Authenticity and Confidentiality in Sharing Digital Objects

Identify Plagiarism in Digital Photography

Amangeet Samra, Amrita Mande, Catherine Jimerson, Diamond Rorie, and Mahesh Arumugam

W233 Project Group #2

1 Problem Statement

We propose investigating the authenticity and confidentiality aspects of sharing digital objects, especially digital photographs, in news publications. More specifically, in the context of recent fake news proliferation, we aim to address the problem of ensuring authenticity to a published photograph while remaining anonymous both to the news publisher and the reader. The project aims to design and implement a system that provides robust confidentiality to a source of a digital object while allowing a publisher to authenticate the object through a trusted authority for authenticity (i.e., original and not fabricated beyond acceptable edits) and verify that the source is the owner of the object. In addition, the project aims to construct a *lineage* of the edits and measure the difference between the objects. In this project, we consider the following use cases.

1. *The owner claims ownership of the object.* For example, a well-known photographer wants to copyright the photographs.
2. *The owner renounces their ownership of the object.* For example, a photographer clicks a photograph of some compromising scenario. And the owner does not prefer to be associated with the click.

2 Literature Review

Since we focus on the authenticity and confidentiality aspects of sharing objects, we investigated existing work on these two aspects.

1. **The case for the confidentiality of the source.** Historically, from the journalism perspective, sources should only be confidential when necessary [1]. Now the ability of the internet to ruin a person's life for a perceived slight or membership to a certain group is a given; everyday people wonder if they will become the next internet's most wanted [2]. In the age of internet confidentiality, privacy has never been more prized and more easily subverted [2, 3]. Frameworks exist that provide sharing pathways where the pathways do not identify the users [4, 5]. Tangentially, we propose a system that provides confidentiality to the source (if desired) while allowing the reporter or any other third party to authenticate the originality and volume of edits done to the piece of media (the main use case being digital photographs).
2. **The case for authenticity.** The proliferation of "deep fakes" in the media has created a need for any third party that wants to take a piece of media and use it to check the providence thoroughly [6]. Providence and edit checking are available to experts in their related fields [7], but may be unusable or impractical for journalists or, say, an art expert who wants to know that they are buying authentic digital art [8]. In addition, other mechanisms (including Blockchain, e.g., [9]) address fake news using a verification framework that involves all the actors (the source, the publisher, and the reader).

3 Preliminary Architecture and Proposal

Figure 1 shows the preliminary architecture of our system. Next, we discuss the architecture for the two use cases we identified in Section 1.

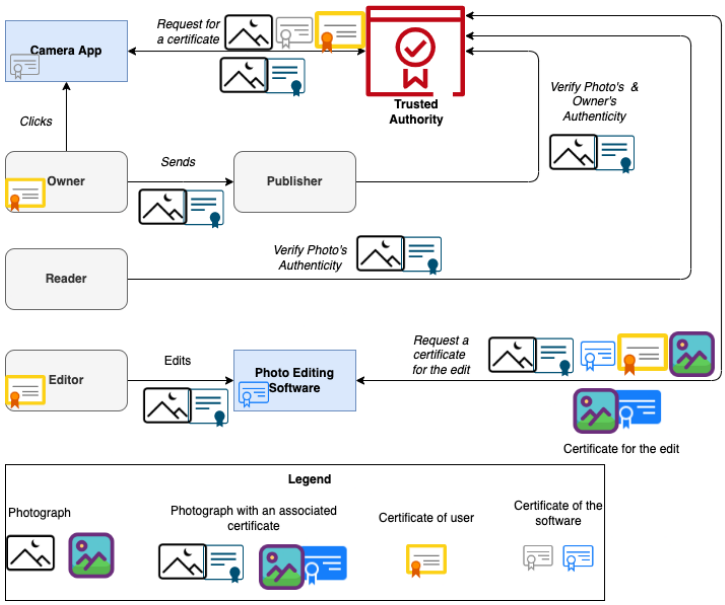

Figure 1: Proposed architecture of the system

The owner claims ownership of the object.

1. Owner takes a picture using a camera app and requests a certificate from a Trusted Authority (*TA*).
2. The TA successfully issues the certificate.
3. Upon being sent to the publisher, the photo's authenticity is cross-verified with the TA.
4. A reader can also verify the photo's authenticity with the TA.
5. On edit of a photograph, the TA will issue a new certificate depending on the level of edits.

The owner renounces their ownership of the object.

1. Suppose the owner does not prefer to be associated with the click. The TA issues the certificate without associating that with the user certificate. For example, if a person sees a celebrity engage in dangerous behavior, there is value in holding the celebrity accountable. However, the person must account for their safety against the fanbase.
2. Owner chooses to remain anonymous, in which case the publisher will accept the denounced owner role and verify the certificate with the TA.
3. A reader can also verify the photo's authenticity with the TA.
4. On edit of a photograph, the TA will issue a new certificate depending on the level of edits.

4 Potential Contributions from Each Member

Table 1 identifies each group member's potential contributions. The team will review these commitments throughout the project and make appropriate adjustments. In addition, the team communications agreement document is available at `https://bit.ly/3SK5MEC`.

Member	Potential Contributions
Amangeet Samra	Coding and final paper discussion
Amrita Mande	Architecture, uses case development, and coding
Catherine Jimerson	Final paper (including methods, results, literature review) and coding
Diamond Rorie	Literature review and final paper (including motivation survey of related work)
Mahesh Arumugam	Architeture, typesetting of the final paper, Grammarly verification, and coding.

Table 1: Potential contributions from each member of Group #2

5 Proposed Milestones

Table 2 identifies the project milestones, deliverables, and deadlines.

Milestone	Description	Expected ETA
Project proposal	Project proposal submission	September 30, 2022
Checkpoint #1	1. Finalize use cases 2. Review and finalize architecture and workflow 3. Design APIs for components	October 19, 2022
Mid-term review	1. Preliminary project presentation & report review 2. Progress and adjustments if needed 3. Coding components of the system	November 4, 2022
Checkpoint #2	1. Coding complete and integration testing 2. Draft project report	November 23, 2022
Presentation rehearsal	Project presentation rehearsal	November 30, 2022
Class project presentation	Class presentation	Week of December 5, 2022
Final paper review	Final paper review	Week of December 5, 2022
Final project paper	Final project report submission	December 9, 2022

Table 2: Proposed milestones of the project

References

[1] K. Tim Wulfemeyer. Use of anonymous sources in journalism. *Newspaper Research Journal*, 4(2):43–50, 1983.

[2] Svana Calabro. From the message board to the front door: Addressing the offline consequences of race-and gender-based doxxing and swatting. *Suffolk UL Rev.*, 51:55, 2018.

[3] Laura Durity. Shielding journalist-"bloggers": The need to protect newsgathering despite the distribution medium. *Duke L. & Tech. Rev.*, 5:1, 2005.

[4] Stefan Contiu, Sébastien Vaucher, Rafael Pires, Marcelo Pasin, Pascal Felber, and Laurent Réveillère. Anonymous and confidential file sharing over untrusted clouds. In *2019 38th Symposium on Reliable Distributed Systems (SRDS)*, pages 21–2110, 2019.

[5] Danan Thilakanathan, Rafael Calvo, Shiping Chen, and Surya Nepal. Secure and controlled sharing of data in distributed computing. In *2013 IEEE 16th International Conference on Computational Science and Engineering*, pages 825–832, 2013.

[6] Christopher Chun Ki Chan, Vimal Kumar, Steven Delaney, and Munkhjargal Gochoo. Combating deepfakes: Multi-lstm and blockchain as proof of authenticity for digital media. In *2020 IEEE/ITU International Conference on Artificial Intelligence for Good (AI4G)*, pages 55–62. IEEE, 2020.

[7] Alan J Cooper. Detecting butt-spliced edits in forensic digital audio recordings. In *Audio Engineering Society Conference: 39th International Conference: Audio Forensics: Practices and Challenges*. Audio Engineering Society, 2010.

[8] Qin Wang, Rujia Li, Qi Wang, and Shiping Chen. Non-fungible token (nft): Overview, evaluation, opportunities and challenges. *arXiv preprint arXiv:2105.07447*, 2021.

[9] Adnan Qayyum, Junaid Qadir, Muhammad Umar Janjua, and Falak Sher. Using blockchain to rein in the new post-truth world and check the spread of fake news. *IT Professional*, 21(4):16–24, 2019.