LITHUANIAN COMPUTER SOCIETY
VILNIUS UNIVERSITY, INSTITUTE OF DATA SCIENCE AND DIGITAL TECHNOLOGIES
LITHUANIAN ACADEMY OF SCIENCES

16th Conference on

DATA ANALYSIS METHODS
for Software Systems

November 27–29, 2025

Druskininkai, Lithuania, Hotel "Europa Royale"
https://www.mii.lt/DAMSS

VILNIUS UNIVERSITY PRESS
Vilnius, 2025

Contacts:

Dr. Jolita Bernatavičienė
jolita.bernataviciene@mif.vu.lt
Prof. Olga Kurasova
olga.kurasova@mif.vu.lt
Tel. (+370 5) 2109 315

https://doi.org/10.15388/DAMSS.16.2025
ISBN 978-609-07-1200-9 (digital PDF)

Zero-Knowledge Proofs for Digital Image Authenticity

Laura Atmanavičiūtė

Kaunas Faculty
Vilnius University

laura.atmanaviciute@knf.vu.lt

Ensuring the authenticity of digital images has become a major challenge in an era where editing tools and generative models can easily alter visual content. It is often difficult to tell whether an image is genuine or the result of manipulation, especially when metadata or watermarks can be removed or forged. Zero-knowledge proofs (ZKPs) provide a cryptographic approach to this problem by allowing one party to prove that an image has undergone only permitted transformations, without revealing any information about the original version. This approach combines verifiability and privacy, offering a possible foundation for privacy-preserving image authentication systems. This study investigates how modern zero-knowledge proof systems can be applied to verify image transformations. It focuses on recent advances in zk-SNARKs, zk-STARKs, and recursive or folding-based proof schemes such as Halo2 and Nova, which make it possible to generate compact proofs that can be quickly verified even for complex computations. The research begins with a theoretical analysis of these systems, comparing their setup assumptions, proof sizes, verification speeds, and scalability. By representing standard image operations, such as cropping, resizing, brightness and contrast adjustment, or filtering as arithmetic circuits, the study shows how visual transformations can be expressed in a form suitable for zero-knowledge verification. This allows the verifier to check that a given output image truly results from a valid transformation of some original image, without ever revealing that original. The experimental part of the research builds on an open-source folding-based zk-SNARK framework designed for verifiable image transformations. The proof-of-concept experiment tests how efficiently such proofs can be generated and verified for high-resolution images, using common transformation scenarios. Several performance indicators are analyzed, including proof

generation time, peak memory use, proof size, and verification speed. The results demonstrate that proofs remain compact and that verification consistently takes less than a second, confirming the practical potential of zero-knowledge verification. However, the proving phase still requires considerable computational effort, particularly for larger images, where time and memory demands grow rapidly. These findings highlight the main trade-off in current zero-knowledge systems: while verification is efficient and independent of input size, the cost of proof generation remains a key limitation. Despite this, the research confirms that zero-knowledge proofs can serve as a promising basis for privacy-preserving verification of digital images and other multimedia content. The approach aligns well with broader trends in decentralized authenticity frameworks and digital provenance systems. Future improvements in circuit optimization, hardware acceleration, and hybrid post-quantum schemes could make zero-knowledge verification practical for real-world use, bridging the gap between cryptographic research and applied media authenticity.