The Future of Deception: Machine-Generated and Manipulated Images, Video, and Audio?

Jonathan Z. Bakdash
U.S. Army Research Laboratory South Field Element at the University of Texas Dallas
Richardson, TX
jonathan.z.bakdash.civ@mail.mil

Char Sample
ICF for the U.S. Army Research Laboratory
Adelphi, MD
Char.Sample@icf.com

Monica Rankin
School of Arts and Humanities University of Texas Dallas
Richardson, TX
mrankin@utdallas.edu

Murat Kantarcioglu
Department of Computer Science University of Texas Dallas
Richardson, TX
muratk@utdallas.edu

Jennifer S. Holmes
School of Economic, Political and Policy Sciences University of Texas Dallas
Richardson, TX
jholmes@utdallas.edu

Sue Kase
Computational and Information Sciences Directorate U.S. Army Research Laboratory
Aberdeen Proving Ground, MD
sue.e.kase.civ@mail.mil

Erin Zaroukian
Computational and Information Sciences Directorate U.S. Army Research Laboratory
Aberdeen Proving Ground, MD
erin.g.zaroukian.ctr@mail.mil

Boleslaw K. Szymanski
Department of Computer Science and Network Science and Technology (NeST) Center RPI, Troy, NY
boleslaw.szymanski@gmail.com

Keywords—deception, propaganda, fake news, machine-generated information, social sensing

VISION STATEMENT

Social sensing techniques were designed for analyzing unreliable data [1], but not explicitly built for adversarial generated and manipulated data. The adversarial use of social media to spread deceptive or misleading information poses a social, economic, and political threat [2]. Deceptive information spreads quickly and inexpensively online relative to traditional methods of dissemination (e.g., print, radio, and television). For example, bots (i.e., dedicated software for sharing text information [3]) can distribute information faster than humans. Such deceptive information is commonly referred to as fake (fabricated) news, which can be a form of propaganda (i.e., manipulation to advance a particular view or agenda). Information spread is particularly effective if the content resonates with the preconceptions and biases of social groups or communities because the spread will be reinforced by implied trust in information coming from other members (echo chambers and filter bubbles) [4].

We conjecture that the future of online deception, including fake news, will extend beyond text to high-quality, mass-produced machine-generated and manipulated images, video, and audio [5]. Visual and auditory information tend to be far more persuasive to people than text. Recent advances in machine learning and hardware (Graphic Processing Units) demonstrate that increasingly realistic deception is fast becoming possible without specialized capabilities [6], [7], see Fig. Although the fake Obama video is a benign example of machine-generated and manipulated information, it alludes to unlimited malicious possibilities for incredibly compelling deception (e.g., creating false statements from politicians, manufacturing fictitious events such as protests).

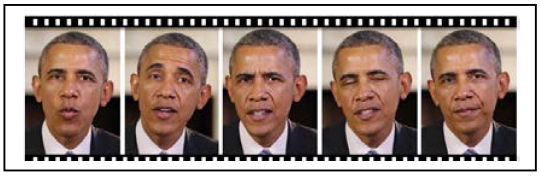

Fig. Stills from the output of machine-synthesized video and audio of former U.S. President Obama. Source: Fig 1. in [6]. Link to the fake Obama video: https://www.youtube.com/watch?v=9Yq67CjDqvw

Mitigating the threats for these new forms of deception requires developing social sensing techniques for *adversarial* visual and auditory content, including methods for detection of manipulation/generation as well as fusion and provenance. Combining computational social sensing with human judgments may be more effective than either alone. Humans can provide insights that are not captured computationally (e.g., the context and meaning of information) and vice-versa. Unchecked propaganda, in fake news and other forms, has the potential to undermine public confidence in institutions, including governments, and democracy itself [8].

REFERENCES

[1] D. Wang, B. K. Szymanski, T. Abdelzaher, H. Ji, and L. Kaplan, "The age of social sensing," *IEEE Computer*, in press.
[2] "The global risks report 12th Ed," World Economic Forum, 2017.
[3] S. C. Woolley and P. N. Howard, *Computational propaganda worldwide: Executive summary*. Oxford: Oxford Internet Institute, University of Oxford, 2017.
[4] M.T. Al Amin, T. Abdelzaher, D. Wang, and B.K. Szymanski, "Crowd-sensing with polarized sources," *Proc. IEEE DCOSS*, 2014, pp. 67-74.
[5] O. Solon, "The future of fake news: Don't believe everything you read, see or hear," *The Guardian*, 26-Jul-2017. [Online]. Available from: http://www.theguardian.com/technology/2017/jul/26/fake-news-obama-video-trump-face2face-doctored-content. [Accessed: 25-Jan-2018].
[6] S. Suwajanakorn, S. M. Seitz, and I. Kemelmacher-Shlizerman, "Synthesizing Obama: Learning lip sync from audio," *ACM Transactions on Graphics*, vol. 36, no. 4, pp. 1–13, Jul. 2017.
[7] T. Karras, T. Aila, S. Laine, and J. Lehtinen, "Progressive growing of GANs for improved quality, stability, and variation," *arXiv:1710.10196 [cs, stat]*, Oct. 2017.
[8] American Views: Trust, media, and democracy. Gallup/Knight. [Online]. Available from: https://knightfoundation.org/reports/american-views-trust-media-and-democracy [Accessed: 5-Feb-2018].

The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the U.S. Army Research Laboratory (ARL) or the U.S. government.

M.K. was supported by ARL under grant W911NF-17-1-0356 and B.S. by ARL under grant W911NF-16-1-0524. E.Z. was supported by an appointment to the ARL Postdoctoral Fellowship Program administered by the Oak Ridge Associated Universities under cooperative agreement W911NF-17-003.

0-7695-6411-9/18/$31.00 ©2018 IEEE
DOI 10.1109/SocialSens.2018.00009