Research Institute (ASTRI, 香港應用科技研究院, https://www.astri.org/) is an important government-funded R&D centre focusing on information and communications technologies, which covers both cyber security and AI – two major areas related to DDD research. In Macao, research activities is mainly conducted at HEIs.

References

[1] Hong Kong Innovation and Technology Commission (ITC), "Research & Development Centres," https://www.itc.gov.hk/en/resources/res_dev_centre.html

[2] Macao SAR Government Portal, search results using the keyword "research", https://www.gov.mo/en/global-search/?q=research

In addition to research organisations and centres, there are also many relevant learned societies and professional associations in Greater China, covering research topics related to DDD. Some notable examples include the China Computer Federation (CCF, 中国计算机学会, https://www.ccf.org.cn/), Chinese Association for Artificial Intelligence (CAAI, 中国人工智能学会, http://www.caai.cn/), Chinese Association of Automation (CAA, 中国自动化学会, http://caa.org.cn/), Chinese Institute of Electronics (CIE, 中国电子学会,https://cie-info.org.cn/), CyberSecurity Association of China (CSAC, 中国网络空间安全协会, https://www.cybersac.cn/), Chinese Information Processing Society of China (CIPSC, 中国中文信息学会, http://www.cipsc.org.cn/), China Institute of Communications (China-CIC, 中国通信学会, http://www.china-cic.cn/), Internet Society of China (ICS, 中国互联网协会), Chinese Psychological Society (CPS, 中国心理学会, https://www.cpsbeijing.org/), Computer Society of the Republic Of China (CSROC, 中華民國電腦學會, http://www.csroc.org.tw/), Association for Computational Linguistics and Chinese Language Processing (ACLCLP, http://www.aclclp.org.tw/), Taiwanese Psychological Association (TPA, 台灣心理學會, https:

//www.tpa-tw.org/), Hong Kong Computer Society (HKCS, 香港電腦學會, http://www.hkcs.org.hk/), Hong Kong Psychological Society (HKPS, 香港心理學會, https://hkps.org.hk/), and Macao Computer Society (MCS, 澳門電腦學會, http://www.mcs.mo/).

Scientific Publishing

According to the language used and the publication venue, Chinese researchers in Greater China publish their scientific results in different ways:

- English publications published at international venues: Such publications are basically the same as how non-Chinese researchers publish their research papers in English.

- English publications published at venues owned or managed by Chinese organisations: Many HEIs, learned societies and research organisations in Greater China publish scientific journals and organise scientific conferences. Some such venues publish all papers in English, and some publish papers written in English and Chinese. Many Chinese journals also have a dedicated English version, which are mostly a completely independent journal (e.g., *Chinese Journal of Electronics*, the English counterpart of the Chinese journal *Acta Electronica Sinica* / 《电子学报》, both owned by the Chinese Institute of Electronics / 中国电子学会). Some scientific journals of this kind are jointly published with major international scientific publishers, and welcome submissions from international researchers. One example is *Science China Information Sciences*, which is jointly published by Science China Press (中国科学出版社) and Springer Nature Switzerland AG.

- Chinese publications published in Chinese journals and conference proceedings: Such Chinese publications normally have an English title and abstract, which allow international scientific services to index selected papers.

A quite unique feature of scientific publishing in Mainland China is that most research-active HEIs have their own journals, some of which have an English version as well. One such English journal is *Tsinghua Science and Technology*, jointly published by the Tsinghua University Press (清华大学出版社) and Elsevier B.V. (see https://www.sciencedirect.com/journal/tsinghua-science-and-technology). For HEIs whose research covers multiple disciplines or discipline groups, they often have different editions of their own journals with different ISSNs, e.g., *Journal of Tsinghua University (Science and Technology)* (《清华大学学报（自然科学版）》, http://jst.tsinghuajournals.com/CN/1000-0054/home.shtml).

Scientific Services in Greater China

All major international scientific services such as Web of Science, Scopus and those provided by major scientific publishers (e.g., Ei Compendex of Elsevier, and Inspec of IET) are also widely used in Greater China. Most of them do index Chinese papers as well, and rely on the English title and abstract to provide sensible summaries of such papers to non-Chinese readers.

In addition to international ones, there are some Chinese scientific services dedicated to cover research publications published in Chinese. There are three major categories of scientific services that are of relevance to DDD research:

- Scientific publishing systems: They are used by scientific journals and conferences to publish papers and sometimes for managing editorial matters of such venues. In Mainland China, two systems are of particular importance because they collectively cover almost all important scientific journals published in Mainland China with a paid fulltext access service: China National Knowledge Infrastructure (CNKI, 中国知网, https://oversea.cnki.net/) and the Wanfang Data Knowledge Service Platform (万方数据知识服务平台, http://www.wanfangdata.com.cn/). Both services also cover some other types of scientific outputs, including master's and PhD theses, conference papers, technical reports, books, standards, patents and relevant regulations published in Mainland China. Another two similar services are VIP Chinese Journal Service Platform (维普资讯中文期刊服务平台, http://qikan.cqvip.com/) and Chaoxing Journals

(超星期刊, http://qikan.chaoxing.com/). For Chinese research papers, theses and books published in Taiwan, the Airiti Library (華藝線上圖書館 / 台湾学术文献数据库, http://www.airitilibrary.cn/), Taiwan Scholar Journal Database (TWS, 台湾学术期刊在线数据库, http://www.twscholar.com/), Taiwan Academic Book Database (TWBOOK, 台湾学术书籍数据库, http://books.twscholar.com/) and HyRead Journal (台灣全文資料庫, https://www.hyread.com.tw/) provide a very good coverage. For Chinese scientific journals published in Hong Kong and Macao, the Hong Kong Index to Chinese Periodicals (HKInChiP, 香港中文期刊論文索引, http://hkinchippub.lib.cuhk.edu.hk/) and Hong Kong Macau Periodicals Network (港澳期刊網, http://hkmpnpub.lib.cuhk.edu.hk/) managed by the Chinese University of Hong Kong (香港中文大學) covers over 300 journals mainly in social sciences and sociology (because papers in those fields are more likely written in Chinese). Another such database is Hong Kong Journals Online (HKJO, https://hkjo.lib.hku.hk/) managed by the University of Hong Kong Libraries, which cover selected academic and professional journals published in Hong Kong, both in English and Chinese.

- Scientific indexing services: Similar to Web of Science and Scopus, there are services in Greater China indexing Chinese research papers. Some major indexing services include Chinese Science Citation Database (CSCD, 中国科学引文数据库, http://www.sciencechina.cn/search_sou.jsp) which is part of Science China (中国科学文献服务系统, http://sciencechina.cn/) managed by the Natural Science Library of CAS (中国科学院文献情报中心, http://www.las.cas.cn/), Chinese Social Sciences Citation Index (CSSCI, 中国社会科学引文索引, http://cssci.nju.edu.cn/), CNKI Chinese Citation Database (中国知网中国引文数据库, https://ref.cnki.net/), and Taiwan Citation Index – Humanities and Social Sciences (TCI-HSS, 臺灣人文及社會科學引文索引, https://tci.ncl.edu.tw/).

- Scientific preprint servers: Many Chinese researchers use international preprint servers such as arXiv (https://arxiv.org/), IACR's Cryptology ePrint Archive (https://eprint.iacr.org/), Elsevier's SSRN (https://www.ssrn.com/), PsyArxiv (https://psyarxiv.com/) and CogPrints (http://cogprints.org/) to publish their pre-prints in English. These international preprint servers do not normally accept papers written in Chinese, so services dedicated to Chinese preprints have been created. Three such preprint servers in Mainland China include the Sciencepaper Online (中国科技论文在线, http://www.paper.edu.cn/) managed by the MoE of Mainland China, ChinaXiv (中国科学院科技论文预发布平台, http://chinaxiv.org/) managed by the National Science Library, Chinese Academy of Sciences, and PsyChinaXiv (中国心理学预印本平台, http://psych.chinaxiv.org/) managed by the Institute of Psychology, Chinese Academy of Sciences. We were not aware of any preprint servers in Taiwan, Hong Kong or Macao, which are dedicated to support Chinese preprints.

References

[1] 浙江大学图书馆 / Zhejiang University Library, "数据库导航 / Guidance for Databases," http://210.32.137.90/s/lib/libtb

[2] Chinese University of Hong Kong Library / 香港中文大學圖書館, "A-Z Databases," https://libguides.lib.cuhk.edu.hk/az.php

[3] Chinese University of Hong Kong Library / 香港中文大學圖書館, "香港中文期刊論文索引 (HKInChiP) / Hong Kong Index to Chinese Periodicals (HKInChiP)," http://hkinchippub.lib.cuhk.edu.hk/

[4] University of Macau Library / 澳門大學伍宜孫圖書館, "Macau Periodical Index (澳門期刊論文索引)," http://libdigital.umac.mo/macau_periodical/journal_title

[5] The Hong Kong University Libraries / 香港大學圖書館, "Pre-print servers," https://libguides.lib.hku.hk/preprint

Selected Chinese Research Papers: AI-related Work

Introduction

To select Chinese research papers, we decided to follow the same systematic literature review procedure of Issue 1, using Scopus as the database as it covers a significant number of high-quality Chinese journals. We also decided to focus on AI-related papers only to be more focused for this issue. We will cover other topics in future issues. Out of all papers returned from Scopus, we identified five papers whose publishers have made their fulltexts publicly available. Two papers selected are surveys and the other three report original research. In the references we also include 13 English papers cited from the five Chinese papers, in order to put the summaries of the Chinese papers into the context of related research outside of Greater China. For all five Chinese papers, we do not include their DOI links because they do not provide a way to download the fulltext. Instead, we include separate URLs on the official websites of the corresponding journals, which provide open access to the papers' fulltexts.

Deepfake Detection: A Survey

Liang (梁瑞刚) et al. [11] gave a survey of audio and visual deepfake detection methods. They first introduced different techniques for generating visual and audio deepfakes. For visual deepfeakes, they used Figure 1 to show a typical procedure of training (a) and generating (b) visual deepfakes (forged facial images), based on GAN (Generative Adversarial Network) encoders and decoders for two persons (Alice and Bob), where the deepfakes are generated by replacing Alice's decoder with Bob's. For audio deepfakes, they briefly explained some typical methods, based on techniques including HMM (Hidden Markov Model), DAE (Denoising Autoencoder) and AR (Autoregressive Model), and a number of recent papers exploring the use of deep learning for

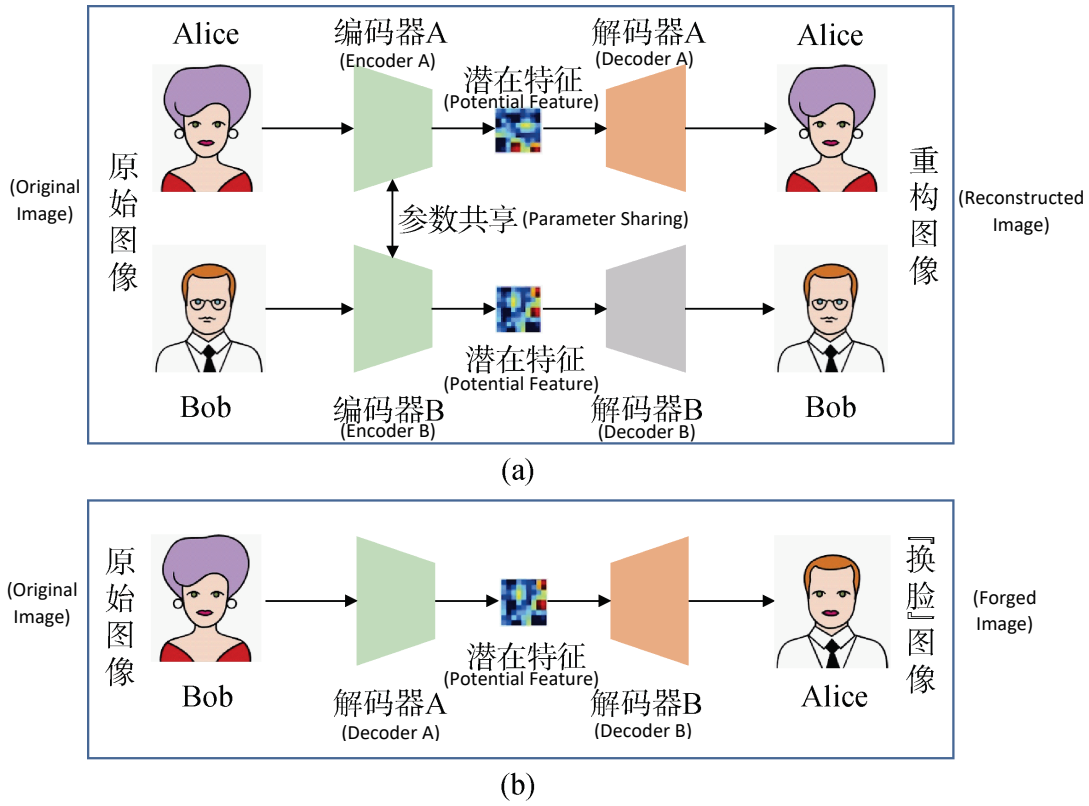


Figure 1: A typical procedure of training (a) and generating (b) visual deepfakes summarised by Liang (梁瑞刚) et al. [11].

audio deepfake generation. For deepfake detection methods, the authors looked at methods for different deepfake data types separately: images, videos and audio/speech. For detection of deepfake images, they classified existing methods into four categories: 1) traditional image forensics-based methods; 2) methods based on customising the CNN architecture; 3) methods based on comparison of differential features between real and forged images; and 4) methods based on detecting unique fingerprints of deepfake GANs. For detection of deepfake videos, they classified existing methods into two categories: 1) methods based on analysis of abnormal temporal (inter-frame) features; 2) methods based on analysis of abnormal spatial (intra-frame) features. For detecting deepfake audio/speech, this paper just reviewed a number of recent papers, mostly around responses to the ASVspoof 2019 competition organised at Interspeech 2019 conference. A more detailed survey on detection of speech spoofing including but not limited to deepfakes [18] is also included in this issue (see below). In addition, the authors also reviewed 15 available deepfake datasets, as shown in Table 2 of [18]. Finally, a number of techniques related to deepfake detection were discussed, including adversarial AI, digital watermarking and AI explainability.

Editorial Comments

This paper includes a blockchain and smart contract based deepfake video detection method. However, it is not actually about detecting deepfakes, but simply provides a way for storing useful information that can facilitate verification of originality of a given video. We do not consider this a relevant part of deepfake detection, so did not include it in the above summary.

Speech Anti-spoofing: A Survey

Zhang (张雄伟) et al. [18] reviewed the state-of-the-art of speech anti-spoofing against automatic speaker verification (ASV) systems. They first discussed four main speech spoofing methods, speech/voice imitation/mimicry by a human impersonator, playback of pre-recorded speech, generating impersonating speech using TTS (Text-to-speech) and voice conversion (VC) techniques, and pointed out that the last two (more advanced) methods pose a bigger challenge to ASV systems. Since the first spoofing method relies on the skill of a human impersonator and there are no available datasets for this particular type of spoofing, for anti-spoofing the authors focused more on the other three methods. They observed that anti-spoofing is generally a step before and independent of the ASV system itself, and summarised its general architecture as shown in Figure 2. They also recommended combining different anti-spoofing methods to increase the detection rate if the spoofing method is unknown. Regarding the evaluation metrics, the authors considered FRR (false rejection rate), FAR (false accept rate), and EER (equal error rate). In terms of datasets, they focused on the three speech spoofing datasets produced for the ASVspoof competitions at the Interspeech conference since 2015 (`https://www.asvspoof.org/database`): ASVspoof 2015 dataset covering TTS- and VC-based spoofing, ASVspoof 2017 dataset covering speech playback-based spoofing, and ASVspoof 2019 covering all three spoofing methods.

Zhang (张雄伟) et al. pointed out that spoofing-specific features are needed for detection purposes, which include constant Q cepstral coefficient (CQCC), linear frequency cepstral coefficient (LFCC), Cochlear filter cepstral coefficients instantaneous frequency (CF-CC-IF), group delay gram

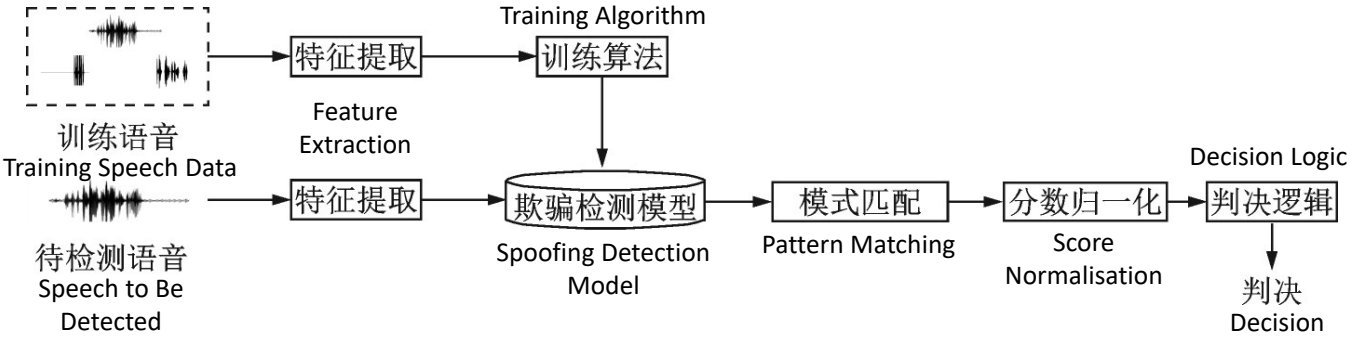


Figure 2: The general architecture of speech anti-spoofing given by Zhang (张雄伟) et al. in [18].

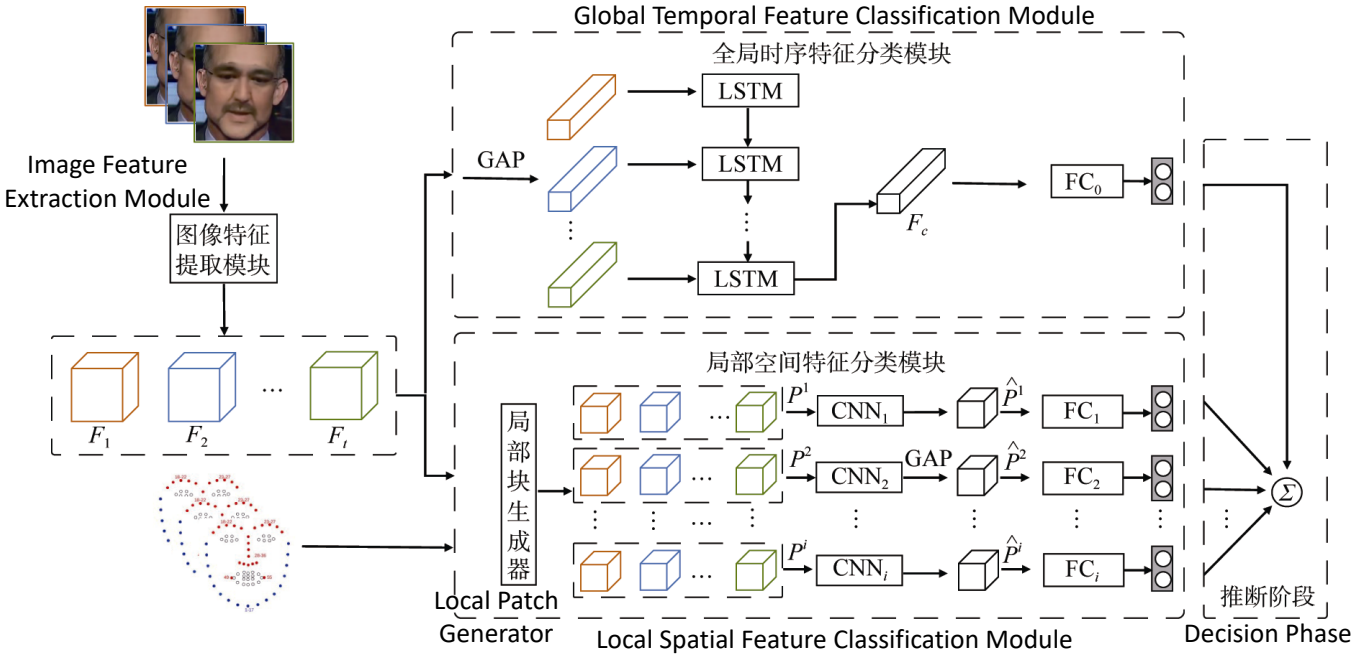


Figure 3: The architecture of Chen (陈鹏) et al.'s proposed method for detecting forged facial videos [4].

(GD-gram), and single frequency filtering cepstral coefficient (SFFCC). They reviewed many different anti-spoofing methods including those based on traditional machine learning methods such as GMM (Gaussian Mixture Model), i-vector, SVM (Support Vector Machine) and PLDA (probabilistic linear discriminant analysis), and also more recent ones based on deep learning techniques such as DNN (Deep Neural Network), CNN (Convolution Neural Network) and RNN (Recurrent Neural Network) and TDNN (Time Delay Neural Network). Using the ASVspoof datasets as the benchmark, many anti-spoofing methods have proven very effective, but the authors identified three directions for further studies: i) robustness of anti-spoofing in more realistic and complicate scenarios; ii) universal anti-spoofing that does not rely on knowledge of spoofing methods; iii) joint anti-spoofing and speaker recognition.

Detection of Forged Facial Videos

Chen (陈鹏) et al. [4] proposed a novel method based the combination of two classification modules, one on global temporal features and the other on local spatial features, for detecting forged facial videos. They proposed to use the VGG16 network without the last pooling layer and the fully-connected layer to extract image features, from an 224×224 facial image extracted from each video frame based on 68 key points. The extracted features are fed to both classification modules for separate processing. For the global temporal feature classification module, a three-step process is followed: a GAP (Global Average Pooling) step is used to compress the spatial information into 512 features, an LSTM (Long Short Term Memory) network takes the 512 features as the input to generate learned temporal features F_c, which passes a fully connected (FC) layer and a softmax normalisation step to produce a decision score S_c summarising the global temporal features. For the local spatial feature classification module, 12 out of the 68 key points are used to general local patches, which are processed by separate CNNs each followed by a GAP layer, a FC layer and softmax normalisation step to produce a number of decision scores $\{S_i\}$ summarising the local spatial features. All decision scores from the two classification modules are finally fused as a weighted sum, which is used to generate the final detection decision. A diagrammatic view of the proposed method can be seen in Figure 3. The authors used 1,000 original videos from the FaceForensics++ dataset [14] and four recent facial video forgery methods (the first two are computer graphics based methods and the other two are deepfake methods) – FaceSwap [9], Face2Face [16], Deepfakes [6] and NeuralTextures [17] – to generate 1,000 forged videos for each method. All videos were compressed using a moderate compression parameter of H.264

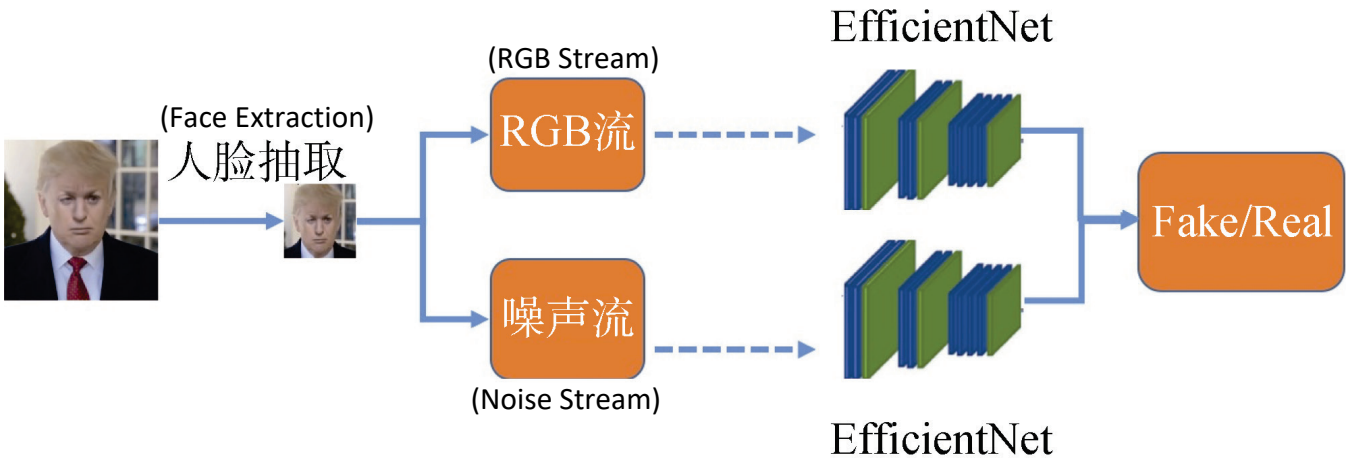


Figure 4: The two-network deepfake video detection framework proposed by Li (李旭嵘) and Yu (于鲲) [10].

encoding. To compare the performance of the proposed method, the authors used two four simpler settings – two base-line settings without any of the classification modules and two with each of the two classification modules alone, and showed that combining the two classification modules outperformed all other simpler settings. They then showed that their proposed method had achieved an accuracy of over 99% for three facial video forgery methods (DeepFakes, Face2Face and FaceSwap), and over 95% for the last one (NeuralTextures), higher than four state-of-the-art detection methods [1, 2, 5, 14] with a significant margin.

Editorial Comments

The experimental results showed that even for much simpler settings (e.g., just using the image feature extraction module with an GAP layer and an FC layer) the proposed detection method also performed very well, just slightly worse than the complicated setting with two classification modules combined.

Li (李旭嵘) and Yu (于鲲) [10] proposed a new deepfake video detection method based on the idea of a two-stream network, i.e., two streams of features representing different aspects of the input video, which are processed independently and then the results fused to make the final decision. The proposed two-stream network was based on EfficientNet [15], with one stream carrying the normal RGB information (i.e., original pixel values) and the second carrying the filtered noise information, as shown in Figure 4. The main hypothesis of the authors is that adding the noise stream can effectively increase the performance of the detection method. To test the performance of their proposed method, the authors used the same setting as in [4]: the FaceForensics++ dataset [14], the four facial video forgery methods – Deepfakes [6], FaceSwap [9], Face2Face [16] and NeuralTextures [17], and 1,000 forged videos for each method. All videos were compressed using three parameters (corresponding to raw video, low and high compression rates) of H.264 encoding, leading to 15,000 videos in total. The authors showed that adding the noise stream did help increase the performance with a significant margin, and then gave results of the proposed method on all $3 \times 4 = 12$ settings (H.264 compression and four facial video forgery methods), showing an accurate rate bewteen 93.57% to 100%. They also compared the performance of their method with that of the Xception method (the one provided in the FaceForensics++ dataset), and showed that the former significantly outperformed the latter, particularly under the high-compression setting (97.57% vs. 85.49%).

Editorial Comments

Both [4] and [10] were published very recently, so neither papers has a comparison of the two method's performance. The forged videos used in both papers are different, so we cannot directly compare the results. Assuming the accuracy figures are generalisable, we predict that the two proposed methods have a comparable performance.

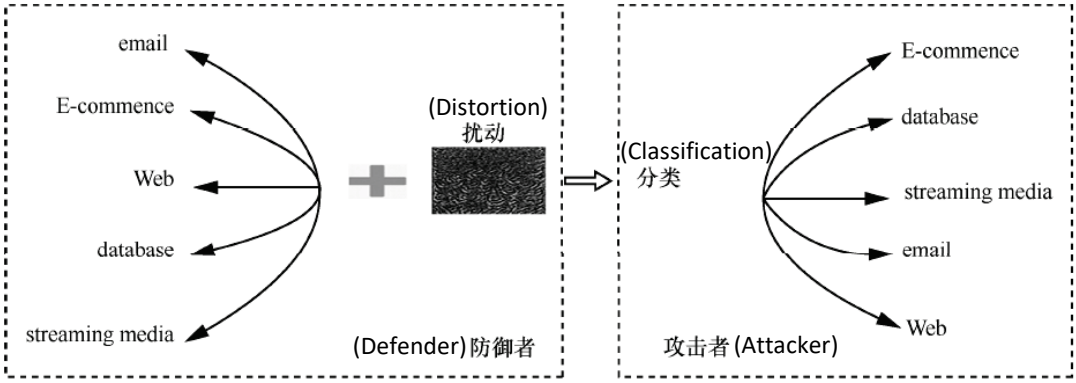


Figure 5: The attack and defence scenario considered by Hu (胡永进) et al. [8].

Adversarial Sample Generation

Hu (胡永进) et al. [8] looked at the problem of an attacker being able to classify network flows between two network nodes to launch targeted traffic blocking and fingerprinting attacks. They proposed to use adversarial samples as an defensive measure to prevent such attacks based on traffic classification. The attack and defence scenario is illustrated in Figure 5. The authors used network flows in the 2005 Moore dataset reported in [12], which includes 377,526 network flows generated by over 1,000 university staff on a 1GB network on 20th August, 2003. The authors classified the flows into 12 classes. A modified LeNet-5 CNN model was then used to build an attacker classification model, which consisted of one input layer, two convolutional layers, two pooling layers, one fully connected layer and one output layer. The classification accuracy of this attacker model was reported to be 99.04% on the Moore dataset. Based on the white-box assumption (the defender knows the attacker model), three adversarial sample generation methods – FGSM (Fast Gradient Sign Method) [7], DeepFool [13] and C&W (Carlini and Wagner) [3] – were used to add noises to the original flows, and then tested to see if they can mislead the attacker model to mis-classify network flows. The experimental results showed that all three methods are effective with an overall success rate of 99.05%, 97.38% and 67.97%, respectively. While the C&W method has the lowest success rate, it was the most efficient among the three.

Editorial Comments

Although the paper reports very good results, the white-box assumption can be less practical in realistic scenarios because attacks are often unknown. In addition, the authors did not make it clear how to apply adversarial samples to the network traffic without affecting normal functionalities of the network. This can be even more difficult when the attack is unknown as we will not know where to deploy the adversarial samples. We therefore suggest that the work reported is not mature and that further research is necessary to make it ready for real-world applications.

References

[1] Darius Afchar, Vincent Nozick, Junichi Yamagishi, and Isao Echizen. 2018. MesoNet: a Compact Facial Video Forgery Detection Network. In *Proceedings of 2018 IEEE International Workshop on Information Forensics and Security*. IEEE, 7. https://doi.org/10.1109/WIFS.2018.8630761

[2] Belhassen Bayar and Matthew C. Stamm. 2016. A Deep Learning Approach to Universal Image Manipulation Detection Using a New Convolutional Layer. In *Proceedings of the 4th ACM Workshop on Information Hiding and Multimedia Security*. ACM, 5–—10. https://doi.org/10.1145/2909827.2930786

[3] Nicholas Carlini and David Wagner. 2017. Towards Evaluating the Robustness of Neural Networks. In *Proceedings of 2017 IEEE Symposium on Security and Privacy*. IEEE, 39–57. https://doi.org/10.1109/SP.2017.49

[4] Peng Chen (陈鹏), Tao Liang (梁涛), Jin Liu (刘锦), Jiao Dai (戴娇), and Jizhong Han (韩冀中). 2020. Forged Facial Video Detection Based on Global Temporal and Local Spatial Feature / 融合全局时序和局部空间特征的伪造人脸视频检测方法. *Journal of Cyber Security* / 《信息安全学报》 5, 2 (2020), 73–83. http://jcs.iie.ac.cn/xxaqxb/ch/reader/create_pdf.aspx?file_no=20200207&flag=1&year_id=2020&quarter_id=2

[5] Davide Cozzolino, Giovanni Poggi, and Luisa Verdoliva. 2017. Recasting Residual-based Local Descriptors as Convolutional Neural Networks: An Application to Image Forgery Detection. Online pre-print, arXiv:1703.04615 [cs.CV]. https://arxiv.org/abs/1703.04615

[6] deepfakes. [n.d.]. FaceSwap. Online code repository. https://github.com/deepfakes/faceswap (The repository has been actively updated and the last update was in 2020. In [4] and [10], for this reference the year was 2017 and 2019, respectively.).

[7] Ian J. Goodfellow, Jonathon Shlens, and Christian Szegedy. 2014. Explaining and Harnessing Adversarial Examples. Online pre-print, arXiv:1412.6572 [cs.CV]. https://arxiv.org/abs/1909.11573

[8] Yongjin Hu (胡永进), Yuanbo Guo (郭渊博), Ma (马骏) Jun, Han Zhang (张晗), and Xiuqing Mao (毛秀青). 2020. Method to Generate Cyber Deception Traffic Based on Adversarial Sample / 基于对抗样本的网络欺骗流量生成方法. *Journal on Communications* / 《通信学报》 41, 9 (2020), 59–70. http://www.infocomm-journal.com/txxb/CN/10.11959/j.issn.1000-436x.2020166

[9] Marek Kowalski. 2015. FaceSwap. Online code repository. https://github.com/MarekKowalski/FaceSwap

[10] Xurong Li (李旭嵘) and Kun Yu (于鲲). 2020. A Deepfakes Detection Technique Based on Two-stream Network / 一种基于双流网络的 Deepfakes 检测技术. *Journal of Cyber Security* / 《信息安全学报》 5, 2 (2020), 84–91. http://jcs.iie.ac.cn/xxaqxben/ch/reader/create_pdf.aspx?file_no=20200208&year_id=2020&quarter_id=2&falg=1

[11] Ruigang Liang (梁瑞刚), Peizhuo Lv (吕培卓), Yue Zhao (赵月), Peng Chen (陈鹏), Hao Xing (邢豪), Yingjun Zhang (张颖君), Jizhong Han (韩冀中), Ran He (赫然), Xianfeng Zhao (赵险峰), Ming Li (李明), and Kai Chen (陈恺). 2020. A Survey of Audiovisual Deepfake Detection Techniques / 视听觉深度伪造检测技术研究综述. *Journal of Cyber Security* / 《信息安全学报》 5, 2 (2020), 1–17. http://jcs.iie.ac.cn/xxaqxb/ch/reader/create_pdf.aspx?file_no=20200202&flag=1&year_id=2020&quarter_id=2

[12] Andrew Moore, Denis Zuev, and Michael Crogan. 2014. *Discriminators for use in flow-based classification*. Technical Report RR-05-13. Department of Computer Science, Queen Mary University of London, UK. https://qmro.qmul.ac.uk/xmlui/handle/123456789/5050

[13] Seyed-Mohsen Moosavi-Dezfooli, Alhussein Fawzi, and Pascal Frossard. 2016. DeepFool: A Simple and Accurate Method to Fool Deep Neural Networks. In *Proceedings of 2016 IEEE Conference on Computer Vision and Pattern Recognition*. IEEE, 2574–2582. https://doi.org/10.1109/CVPR.2016.282

[14] Andreas Rössler, Davide Cozzolino, Luisa Verdoliva, Christian Riess, Justus Thies, and Matthias Niessner. 2019. FaceForensics++: Learning to Detect Manipulated Facial Images. In *Proceedings of 2019 IEEE/CVF International Conference on Computer Vision*. IEEE, 11. https://doi.org/10.1109/ICCV.2019.00009 (The dataset can be downloaded at https://github.com/ondyari/FaceForensics.).

[15] Mingxing Tan and Quoc V. Le. 2019. REfficientNet: Rethinking Model Scaling for Convolutional Neural Networks. In *Proceedings of the 36th International Conference on Machine Learning*. ML Research Press, 10. http://proceedings.mlr.press/v97/tan19a.html (In [4], this paper was cited as an arXiv.org preprint at https://arxiv.org/abs/1905.11946.).

[16] Justus Thies, Michael Zollhofer, Marc Stamminger, Christian Theobalt, and Matthias Niessner. 2016. Face2Face: Real-Time Face Capture and Reenactment of RGB Videos. In *Proceedings of 2016 IEEE Conference on Computer Vision and Pattern Recognition*. IEEE, 2387–2395. https://doi.org/10.1109/CVPR.2016.262

[17] Justus Thies, Michael Zollhöfer, and Matthias Nießner. 2019. Deferred Neural Rendering: Image Synthesis Using Neural Textures. *ACM Transactions on Graphics* 38, 4, Article 66 (2019), 12 pages. https://doi.org/10.1145/3306346.3323035 (Part of Proceedings of SIGGRAPH 2019. In [4] and [10], this paper was cited as https://arxiv.org/abs/1904.12356.).

[18] Xiongwei Zhang (张雄伟), Jiakang Li (李嘉康), Meng Sun (孙蒙), and Linlin Zheng (郑琳琳). 2020. Speech Anti-spoofing: The State of the Art and Prospects / 语音欺骗检测方法的研究现状及展望. *Journal of Data Acquisition and Processing* / 《数据采集与处理》 35, 5 (2020), 807–823. http://sjcj.nuaa.edu.cn/ch/reader/create_pdf.aspx?file_no=202005002&year_id=2020&quarter_id=5&flag=1