NISTIR 8396

Open Media Forensics Challenge (OpenMFC) 2020-2021: Past, Present, and Future

Haiying Guan
Yooyoung Lee
Lukas Diduch
Jesse G. Zhang
Ilia Ghorbanian
Timothee Kheyrkhah
Peter C. Fontana
Jon Fiscus
James Filliben

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8396

National Institute of Standards and Technology
U.S. Department of Commerce

NISTIR 8396

Open Media Forensics Challenge (OpenMFC) 2020-2021: Past, Present, and Future

Haiying Guan
Yooyoung Lee
Lukas Diduch
Jesse G. Zhang
Ilia Ghorbanian
Timothee Kheyrkhah
Peter C. Fontana
Jon Fiscus
Multimodal Information Group
Information Access Division

James Filliben
Statistical Engineering Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8396

September 2021

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce for Standards and Technology & Director, National Institute of Standards and Technology

National Institute of Standards and Technology Interagency or Internal Report 8396
Natl. Inst. Stand. Technol. Interag. Intern. Rep. 8396, 33 pages (September 2021)

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8396

Abstract

This document describes the online leaderboard public evaluation program, Open Media Forensics Challenge (OpenMFC) 2021-2022. OpenMFC is the annual evaluation open to public participants worldwide to support research and help advance the state of the art for imagery (i.e., images and videos) forensics technologies. Participation is free. NIST does not provide funds to participants.

To facilitate development of systems that can automatically detect and locate manipulations in imagery, OpenMFC releases a series of media forensics development and evaluation datasets to support different evaluation tasks. The evaluation is being conducted to examine the performance of system's accuracy and robustness over diverse datasets. The participants can visualize their system performance on an online leaderboard evaluation platform.

In the OpenMFC 2020-2021 evaluation, 59 participants registered to participate in the program, and 224 public researchers worldwide received MFC datasets. Since 2016, NIST has released MFC dataset to more than 500 individuals and 200 organizations from 26 countries and regions worldwide.

In the report, first, the introduction, objectives, challenges, contributions, and achievements of the evaluation program are covered and discussed in the Section 1. Second, the evaluation website, tasks, datasets, and the leaderboard interface are described in the Section 2. The participants' system performance results are also presented in this section. Third, the community engagements, findings, and public participants' difficulties are summarized in the Section 3. Then, two new studies for the next year evaluation, OpenMFC 2021-2022, are introduced in the same section. After that, the solutions to help public participants and the OpenMFC 2021-2022 work plan are proposed in the Section 4. Finally, the potential impacts are discussed in the Section 5.

Key words

Media Forensics, DARPA MediFor (Media Forensic) program, Media Forensic Challenge (MFC) Evaluation, Image Manipulation Detection and Localization (IMDL), Video Manipulation Detection (VMD), Image GAN Manipulation Detection (IGMD), Video GAN Manipulation Detection (VGMD), Deepfakes, and Steganography.

Acknowledgments

The authors gratefully acknowledge Prof. Jennifer Newman, Prof. Yong Guan, Li Lin from Iowa State University, Prof. Roy A. Maxion from Carnegie Mellon University, and Barbara Guttman from NIST for their work, discussions, and support on building OpenMFC Steganography detection datasets.

Grateful thanks go to Prof. Siwei Lyu in University of Buffalo and his team member, Yuezun Li and Yan Ju for their collaborations, valuable discussions, information sharing, code sharing, and support on building Deepfake detection dataset.

Disclaimer

Certain commercial equipment, instruments, software, or materials are identified in this article in order to specify the experimental procedure adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the equipment, instruments, software, or materials are necessarily the best available for the purpose.

The views, opinions and/or findings expressed are those of the author and should not be interpreted as representing the official views or policies of the Department of Defense or the U.S. Government.

Table of Contents

List of Tables

List of Figures

Glossary

Nimble Challenge (NC) – The name of NIST media forensic challenge kickoff dataset in 2016 and the challenge evaluation in 2017.

Media Forensic Challenge (MFC) – In 2018 the Nimble Challenge was renamed to the Media Forensic Challenge and became the evaluation series that supported the DARPA MediFor Program's performer evaluations from 2018-2020.

Open Media Forensic Challenge (OpenMFC) – The successor of the MFC media forensic evaluation series, supported by NIST and open to public participation.

1. Introduction

With the fast emerging technologies in artificial intelligence (AI) and machine learning (ML), media generation and falsification techniques such as Generative Adversarial Networks (GAN) (e.g., Deepfakes) [1][2][3], new features in Adobe Photoshop, and anti-forensic technologies bring new challenges to current media forensic technologies. The threat to employ them to maliciously manipulate images and videos is pressing, which seriously increases the doubt in the trustworthiness of the media used in all kinds of applications, such as social media (Facebook, Instagram, Twitter, YouTube etc.), research funding application (e.g., publication integrity verification), law enforcement, military applications, and security applications.

Researchers are dedicated to developing forensic technologies to identify media manipulations for stakeholders such as media verification specialists, fact-checkers, journalists, media platform providers, policymakers, and human rights defenders etc. As a government agency, NIST also supports US congress passed a bill, Identifying Outputs of Generative Adversarial Networks Act, or the S.2904-IOGAN Act[1], into law on Dec. 2020. The bill directs "the National Science Foundation (NSF) and the National Institute of Standards and Technology (NIST) to support research on generative adversarial networks." "Specifically, the NSF must support research on manipulated or synthesized content and information authenticity and the NIST must support research for the development of measurements and standards necessary to accelerate the development of the technological tools to examine the function and outputs of generative adversarial networks or other technologies that synthesize or manipulate content."

1.1. The evolution of media forensic research

The earliest media forensics related study sprouted around 2003 – 2004 [26]. The media forensics research field was established around 2008 – 2013 by several survey papers [27][28][29][30]. The first media forensic evaluation program, IFS-TC Image Forensics Challenge, was organized by Prof. Anderson Rocha, UNICAMP, Brazil, Prof. Alessandro Piva, University of Florence, Italy, and Prof. Jiwu Huang from Sun Yat-sen University, China. In 2016, Prof. David Doermann from University at Buffalo established the DARPA MediFor program[2]. After that, more and more industry, academia, and government, researchers started to work on this field, many papers were published, and forensic detection tools or product prototypes were transferred to stakeholders. In 2020, Dr. Matt Turek built the SemaFor[3] program to extend the forensic research to include the semantic applications.

1.2. OpenMFC overview

To support the rapid growth of media forensics technologies in the public domain, NIST team built the Open Media Forensics Challenge (OpenMFC) evaluation program to measure how well forensic systems can automatically detect and locate manipulations in imagery (i.e., images and videos). OpenMFC is the subsequent program of Media Forensics Challenge (MFC), which was built for DARPA MediFor 2017-2020 [4]. Since 2015, the NIST team systematically established MFC evaluation infrastructure. We designed evaluation tasks, datasets, metrics and the scoring software, and held 4 yearly evaluations to evaluate the

[1] https://www.congress.gov/bill/116th-congress/senate-bill/2904?ref=hackernoon.com
[2] https://www.darpa.mil/program/media-forensics
[3] https://www.darpa.mil/program/semantic-forensics

DARPA performer teams' systems. We reported the state-of-the-art of media forensic technologies [6]-[21] to fulfill the DARPA mission.

The MediFor program was heavily focused on the technology transition of forensic tools developed by 11 DARPA performer teams. The previous MFC evaluation program deployed a container system evaluation infrastructure to meet the DARPA program specifications. It asked performers to submit their container systems to the DARPA MediFor computation platform, which made it difficult to enroll external teams and greatly restricted researchers outside the program from participating in the evaluation.

OpenMFC is an online leaderboard open evaluation program for public participants. NIST team releases the evaluation data to the participants. Instead of submitting a functional system, the participants run the system themselves, and submit the system output results the NIST online evaluation platform. Then evaluation website runs the evaluation on the scoring server and provides the evaluation report in the online evaluation leaderboard, which makes the OpenMFC participation much easier and more convenient.

1.3. Challenges

Intrinsically different from other detection technologies, the field of media forensics faces very challenging problems: to find and detect an unknown manipulation. That is, a traditional detection system trained by well-known manipulations (such as clone, splice, or removal) could work well with known manipulations. While when a new manipulation approach is emerging (e.g., the latest Deepfakes algorithm), existing forensic detection tools may work poorly as the random guess and their performance drops greatly.

In addition, anti-forensic technologies [22] are also improving everyday by exploiting known weaknesses and capabilities of existing forensic detection systems. If media forensic systems are exposed enough, anti-forensic technologies will learn how to hide manipulation traces and fool existing forensic systems [23].

A system designed for face or fingerprint detection, whose detection targets are fixed, would show that the system performance could improve consistently and steadily each year. However, with the emerging and dynamically updated manipulation approaches, the performance of a media forensic system could dramatically decrease, and continuous development and evaluation are essential. The deployment of measurement techniques on media forensics additionally faces the challenging problems of constantly and swiftly adapting datasets [6] [7] [8], evaluation tasks [9], and evaluation metrics [15][16], which are needed to stay up to date with rapid advancements in AI technologies. Please refer to our previous publications [6] - [21] for the challenges and solutions on designing and developing an evaluation program.

1.4. OpenMFC objectives and features

Media forensic technologies are still under development. While focusing on the new emerging technologies, OpenMFC continued the MFC evaluation to report the state-of-the-art of media forensics and provide the cross-year performance comparisons. OpenMFC aims to engage the larger research community, to serve participants worldwide, to stimulate the public researchers to meet the tremendous challenges in media forensic applications, to foster progress in developing novel media forensic technologies, and expanding the NIST influence worldwide.

OpenMFC 2020-2021 has three major features:

(1) AI emerging technologies evaluation (e.g., image/video GAN detection tasks). OpenMFC supports the advancement and deployment of the measurement of the existing and emerging AI technologies in the media forensic field. OpenMFC also serves as a testbed to identify the potential issues of ML systems, and to design and deploy the evaluation program to help the participants to recognize the potential issues of their systems and improve the system performance through evaluation programs.

(2) Online leaderboard evaluation: the participants obtain the results immediately.

(3) No container submission requirements: OpenMFC allows researchers to only submit the system outputs, rather than software systems, thus making it possible to engage the larger research community. The participants focus on new idea and algorithm design instead of industry-level code packing, debug, and implementations. On the other hand, without submitting software system, the public researchers don't have any Intellectual property (IP) concerns.

OpenMFC 2021-2022 is deploying the following features:

(1) Add new tasks to adapt to the rapidly emerging manipulation technologies (e.g., Steganography Detection task and Deepfakes Detection task).
(2) Update the online leaderboard infrastructure to dynamically adapt to the new tasks easily.
(3) Deploy system performance analyzing tools to help participants to improve their algorithm and technologies.

1.5. OpenMFC 2020-2021 contributions and achievements

The following contributions and achievements are made in the OpenMFC 2020-2021:

- Built the OpenMFC website: https://mfc.nist.gov with public facing overview, tasks, datasets, schedules, resources etc., and private internal account management (users/sites/teams), evaluation management and submission/result management etc.
- Developed an evaluation infrastructure for a leaderboard evaluation platform, which brings more adaptability, flexibility, and visibility to the open evaluation; deployed six leaderboards for four evaluation tasks.
- Advertised the OpenMFC 2020-2021 evaluation to public researchers to inspire more people to work on this field.
- Released the MFC dataset to 210 public researchers last year. Since 2016, NIST has released MFC dataset to more than 500 individuals and 200 organizations from 26 countries and regions worldwide.
- Published the OpenMFC 2020-2021 evaluation plan [15] and MFC dataset user guide NISTIR report [6].
- Publishing the evaluation report on the current media forensic state-of-the-art in public domain and OpenMFC 2020-2021 result (this report).
- Organized and deployed the OpenMFC 2020-2021 evaluation with 59 participants.
- Accomplished OpenMFC 2020-2021 to minimize the barriers for public researchers' participation in media forensics.
- Engaged with Media Forensic community, understood the participants' difficulties, and proposed the solutions in the next year OpenMFC 2021-2022 evaluation to help public researchers on the system developments.

- Designed Steganography Detection (StegD) task for the OpenMFC 2021-2022; Outreached to external experts and collaborated with the external team on the new dataset: StegD evaluation dataset. IRB annual report about MFC, StegD, and SemaFor datasets was approved by NIST Research protection Office (RPO).
- Designed Video Deepfakes Detection (VDD) task for the OpenMFC 2021-2022; Collaborating with the external teams on the dataset.
- Preparing OpenMFC 2020-2021 Workshop.
- Proposed OpenMFC 2021-2022 evaluation program and publishing OpenMFC 2021-2022 evaluation plan [16].

2. OpenMFC 2020-2021

2.1. OpenMFC evaluation website

Through the OpenMFC evaluation website, https://mfc.nist.gov, as shown in Figure 1, the public researcher could obtain the evaluation program information, which includes overview, tasks, data, schedule, submission rules, resources, and contact information.

The website also provides the program participants an online leaderboard evaluation platform to register the evaluation, signup the data agreement form, download the evaluation datasets, upload their system output files, and visualize the evaluation results and the scoring table in the leaderboard section.

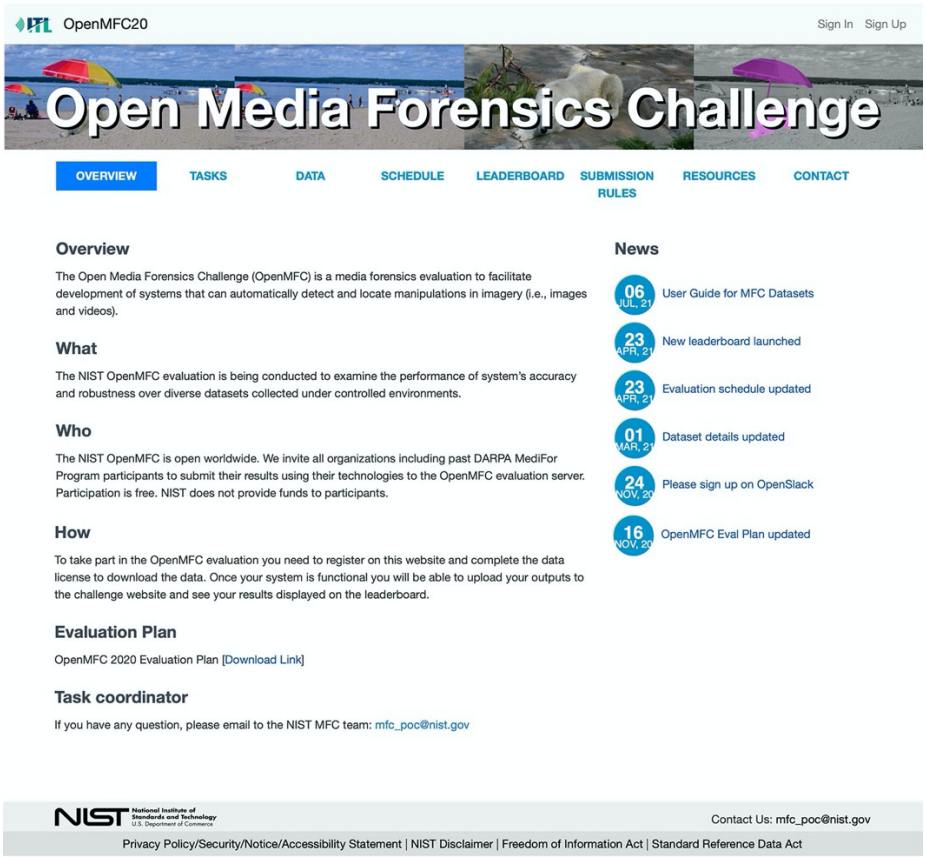


Figure 1. OpenMFC evaluation website.

2.2. OpenMFC 2020-2021 tasks and conditions

OpenMFC 2020-2021 contains the following 4 tasks [15]:

- Image Manipulation Detection and Localization (IMDL) – to detect whether a probe image was manipulated and, if so, to spatially localize the manipulations. Manipulations are deliberate, purposeful manipulations such as splicing and cloning etc. Localization task is encouraged but not required for OpenMFC. For detection evaluation, an IMDL system provides a confidence score for each trial with higher numbers indicating the image was more likely to be manipulated. Receiver Operating Characteristic (ROC) curve and Area Under the Curve (AUC) (see the detection system evaluation metrics in [15] for details) are two metrics used for the detection system. For the localization evaluation, the system provides a mask and its bit plane that indicate the manipulated region(s) with a manipulation type.
- Video Manipulation Detection (VMD) – to detect whether a probe video was manipulated. A VMD system provides a confidence score for each trial with higher numbers indicating the video was more likely to be manipulated. OpenMFC doesn't have the video localization task.
- Image GAN Manipulation Detection and Localization (IGMDL) – to detect whether a probe image was manipulated using generative adversarial network (GAN) based techniques and, if so, to spatially localize the manipulations. Localization task is encouraged but not required for OpenMFC.
- Video GAN Manipulation Detection (VGMD) – to detect whether a probe video was manipulated using generative adversarial network (GAN) based techniques. OpenMFC doesn't have the video GAN localization task.

IMDL is evaluated under two conditions [15]:

- Image Only (IO) – the system is only allowed to use the pixel-based content for images as input. No image header or other information should be used.
- Image and Metadata (IM) – the system is allowed to use metadata, including image header or other information, in addition to the pixel-based content for the image, as input.

VMD is evaluated under two conditions:

- Video Only (VO) – the system is only allowed to use the pixel-based content for videos and audio if it exists as input. No video header or other information should be used.
- Video and Metadata (VM) – the system is allowed to use metadata, including video header or other information, in addition to the pixel-based content for the video and audio if it exists, as input.

IGMD is evaluated under Image Only condition.

VGMD is evaluated under Video Only condition.

2.3. OpenMFC 2020-2021 datasets

Table 1 summarizes the number of probes of the OpenMFC datasets. OpenMFC2020-2021 IMDL and VMD tasks use of the MFC19 testing datasets. IGMDL and VGMD tasks use of the MFC18 GAN challenge datasets.

Table 1: Evaluation Datasets

Dataset	Task	number of probes
OpenMFC20_Image_IMDL	IMDL	16 029
OpenMFC20_Video_VMD	VMD	1 530
OpenMFC20_Image_IGMDL	IGMDL	1 340
OpenMFC20_Video_VGMD	VGMD	118

2.4. OpenMFC 2020-2021 leaderboard

To engage and shorten the development cycle of the research community, the OpenMFC2020-2021 evaluation introduced a set of six leaderboards given the evaluation task and their evaluation conditions [15]: IMDL-IO, IMDL-IM, VMD-IO, VMD-IM, IGMD, VGMD.

Leaderboards update with every single submission made, allowing participants to instantly compare results across their own technologies as well as other participants contributions. Currently each leaderboard consists of a table as well as a combined ROC graph. The leaderboard generation process is conducted as follows:

Each system submission undergoes a scoring process including output download, validation, and scoring. Once the process completes successfully, a related leaderboard aggregation job is triggered. During the aggregation, main output metrics and ROC data across each submission task are collected (AUC and CDR@0.05FAR). The resulting metrics table is then sorted by rank based on AUC and presented to the public in the form of a sortable leaderboard on the evaluation frontend (https://mfc.nist.gov/#pills-leaderboard). Additionally, ROC curves are combined into a single overlay graph and presented below each leaderboard for a visual comparison amongst systems. The backend system has been implemented using a combination of automated processing pipelines developed by NIST team, orchestrating scoring software tasks (MediScore[4]) as well as a database for persistence of metrics, access control, and metadata access (through a PostgreSQL database).

2.5. DARPA MFC system performance on the same OpenMFC evaluation dataset

The OpenMFC online leaderboard evaluation shares the same datasets as DARPA MFC19 container evaluation. Figure 2 shows the system performance of the DARPA MFC19 on the same IMDL-IO task.

The AUC of the best performing system was 0.866. This best result was achieved by DARPA selected performer teams funded by the DARPA MediFor project. This project encompassed four years of groundbreaking work by top-level media forensic researchers from both industry and academia.

[4] https://github.com/usnistgov/MediScore

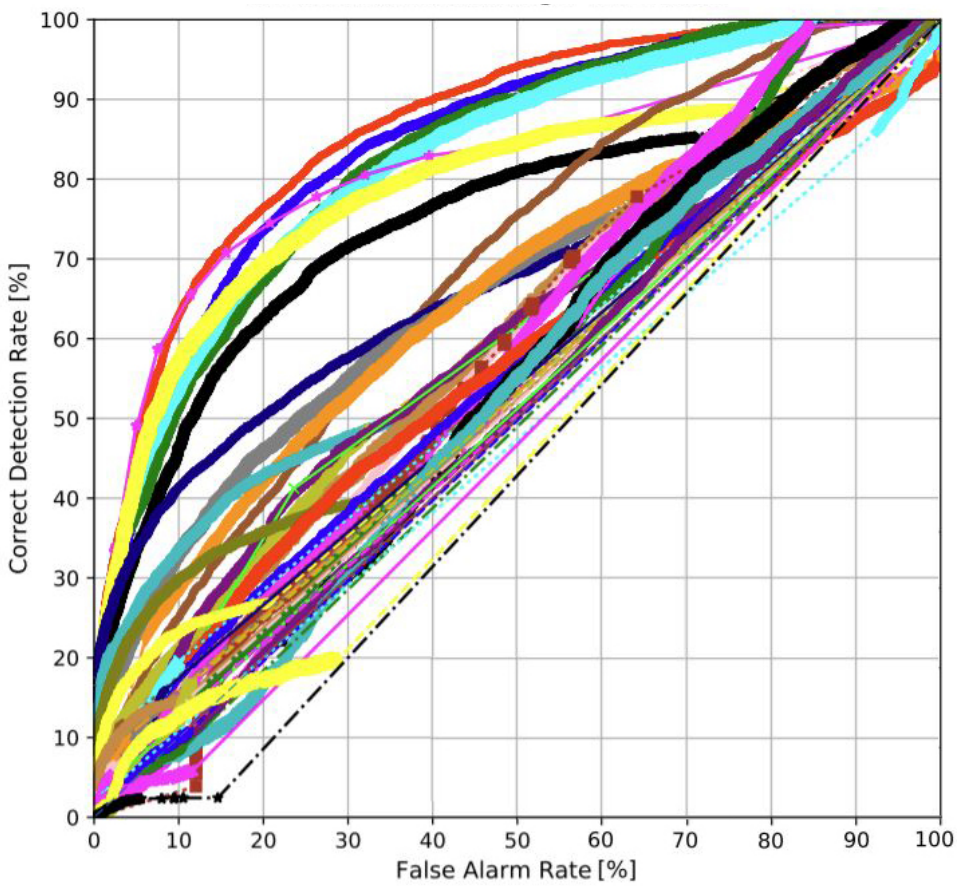


Figure 2. DARPA MFC 2019 system performance on the Image Manipulation Detection and Localization - Image Only (IMDL-IO) task.

2.6. OpenMFC 2020-2021 results and analysis

2.6.1. The performance comparison using different training data

It is well known that the performance of the machine learning system not only depends on the learning algorithm, but also is heavily affected by the size and quality of the training data and the reference ground-truth annotation in many applications.

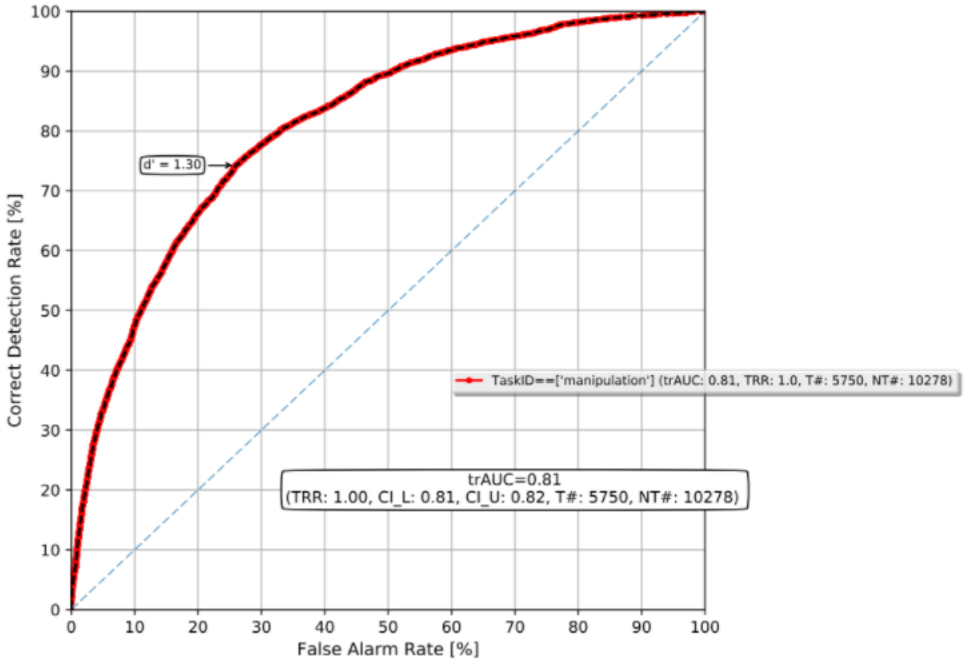


Figure 3. Team1 system performance without using the MFC19 dataset as training.

Figure 3 shows the Team1 image manipulation detection system's ROC curve on the testing data in the MFC19 evaluation in the DARPA MediFor program. The AUC is 0.81. The reference ground-truth of MFC19 dataset was not released to the DAPRA performer team at that time. Thus, the detection system was not able to train on the MFC19 dataset.

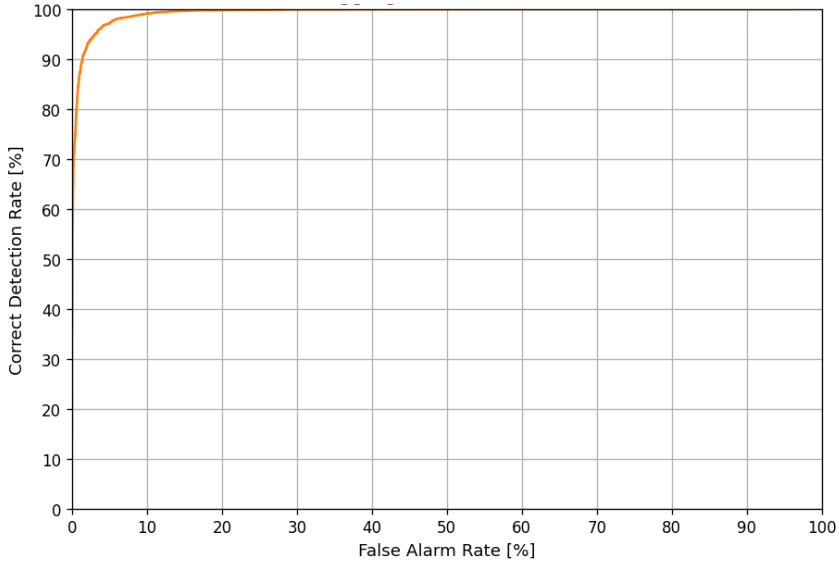


Figure 4. Team1 system performance using the MFC19 dataset as training.

After the DARPA MFC19 evaluation, NIST released the reference ground-truth of the MFC19 dataset. Team1 trained the detection system with the MFC19 dataset. The red ROC curve in Figure 4 shows the same team's system performance on the same testing data in the OpenMFC 2020-2021 evaluation. The AUC is 0.99. Compared with the NC16, NC17, and

MFC18 datasets, the MFC19 dataset is larger and describes manipulation operations with high quality of annotation (see [6] for the MFC datasets summary). It shows that with the larger data size and more sample data coverage (e.g., the larger number of the manipulation operations), the system performance could improve greatly. If the data distribution of the training data aligns well with the data distribution of the testing data, the detection algorithm could provide a very good detection result. At the same time, it also shows that machine learning systems could perform very well on the training data. An evaluation program in the neutral position without bias to any participant team is essential for providing a convincing report instead of system developers' self-evaluation results. Continuous cross-year performance comparisons are more valuable to track the technology improvement than a one-time evaluation report.

2.6.2. OpenMFC2020-2021 testing system performance

For the IMDL-IO manipulation detection task, without using the MFC19 dataset as training, the best AUC score in OpenMFC 2020-2021 is 0.81 (the team is the previous DARPA performer team) with the ROC curve shown in Figure 3. The second-best system's AUC score from the public participant is 0.62 as shown in Figure 5.

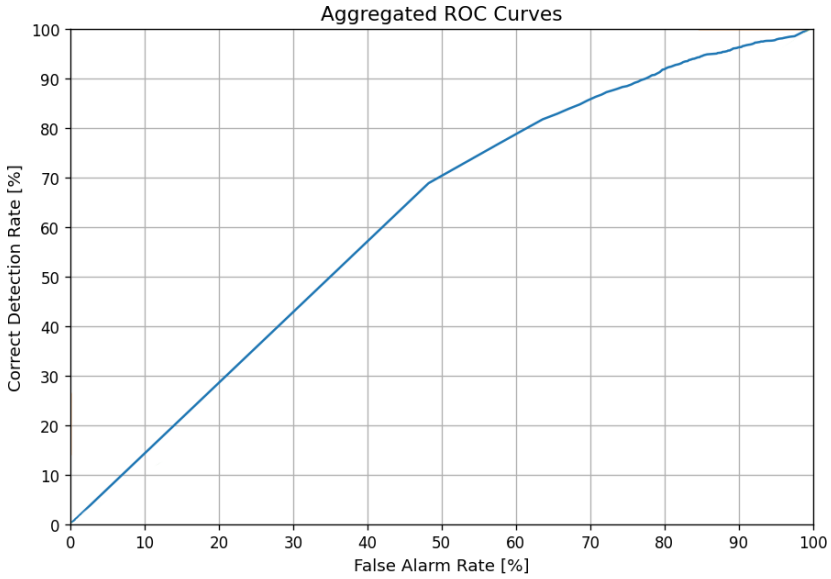


Figure 5. Team2 system performance without using MFC19 dataset as training.

For the IMDL-IO manipulation localization task, the best public team's MCC score [15] in OpenMFC 2020-2021 is 0.055 compared with 0.224, which is the best MCC score on the same dataset in MFC19 evaluation in the DARPA MediFor project.

For the IGMD task, the best AUC score in OpenMFC 2020-2021 from the public participant is 0.69, compared with the best AUC score, 0.79, on the same dataset in the previous MFC18 evaluation in the DARPA MediFor project.

3. Community Engagements: Findings, Challenges, and Studies

Based on the information collected from OpenMFC 2020-2021 participant webinars, media forensic community engagement, recent media forensic workshops and conferences, the past DARPA MediFor project, and the current DARPA SemaFor project, the summary of current

media forensics current research and evaluation status is given in this section. The public participants' challenges and difficulties in participating the evaluation are collected and presented. In addition, two studies collaborated with external teams for the future new evaluation tasks are presented in this section.

3.1. OpenMFC 2020-2021 findings

Media forensics is an extremely challenging research domain. It includes many sub-domain applications and there are different types of tasks in each sub-domain. No single technology can resolve all forensics problems alone. It is still a long run to go before the automatic detection system could be widely used and accepted by consumers in real-world applications. Here are the key features of the current state-of-the-art of media forensics:

- There are large and demanding markets in different applications (social media, forensics, government, military, education, and law enforcement etc.).
- The hot topics in social media bring lot of attentions (e.g., Deepfakes [31]).
- Public researchers are devoting time and resources to this evaluation: there are more than 500+ researchers from 200+ organizations in 26+ countries that have downloaded and used NIST MFC datasets.
- The evaluation of media forensics must be dynamically upgraded with the newest emerging manipulation tools and software.
- Media forensic technologies are still under development and not fully mature.

Although lots of academic research papers achieved very high detection rate, the performance may drop when the testing dataset is changed (that is, its sample distribution is not consistent with the training data). The highest AUC scores in both OpenMFC 2020-2021 and MFC20 on the Image Manipulation Detection (IMD) task are about 0.8. But it is not surprising that the system performance is dramatically reduced in real-world applications with the data collected 'in the wild', especially when the test data are generated by the new emerging manipulation tools [23]. The performance of other tasks like manipulation localization also needs further improvements. The current forensic technologies have a long way to go to make a fully automatic system to detect image/video manipulations and to provide a meaningful integrity report.

Based on the DARPA media forensic evaluation, if the training samples and testing samples are drawn from the same distribution (within evaluation year comparison), the performance in an open evaluation is slightly higher than the corresponding sequestered evaluation. If the testing datasets are upgraded (cross-year evaluation comparison), the system performance dropped, and the detection system needs to be upgraded with the new training data.

3.2. Public participants' challenges and difficulties

Based on the OpenMFC webinar feedback and other communications with the media forensic community, here are the major challenges and difficulties for public researchers:

- Increases in technical diversity as well as rapid changes in the nature of tools, software, applications and operations used in media manipulation, are occurring at an overwhelming pace.

- There is a limited amount of time and effort that public researchers can devote to work on an evaluation without additional funding and support.
- The content and complexity of the training data collection is a major consideration.
- The technical expertise and diversity of skills that make up public research teams.

The solutions addressing above challenges and helping public participants are proposed in Section 4.

3.3. Studies for new tasks in OpenMFC 2021-2022

Unlike evaluating other traditional technologies, the evaluation of media forensic detection technologies requires continuously upgrading the evaluation tasks and datasets to adapt to the novel emerging and image/video editing/manipulation software and tools.

In the OpenMFC, we updated our evaluation infrastructure and platform to quickly add the new challenges/tasks, evaluated new detection technologies, and provided the performance assessments. We designed and deployed two new challenges/tasks for OpenMFC 2021-2022, steganography detection and Deepfakes detection, to fulfill the current media forensic market needs and encourage public researchers to work on those two specific fields.

3.3.1. Steganography study

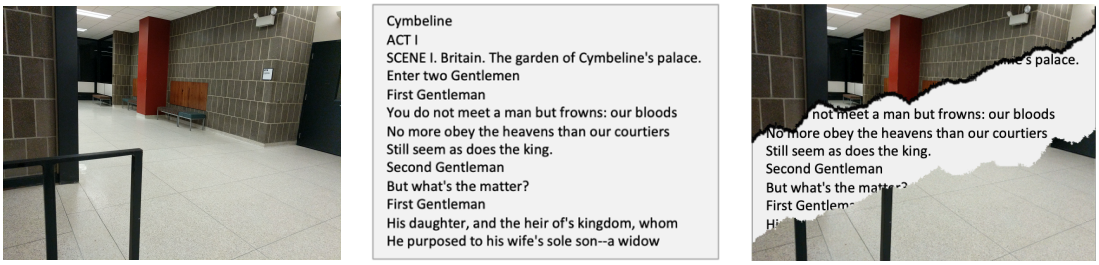
One specific research area of media forensics is steganography image detection and analysis. "Steganography is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection; the secret data is then extracted at its destination. The use of steganography can be combined with encryption as an extra step for hiding or protecting data." [25] Steganography hides data (payload) in an innocent file (cover), producing a steganographic image.

Collaborating with Prof. Jennifer Newman, Prof. Yong Guan, Li Lin from Iowa State University, Prof. Roy A. Maxion from Carnegie Mellon University, and Barbara Guttman from NIST, we designed Steganography Detection (StegD) task for OpenMFC2021-2022. The task is to detect if a probe is a steganographic image, which contains the hidden message either in pixel values or in optimally selected coefficients [5].

In addition, we constructed the StegD datasets using the data from StegoAppDB [24]. Figure 6 shows one testing example in the StegD dataset. The test image is a steganographic image shown in Figure 6 (c), which is generated with Passlok embedding method [25] given the cover image shown in Figure 6 (a), and a paragraph extracted from Cymbeline by Shakespeare as the payload message. If we compare Figure 6 (a) and Figure 6 (c) visually using human eye, there is no visual difference, but Figure 6 (c) has hidden information defined by the payload. The StegD dataset's ReadMe file with the definitions of the evaluation index file and reference file for the participants are defined in Appendix A. This information will be released to the participants in the OpenMFC evaluation. The ReadMe file for the evaluators is defined in Appendix B. This information will be released after the OpenMFC evaluation is complete. The evaluator version is an extended version of the participant version with the rich metadata information related with the steganography application, which could expose the information about the manipulation tool and will not be released early. After the evaluation

[5] https://en.wikipedia.org/wiki/Steganography

report is finalized, we may release the evaluator's reference file, and the participants could use it for performance analysis to improve the system. The OpenMFC program sequestered the information about steganography applications and their parameters to avoid that the participants' systems only training on the specific applications used in the testing datasets.



(a) Cover image (b) Payload (c) Steganographic image

Figure 6. An example in the OpenMFC Steganography Detection (StegD) dataset.

3.3.2. Deepfakes study

The idea of Deepfakes was proposed in the late 2017 and has become one of the hottest topics in the media forensic field [1][2][3]. Deepfakes are photorealistic images and videos built using GAN (generative adversarial network) techniques originated within the Artificial Intelligence (AI) domain.

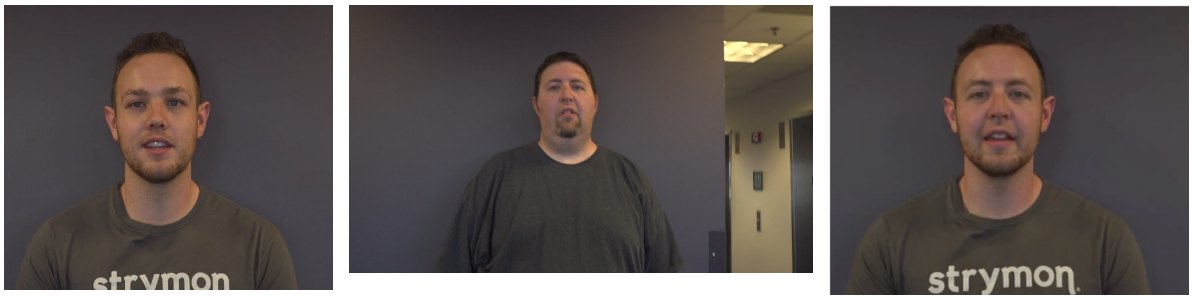
We designed a Deepfake detection task for the OpenMFC 2021-2022. The Video Deepfake Detection (VDD) task is to create a tool that can detect if a probe video has been Deepfaked[6]. We are working on Deepfake tool testing, automated manipulation data creation, and evaluation dataset generation.

Figure 7 - Figure 9 show Deepfake testing examples. Figure 7 shows a Deepfake face swap example. The original video, shown in Figure 7 (a), and the donor video, shown in Figure 7 (b), were the videos in the MFC dataset. The two videos were collected by University of Colorado Denver team in DARPA MediFor project. The Deepfaked video shown in Figure 7 (c) was also generated with DeepFaceLab tool given the original and the donor videos.

(a) Original video (b) Donor video (c) Deepfaked video

Figure 7. A Deepfaked video example using the MFC videos and the DeepFaceLab tool.

[6] https://en.wikipedia.org/wiki/Deepfake

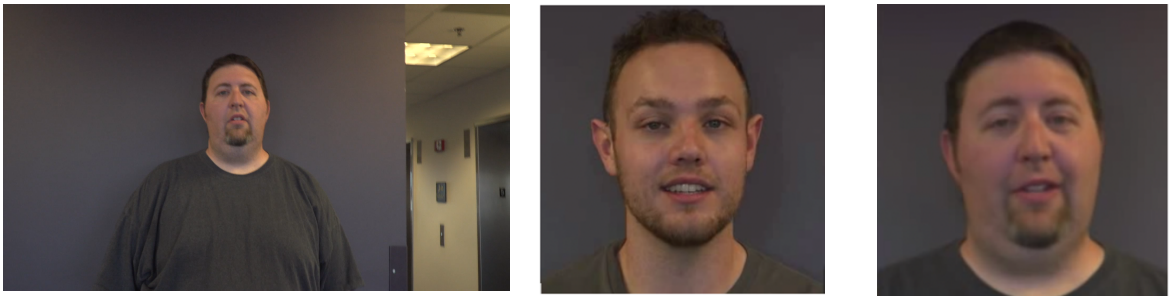


(a) Original video (b) Donor video (c) Face swap video

Figure 8. A face swap video example using the MFC videos and the Celeb-DF tool.

Figure 8 shows another face swap testing example. The original video is shown in Figure 8 (a), and the donor video is shown in Figure 8 (b). We switched the original video and donor video as shown in Figure 7 (a) and (b) in this test case. Figure 8 (c) shows the Deepfaked video using the face swap function of the Celeb-DF tool provided by Prof. Siwei Lyu's team from the University of Buffalo.

"Face Reenactment is an emerging conditional face synthesis task that aims at fulfilling two goals simultaneously: 1) transfer a source face shape to a target face; while 2) preserve the appearance and the identity of the target face."[7] Figure 9 shows a face reenact testing example. Figure 9 (a) is the original image. Figure 9 (b) shows the cropped donor facial expression image. Using the face reenact function of the Celeb-DF tool provided by Prof. Siwei Lyu's team, Figure 9 (c) shows the cropped face reenact image, which mimic the facial expression of the donor video.



(a) Original video (b) Facial expression donor video (c) Face reenact video of the similar facial expression

Figure 9. A face reenact video example using the MFC videos and the Celeb-DF tool.

The following tools are also tested in this study: DeepFakes FaceSwap[8], First order motion model[32], FaceApp[33] and Reface[34], etc. We are continuously working on Deepfakes tool testing and Deepfakes dataset generation.

4. OpenMFC 2021-2022 Work Plan and Expected Delivery

Media Forensics is a relatively new research field with many challenges. The public researchers have limitations on the research capability, skills, worktime, workload, and

[7] https://paperswithcode.com/task/face-reenactment
[8] https://faceswap.dev

funding. These researchers need to expend significant time and efforts to make progress in this fast-changing field. NIST has a government evaluation team that acts as a neutral facilitator. As such, one of the major tasks for the NIST OpenMFC next year is to encourage researchers to work on media forensics, make evaluations more accessible to all, including low resource participants, resolve the participants major difficulties and assist them to ensure they get maximum value from participation.

To reduce the burden on public researchers and provide them with a flexible and feasible evaluation program, the following solutions are proposed in the OpenMFC 2021-2022 work plan:

- Design evaluation tasks varying in difficulty level and technical scope: adapt aforementioned needs from public researchers with different skill sets, we introduce Image Splice Detection (ISD) task to greatly reduces researchers' workload. We design Steganography Detection task [6, 7] and Deepfakes Detection task [6, 8] focusing on the new advanced emerging topics.
- Upgrade online leaderboard scoring infrastructure to easily adapt to new tasks: deploy an easily accessible, flexible, and scalable evaluation infrastructure consisting of frontend and backend systems, to meet the requirements of testing and evaluation protocols of rapidly growing AI technologies in media forensics.
- Provide more data resources: we will propose a strategy to divide the existing data resources into training and testing datasets. The training data with reference will be used for participants to train their AI systems. This aims to attract more participants who don't have the capacity to collect training data in order to join the OpenMFC evaluation.
- Deploy an interactive data analysis interface: add a web-application for in-depth analysis and comparison of system performance based on R-Shiny[9]. Participants and evaluators can analyze system performance interactively using the online tool. The data analysis feedback will provide the participants a guidance or insight on how to improve their systems.

  To further improve reporting detail of scoring output across performers, we are developing an interactive web-application. The application can be embedded into the existing evaluation replacing the current leaderboard view and will be publicly available to performers. We are leveraging the R language[10] eco-system for statistical computing and graphics combined with the R-Shiny framework providing an interactive web-interface. The application uses our existing scoring database (PostgreSQL[11]) to retrieve data for analysis. Besides providing the already existing leaderboard capabilities, this new platform will allow participants to introspect their data further interactively across metrics and technologies. Furthermore, by using a high-level programming language it will allow us, the evaluators, to promptly develop new visualizations and metric comparisons.

[9] https://shiny.rstudio.com
[10] https://en.wikipedia.org/wiki/R_(programming_language)
[11] https://www.postgresql.org

- Provide the OpenMFC 2021-2022 evaluation report with cross-year performance comparisons.
- Organize OpenMFC 2021-2022 workshop and increasingly develop a media forensics research community.

5. Conclusions and Potential Impacts

Media forensics is an extremely challenging topic due to its technical complexity, data variability, and application diversity in combination with the dynamic nature of the problem. There is still a long way to go to develop products with a reasonable detection rate for robust real-world applications.

NIST has designed an open evaluation, OpenMFC 2020-2021, updated the evaluation design infrastructure, developed a leaderboard evaluation platform[12], and published the evaluation plan [15] and dataset documentation [6] and reported the evaluation results (contained in this document).

As new technologies emerging, we designed two special tasks for OpenMFC 2021-2022: Deepfakes and steganography. Based on the media forensics state-of-the-art and the feedback collected from the community engagements, to better serve the public participants at different levels with different backgrounds, we will upgrade OpenMFC 2021-2022 with new evaluation tasks, datasets, and leaderboard platform to adapt to the public researchers' needs.

The impacts are three-fold: first, we proposed an easily accessible, flexible, and scalable evaluation infrastructure to meet the special requirements of the testing and evaluation of the rapidly growing AI technologies in media forensics. We can quickly design and update the evaluation tasks, datasets, and metrics to measure performance of new emerging technologies. We can quickly design and update the evaluation tasks, datasets, and metrics, and adapt our evaluation infrastructure to measure performance of new emerging technologies. The work greatly enhances our evaluation capabilities on the AI and ML test and evaluation.

Second, our work lays the foundation for us to understand the developments of media forensic technology worldwide and accelerating AI innovation in this field. We have been providing evaluation series since 2017 till now to provide cross-year comparison results and keep NIST's reputation as a leader in media forensic evaluation.

Third, our hand-on experiences as a government agency evaluation team allows us to provide valuable expertise on the development of approach, standards, guides, and best practices for the measurement and evaluation of AI technologies in media forensics to both internal and external research stakeholders.

[12] https://mfc.nist.gov

References

[1] Karras, T., Aila, T., Laine, S., & Lehtinen, J. (2017). Progressive growing of gans for improved quality, stability, and variation. arXiv preprint arXiv:1710.10196, Available at https://arxiv.org/abs/1710.10196.

[2] Hulzebosch, N., Ibrahimi, S., & Worring, M. (2020). Detecting cnn-generated facial images in real-world scenarios. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (pp. 642-643).

[3] Karras, T., Aittala, M., Laine, S., Härkönen, E., Hellsten, J., Lehtinen, J., & Aila, T. (2021). Alias-Free Generative Adversarial Networks. arXiv preprint arXiv:2106.12423. https://arxiv.org/abs/2106.12423

[4] DARPA Media Forensics (MediFor) Program, https://www.darpa.mil/program/media-forensics.

[5] Leibowicz, C., McGregor, S., & Ovadya, A. (2021). The Deepfake Detection Dilemma: A Multistakeholder Exploration of Adversarial Dynamics in Synthetic Media. arXiv preprint arXiv:2102.06109.

[6] Guan, H., A., Delgado, Lee, Y., Yates, A., Zhou, D., Kheyrkhah, T., and Fiscus, J. (2021), User Guide for NIST Media Forensic Challenge (MFC) Datasets, NIST Interagency/Internal Report (NISTIR) Number 8377, Available at https://doi.org/10.6028/NIST.IR.8377.

[7] Robertson, E., Guan, H., Kozak, M., Lee, Y., Yates, A., Delgado, A., Zhou, D., Kheyrkhah, T., Smith, J. and Fiscus, J. (2019), Manipulation Data Collection and Annotation Tool for Media Forensics, IEEE computer vision and pattern recognition conference 2019, Long Beach, CA. Available at https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=927817.

[8] Guan, H., Kozak, M., Robertson, E., Lee, Y., Yates, A., Delgado, A., Zhou, D., Kheyrkhah, T., Smith, J. and Fiscus, J. (2019), MFC Datasets: Large-Scale Benchmark Datasets for Media Forensic Challenge Evaluation, IEEE Winter Conference on Applications of Computer Vision (WACV 2019), Waikola, HI. Available at https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=927035.

[9] Fiscus, J. and Guan, H. (2020), Media Forensics Challenge Evaluation Overview, ARO Sponsored Workshop on Assured Autonomy, Workshop Talk. Available at https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=930628.

[10] Fiscus, J., Guan, H., Lee, Y., Yates, A., Delgado, A., Zhou, D., Joy, D. and Pereira, A. (2017), MediFor Nimble Challenge Evaluation 2017, Evaluation Presentation. Available at https://www.nist.gov/system/files/documents/2017/07/31/nist2017mediaforensicsworkshop_20170726.pdf.

[11] Fiscus, J., Guan, H., Delgado, A., Kheyrkhah, T., Lee, Y., Zhou, D. and Yates, A. (2018), 2018 MediFor Challenge, Evaluation Presentation. Available at https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=928264.

[12] Fiscus, J., Guan, H., Lee, Y., Yates, A., Delgado, A., Zhou, D., Kheyrkhah, T., and Jin, X. (2020), NIST Media Forensic Challenge (MFC) Evaluation 2020 - 4th Year DARPA MediFor PI meeting, Evaluation Presentation. Available at

https://www.nist.gov/publications/nist-media-forensic-challenge-mfc-evaluation-2020-4th-year-darpa-medifor-pi-meeting.
[13] Yates, A., Guan, H., Lee, Y., Delgado, A., Zhou, D., and Fiscus, J. (2018), Media Forensics Challenge 2018 Evaluation Plan, Evaluation Plan, Available at https://www.nist.gov/system/files/documents/2018/10/30/mfc2018evaluationplan-clean3_werb.pdf.
[14] Yates, A., Guan, H., Lee, Y., Delgado, A., Zhou, D., Kheyrkhah, T. and Fiscus, J. (2019), Media Forensics Challenge 2019 Evaluation Plan, Evaluation Plan. Available at https://www.nist.gov/system/files/documents/2019/03/12/mfc2019evaluationplan.pdf.
[15] Yates, A., Guan, H., Lee, Y., Delgado, A., Kheyrkhah, T., Fontana, P. C., and Fiscus, J. (2020), Open Media Forensics Challenge (OpenMFC) 2020-2021 Evaluation Plan, Evaluation Plan. Available at https://www.nist.gov/publications/open-media-forensics-challenge-2020-evaluation-plan.
[16] Guan, H., Lee, Y., Diduch L., Zhang, J., Fontana, P. C., and Fiscus, J. (2021), Open Media Forensics Challenge (OpenMFC) 2021-2022 Evaluation Plan, Evaluation Plan. NIST IR, to be published.
[17] Fiscus, J., Guan, H., Lee, Y., Yates, A., Delgado, A., Zhou, D., Joy, D., and Pereira, A., Nimble Challenge 2017 Evaluation, Evaluation Website. Available at https://www.nist.gov/itl/iad/mig/nimble-challenge-2017-evaluation.
[18] Fiscus, J., Guan, H., Delgado, A., Kheyrkhah, T., Lee Y., Zhou, D. , and Yates, A., NIST Media Forensic team, Media Forensics Challenge 2018, Evaluation Website. Available at https://www.nist.gov/itl/iad/mig/media-forensics-challenge-2018.
[19] Fiscus, J., Guan, H., Lee, Y., Yates, A., Delgado, A., Zhou, D., and Kheyrkhah, T., Media Forensics Challenge 2019, Evaluation Website. Available at https://www.nist.gov/itl/iad/mig/media-forensics-challenge-2019-0.
[20] Guan, H., Lee, Y., Kheyrkhah, T., Fontana, P. C., and Fiscus, J. (2020), Open Media Forensics Challenge (OpenMFC) 2020 Evaluation, Evaluation Website. Available at https://mfc.nist.gov.
[21] Lee, Y., Yates, A., Guan, H., Delgado, A., Zhou, D., Kheyrkhah, T., and Fiscus, J., 2018 Multimedia Forensics Challenges (MFC18): Summary and Results, NIST Interagency/Internal Report (NISTIR) Number 8324, Available at https://doi.org/10.6028/NIST.IR.8324
[22] Barni, M., Stamm, M. C., & Tondi, B. (2018, September). Adversarial multimedia forensics: Overview and challenges ahead. In 2018 26th European Signal Processing Conference (EUSIPCO) (pp. 962-966). IEEE.
[23] Leibowicz, C., McGregor, S., & Ovadya, A. (2021). The Deepfake Detection Dilemma: A Multistakeholder Exploration of Adversarial Dynamics in Synthetic Media. arXiv preprint arXiv:2102.06109.
[24] Newman, J., Lin, L., Chen, W., Reinders, S., Wang, Y., Wu, M., & Guan, Y. (2019). Stegoappdb: a steganography apps forensics image database. Electronic Imaging, 2019(5), 536-1. Available: https://forensicstats.org/stegoappdb/.
[25] Semilof, Margie and Clark, Casey. (July 2021). What is steganography? Available: https://searchsecurity.techtarget.com/definition/steganography.

[26] Ng, T. T., Chang, S. F., & Sun, Q. (2004). A data set of authentic and spliced image blocks. Columbia University, ADVENT Technical Report, 203-2004.
[27] Sencar, H. T., & Memon, N. (2009). Overview of state-of-the-art in digital image forensics. Algorithms, Architectures and Information Systems Security, 325-347.
[28] Farid, H. (2009). Image forgery detection. IEEE Signal processing magazine, 26(2), 16-25.
[29] Piva, A. (2013). An overview on image forensics. International Scholarly Research Notices, 2013.
[30] Stamm, M. C., Wu, M., & Liu, K. R. (2013). Information forensics: An overview of the first decade. IEEE access, 1, 167-200.
[31] Al Jazeera English. (2021). What are deepfakes and are they dangerous? | Start Here, Available: https://www.youtube.com/watch?v=pkF3m5wVUYI, Jun 21, 2021.
[32] Siarohin A, Lathuilière S, Tulyakov S, Ricci E, Sebe N. First order motion model for image animation. Advances in Neural Information Processing Systems. 2019;32:7137-47.
[33] FaceApp Technology Ltd, FaceApp - AI Face Editor, https://www.faceapp.com.
[34] NEOCORTEXT, INC. Entertainment, Reface: Face swap videos and memes with your photo, https://hey.reface.ai.
[35] The State of Deepfakes, Deeptrace, Sensity, https://sensity.ai/reports/#.
[36] Yang, X., Li, Y., Qi, H., & Lyu, S. (2019, July). Exposing gan-synthesized faces using landmark locations. In Proceedings of the ACM Workshop on Information Hiding and Multimedia Security (pp. 113-118).
[37] Sanderson, Conrad and Lovell, Brian C. (2009). Multi-Region Probabilistic Histograms for Robust and Scalable Identity Inference. Lecture Notes in Computer Science (LNCS), Vol. 5558, pp. 199-208.

Appendix A: Steganography detection dataset ReadMe file for performer

```
                Open Media Forensics Challenge (OpenMFC) Steganography Detection Dataset

1. Introduction

OpenMFC Steganography Detection Dataset (OpenMFC-StegD) is a test and evaluation dataset built by the
NIST OpenMFC Program in collaboration with steganography team in Iowa State University. This release
is ONLY being released for program-internal discussions.

The dataset is structured similarly to the OpenMFC20 Image dataset.

2. Directory Structure

    ReadMe.txt - This file

    /probe     - Directory of images to be analyzed for various manipulations

    /world     - Directory of images that simulate a real-world collection of images or base images

    /indexes   - Directory of index files indicating which images should be analyzed

    /reference - Directory of subdirectories for each evaluation task, containing a file of trial
metadata, the reference masks, and the journal files.

    /documents - Directory of required documents

3. System Input Files

The index files are pipe-separated CSV formatted files.
The index file for the STEG Manipulation task has the columns:

Required columns:

    TaskID            Detection task ID
                      For STEG detection datasets, the value is fixed as 'stegd'.
                      (e.g., "stegd")

    ProbeFileID       Label of the probe image
                      (e.g., "00003e6a1efc7022da825396dc680343")

    ProbeFileName     Full filename and relative path of the probe image
                      (e.g., "/probe/00003e6a1efc7022da825396dc680343.jpg")

    ProbeWidth        Width of the probe image
                      (e.g., 4000)

    ProbeHeight       Height of the probe image
                      (e.g., 300)

    ProbeFileSize     File size of probe
                      (e.g., 2500)

Optional columns:

    None

4. Reference Files

Reference files will be released after whole evaluation cycle is done.

5. File Naming

The image files in this release will be named <randomString (or MD5 of the probe file)>.<extension>.

6. Distribution
```

THIS DATA IS PROVIDED "AS IS" for use in the OpenMFC Program. Regarding this data, NIST/ISU/CMU MAKES NO EXPRESS OR IMPLIED WARRANTY AS TO ANY MATTER WHATSOEVER, INCLUDING MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE.

7. Contacts

If you have any questions about this dataset, please contact the following people:

Iowa State University team (source data collection and evaluation dataset generation):
    Jennifer L Newman <jlnewman@iastate.edu>
    Yong Guan <guan@iastate.edu>
    Li Lin <llin@iastate.edu>
    Wenhao Chen <wenhaoc@iastate.edu>
    Stephanie Reinders <srein@iastate.edu>.

NIST team (evaluation dataset structure, evaluation design and report):
    Haiying Guan <haiying.guan@nist.gov>
    Jonathan Fiscus <jonathan.fiscus@nist.gov>

2021.08.09 - README updated by Haiying Guan
2020.11.05 - README updated by Haiying Guan
2020.10.14 - README updated by Haiying Guan
2020.09.24 - README created by Haiying Guan

Appendix B: Steganography detection dataset ReadMe file for evaluator

Open Media Forensics Challenge (OpenMFC) Steganography Detection Dataset

1. Introduction

OpenMFC Steganography Detection Dataset (OpenMFC-StegD) is a test and evaluation dataset built by the NIST OpenMFC Program in collaboration with steganography team in Iowa State University. This release is ONLY being released for program-internal discussions.

The data consists of test material derived from Open-Source Forensic Data (https://forensicstats.org/) produced by Center for Statistics and Applications in Forensic Evidence (CSAFE).

All images in this dataset have been sampled and extracted from StegoAppDB (SADB) (https://forensicstats.org/stegoappdb/), a forensics image database for mobile steganography collected by ISU forensic team. Steganography hides data (payload) in an innocent file (cover), producing a stego image. The goal of steganography is to make payload (visually and statistically) undetectable so there is no evidence of a covert communication.

Here are the image terminology definitions used in this README file. They are the same as used in SADB.

Original image - the image directly captured from the camera on the mobile device, as stored in SADB. Original image dimensions are determined by the device camera. The original image (IsOriginal = 'Y') is not a stego image (IsSteg = 'N'); and it is not a target image (IsTarget = 'N').

Input image - the image processed (downsize/crop/edit) by user. The input image could be captured from a different source camera.

Cover image - the image directly input to steganography algorithm for processing. A cover image could be an original image or an image cropped from the original image. The cropped cover image is not an original image (IsOriginal = 'N'), it is not a stego image (IsSteg = 'N'), and it is not a target image (IsTarget = 'N'). A cover image can be viewed as a 0% embedded stego image.

Stego image - Steganography processed image, which is the cover image containing payload information. The stego image is not an original image (IsOriginal = 'N'), it is a stego image (IsSteg = 'Y'), and it is a target image (IsTarget = 'Y')

A Cover image and a Stego image are a pair with the same image dimensions, one has payload and the other does not.

The major objective of this project is to use the SADB dataset to evaluate the current state-of-the-art of technologies in two research directions:

(1) Steganalysis (steg detection): to detect steganography; that is, if the probe image is stego or not;
    Target: stego image
    NonTarget: original image, input image, cover image, manipulated image which is not steg processed <e.g., splice manipulated image etc.>.

(2) Image forensics detection: to detect if the probe image is manipulated or not in general;
    Note: in forensic detection evaluation, image edition for STEG dataset is considered as benign, and is not considered as manipulated image. The edition operations include crop/cut, save as another image format, and resize.
    Target: any manipulated image (both stego image and manipulated image <e.g., splice manipulated image etc.>)
    NonTarget: original image, input image, cover image.

StegoAppDB consists of mobile phone photographs and stego images produced from mobile stego apps and includes a rich set of provenanced information for each image. StegoAppDB contains over 960,000 innocent and stego images using 10 different phone models from 24 distinct devices, whose provenanced data contains ISO and exposure settings, EXIF data, stego app, message information, embedding rate, and other information.

The dataset is structured similarly to the OpenMFC20 Image dataset.

The dataset was generated from a collection of approximately 56,000 images.

```
2. Directory Structure

  ReadMe.txt - This file

  /probe     - Directory of images to be analyzed for various manipulations

  /world     - Directory of images that simulate a real-world collection of images and base images

  /indexes   - Directory of index files indicating which images should be analyzed

  /reference - Directory of subdirectories for each evaluation task, containing a file of trial
metadata, the reference masks, and the journal files

  /documents - Directory of required documents

3. System Input Files

The index files are pipe-separated CSV formatted files.
The index file for the STEG Manipulation task has the columns:

Required:

  TaskID                Detection task ID
                        For STEG detection datasets, the value is fixed as 'stegd'
                        (e.g., "stegd")

  ProbeFileID           Label of the probe image
                        In general, the MD5 of the probe file is used as ProbeFileID.
                        (e.g., "00003e6a1efc7022da825396dc680343")

  ProbeFileName         Full filename and relative path of the probe image
                        In general, the MD5 of the probe file with extension is used as ProbeFileName.
                        (e.g., "/probe/00003e6a1efc7022da825396dc680343.jpg")

  ProbeWidth            Width of the probe image
                        'image_width' in the ISU sample spreadsheet
                        (e.g., 4000)

  ProbeHeight           Height of the probe image
                        'image_height' in the ISU sample spreadsheet
                        (e.g., 300)

  ProbeFileSize         File size of probe
                        'image_bytes' in the ISU sample spreadsheet
                        (e.g., 2500)

Optional:

  None

4. Reference Files

The reference files are pipe-separated CSV formatted files.

All column value type is string (if possible).

The reference file for the STEG Manipulation task has the columns:

Required columns:

  TaskID                Detection task
                        For STEG detection datasets, the value is fixed as 'stegd'
                        (e.g., "stegd")

  ProbeFileID           Label of the probe image
                        In general, the MD5 of the probe file is used as ProbeFileID.
                        Note: If the MD5 of two different files are the same, remove one of the test
                        probe.
                        (e.g., "001f9af3165a39c9e42aee922f874326")
```

ProbeFileName	Full filename and relative path of the probe image In general, the MD5 of the probe file with extension is used as ProbeFileName. Note: The test (probe) file (both the target STEG file and the non target original file) are all in the "/probe" directory. (e.g., "/probe/001f9af3165a39c9e42aee922f874326.jpg")
IsTarget	If the image is manipulated ("Y") or not ("N") 'IsTarget' in the ISU sample spreadsheet (e.g., "Y")
BaseFileName	Full filename and relative path of the base image (before STEG) of the given probe (after STEG) Note: The base file of a target probe file is in the '/world' directory. In general, the base file should be the original image directly captured from the camera. In practice, if the original image is hard to retrieve, the cover image or input image can be used as base image. (e.g., "/world/d247cf38f1ee6c03f605d251b44b6bfd.jpg")
HPDeviceID	Camera device ID (not camera model ID) provided by the data collection team 'HPDeviceID' in the ISU sample spreadsheet If "UNDEF", the data is unknown, or not provided for training. (e.g., "MK-NEX5T", or "Pixel2-1")
HPSensorID	Camera sensor ID provided by the data collection team Format: HPDeviceID_primary or HPDeviceID_secondary For iPhone camera, the back camera is primary, and the front camera is the secondary camera. (e.g., "IPhoneX6_primary" is the back camera of IPhoneX, device #6; "IPhoneX6_secondary" is the front camera of IPhoneX, device #6; "Pixel2-1_primary") 'HPSensorID' in the ISU sample spreadsheet
IsSteg	If the image is STEG manipulated or not. 'IsSteg' in the ISU sample spreadsheet (e.g., "Y")
ImageType	The image type in STEG dataset enumerate value ["original", "input", "cover", "stego"] 'ImageType' in the ISU sample spreadsheet (e.g., "stego")
ExposureMode	The exposure mode of the original image ExposureMode value ["Auto", "Manual"] 'ExposureMode' in the ISU sample spreadsheet (e.g., "Auto")
ExposureTime	The exposure time of the original image ExposureTime value is of form: 1/k where k is an integer greater than zero. 'ExposureTime' in the ISU sample spreadsheet (e.g., "1/120")
CameraISO	The camera ISO setting. 'CameraIso' in the ISU sample spreadsheet (e.g., "460")
EmbeddingMethod	The embedding method of the STEG app EmbeddingMethod value ["PixelKnot", "PocketStego", "Pictograph", "Passlok", "MobiStego", "Steganography-Meznik"] 'EmbeddingMethod' in the ISU sample spreadsheet (e.g., "PixelKnot")
EmbeddingRate	The embedding rate (percentage) EmbeddingRate value should be a floating-point number 'EmbeddingRate' in the ISU sample spreadsheet (e.g., 0.19999187)
ImageFormat	The image format of the test probe 'ImageFormat' in the ISU sample spreadsheet

```
                        (e.g., "PNG", or "JPG")

  CameraModel           The camera model or the device model
                        'CameraModel' in the ISU sample spreadsheet
                        (e.g., "Pixel2")

  JPGQuality            If the test probe image is JPG image, then JPG quality;
                        If the test probe image is not JPG image, do not fill the value.
                        'JPGQuality' in the ISU sample spreadsheet
                        (e.g., 90)

  FNumber               Aperture controls the brightness of the image that passes through
                        the lens and falls on the image sensor. It is expressed as a f-number.
                        'FNumber' in the ISU sample spreadsheet
                        (e.g., 1.8)

Optional:

  StegImageID           The image ID in the original dataset
                        'StegImageID' in the ISU sample spreadsheet
                        (e.g., "610822")

  StegImageFilename     The image filename in the original dataset
                        'StegImageFilename' in the ISU sample spreadsheet
                        (e.g., "610822.JPG")

  CoverFileName         Full filename and relative path of the cover image of the given probe
                        Note: The cover image file of a target probe file is in the '/world'
                        directory.
                        (e.g., "/world/d247cf38f1ee6c03f605d251b44b6bfd.jpg")

  CameraManufacturer    The camera manufacturer company name in the ISU sample spreadsheet
                        (e.g., "Google")

  CameraModelName       The camera model name
                        'CameraModelName' in the ISU sample spreadsheet
                        (e.g., "Pixel 2")

  WhiteBalance          The white balance
                        'WhiteBalance' in the ISU sample spreadsheet
                        (e.g., "Auto")

  MessageLength         The message length
                        'MessageLength' in the ISU sample spreadsheet
                        (e.g., 769)

  MessageDictionary     The message dictionary filename
                        'MessageDictionary' in the ISU sample spreadsheet
                        (e.g., "shakespeare_henryviii.txt")

  MessageStartingIndex  The message starting index
                        'MessageStartingIndex' in the ISU sample spreadsheet
                        (e.g., 2810)

  StegPassword          The password used in the steg app
                        'StegPassword' in the ISU sample spreadsheet
                        (e.g., "82f7fb4e-f4")


5. Dataset Generation

In general, there are two types of stego processing pipelines:
```

(1) original image (original.jpg) -> steg system -> steg image (steg.jpg)

The dataset could include the following two probe images with reference columns like this:

ProbeFileName	BaseFileName	CoverFileName	IsTarget
probe/steg.jpg	world/original.jpg	world/original.jpg	Y
probe/original.jpg	world/original.jpg		N

(2) app -> crop cover (cropcover.jpg) -> steg system -> steg image

The dataset could include the following two probe images with reference columns like this:

ProbeFileName	BaseFileName	CoverFileName	IsTarget
probe/steg.jpg	world/original.jpg	world/cropcover.jpg	Y
probe/cropcover.jpg	world/original.jpg		N

6. File Naming

The image files in this release will be named <randomString (or MD5 of the probe file)>.<extension>.

7. Distribution

THIS DATA IS PROVIDED "AS IS" for use in the OpenMFC Program. With regard to this data, NIST/ISU/CMU MAKES NO EXPRESS OR IMPLIED WARRANTY AS TO ANY MATTER WHATSOEVER, INCLUDING MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE.

8. Contacts

If you have any questions about this dataset, please contact the following people:

Iowa State University team (source data collection and evaluation dataset generation):
Jennifer L Newman <jlnewman@iastate.edu>
Yong Guan <guan@iastate.edu>
Li Lin <llin@iastate.edu>
Wenhao Chen <wenhaoc@iastate.edu>
Stephanie Reinders <srein@iastate.edu>.

NIST team (evaluation dataset structure, evaluation design and report):
Haiying Guan <haiying.guan@nist.gov>
Jonathan Fiscus <jonathan.fiscus@nist.gov>

2021.08.09 - README updated by Haiying Guan
2020.11.09 - README update by Jennifer Newman - updated metadata definitions with values and names
2020.11.05 - README updated by Haiying Guan - separate README_performer and README_evaluator, update the reference metadata definition with more details.
2020.10.14 - README updated by Haiying Guan - define the reference columns given ISU metadata spreadsheet
2020.09.24 - README created by Haiying Guan