Secure Media Timestamping: Challenges, Solutions, and Frameworks

Hosam Alamleh and Laura Estremera

Newspaper proof-of-life problem

Understanding issues in secure timestamping

- **The first problem** is to prove that specific media was recently created, rather than in the past, is akin to what is known as the "Newspaper proof-of-life problem," as popularized in movies. In this scenario, kidnappers provide evidence of the hostage's current status by sending a photo of the hostage alongside a newspaper from the same day. The newspaper serves as evidence that the media is recent.
- **The second problem** is to prevent someone to create media in the future and claim it was created in the past. An example of this could be fabricating an alibi for a crime. Suppose someone committed a crime at a specific location on a particular day. To evade suspicion, they take a photograph of themselves at a different location but alter the metadata of the image to reflect the date and time of the crime. They could then present this falsified media as evidence to support their claim that they were elsewhere during the commission of the crime.

Current solutions

- Metadata
- Watermarking
- Blockchain Technology
- Stenography

Design requirement

1. time-proving knowledge:
    a. Accessing temporal information via media depends on obtaining knowledge not available at various time points, which is straightforward in scenarios where future knowledge is disclosed, but challenging when dealing with past-exclusive knowledge.
    b. One approach to acquiring past-exclusive information involves a third-party entity digitally signing the timestamp, ensuring exclusivity since only the third party possesses the private key.
    c. Another method involves entrusting a third party to both conceal and provide the confidential past-exclusive information

Design requirement (cont)

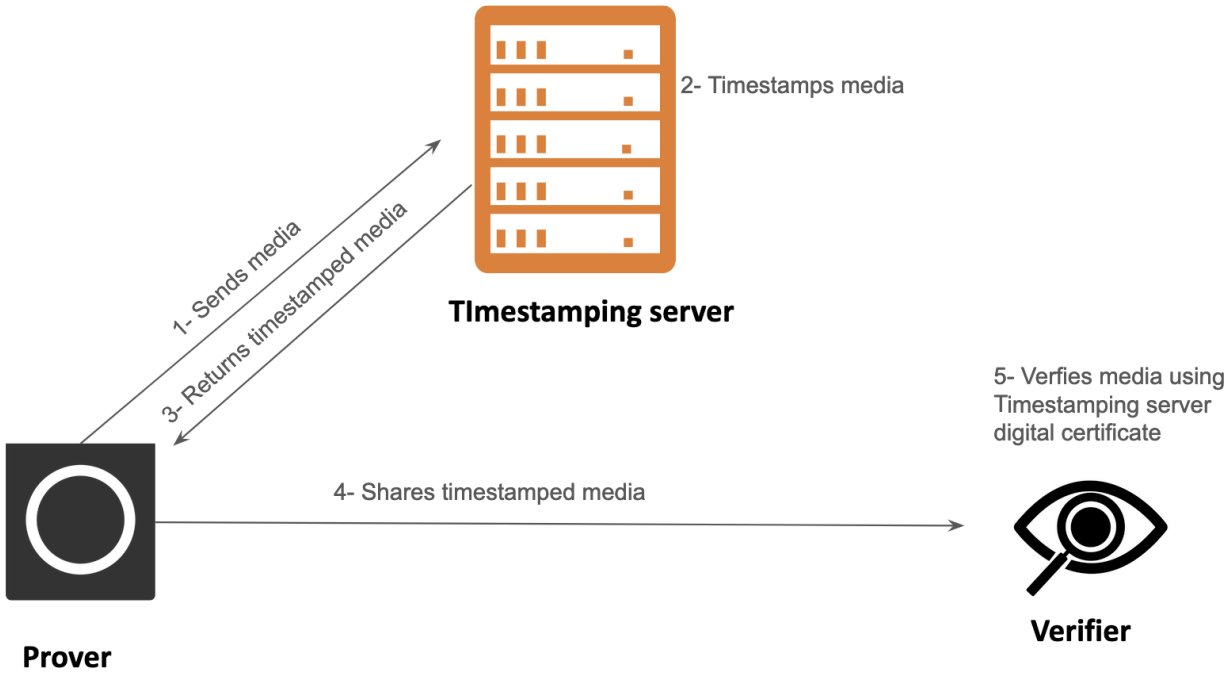
2. Embedding timestamp:
    a. To securely implement time-proving knowledge and prevent misuse, it is essential to involve a third party in the media generation process, either by having the media generator reside within a third-party entity or having a third-party entity oversee the media generation process.
    a. Traditional metadata is inadequate for verification, and while blockchain implementation is a potential solution, it introduces trust concerns regarding third-party entities within the system, such as malicious blockchain entities or manipulation by oracles.
    b. Watermarking and stenography emerge as viable alternatives, with watermarking being preferred as it offers a more uniform and verifiable approach while avoiding loss of information.

Design requirement (cont)

3. Verifying timestamp:
    a. To verify the attached timestamp, it is essential to first extract the timestamp from the digital media through methods such as stenography or watermarking.
    b. The next step involves verifying the extracted timestamp against the time when the time-proving knowledge was generated, such as confirming the authenticity of a digital signature using the public key of the third-party entity.

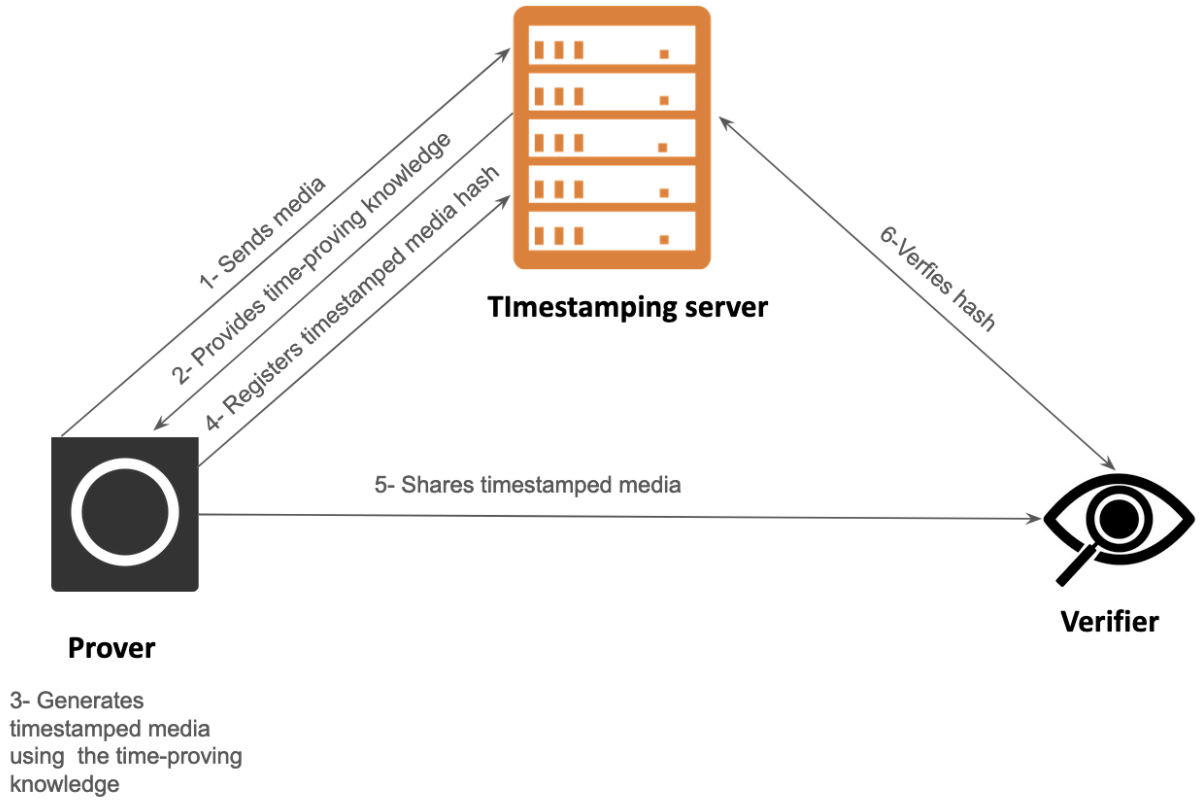
Proposed frameworks

- Media generation at timestamping server



Proposed frameworks

- Media generation under timestamping supervision



Discussion

- Timestamping is an important issue that currently lacks satisfactory solutions, and the proposed solutions offer unrealistic approaches for a very complex problem.
- One drawback of the proposed frameworks is a single point of failure, where if the timestamping server fails, the entire system fails.
- Another issue is the difficulty in scaling, as an increasing number of participants and large media files could overload the system.
- A potential solution could be to implement distributed timestamping servers similar to Domain Name Servers, but until a breakthrough in systems architecture or cryptography emerges, solving this problem effectively will remain very challenging

Questions?

- hosam.amleh@gmail.com