

УДК 621.391

Vlasenko Pavlo¹

¹ PhD student, National University «Zaporizhzhia Polytechnic»

A METHOD FOR SOURCE-SIDE AUTHENTICATION IN ANALOG VIDEO TRANSMISSION

As previously emphasized by the authors in their prior research [1], the critical role of analog video systems in mission-critical unmanned applications is attributed to their low latency, cost-effectiveness and resilience in noisy environments and signal conditions. However, these systems remain inherently insecure, which highlights the necessity not only for incorporation of strong encryption methods, but also incorporation of reliable mechanisms of signal source verification to counter spoofing and ensure signal origin authenticity.

Historically, the primary focus of analog video protection systems has been on prevention of content unauthorized viewing and copying, rather than origin of the signal verification. Techniques such as Macrovision analog copy protection and

the Copy Generation Management System for Analog (CGMS-A) were designed to defeat duplication devices but lacked any capability to verify the identity of the transmitter. Even more advanced methods, such as watermarking and embedded control bits, did not incorporate cryptographically secure authentication mechanisms, leaving such systems vulnerable to spoofing, relay, and signal injection attacks [2][3]. The absence of standardized asymmetric cryptographic approaches to analog signal source verification represents a critical gap in the design of secure, mission-critical video transmission infrastructure, and presents a viable field of research.

Early conditional-access systems for analog broadcasting were primarily concerned with content encryption and subscriber authorization, using techniques such as session key distribution and scrambling control signals, embedded within VBI lines. However, these mechanisms addressed content confidentiality rather than source authentication. As noted by Yang [4], “one-way authentication is also needed to verify the origin of services” yet implementations were mostly based on symmetrical algorithms and private-key systems that provided no cryptographic proof of transmitter identity. This persistent gap in the analog signal protection model reinforces the need for secure and verifiable methods of source validation in modern unidirectional transmission environments.

The system described in the paper is designed to embed cryptographic metadata, generated using asymmetric algorithms instead of group-master keys system [4], into the video signal path without requiring a reverse communication channel, making it suitable for one-way or offline validation scenarios.

Potential application domains include: (1) multi-source environments where source trust is essential; (2) resistance to spoofing by fake or hijacked transmitters; (3) mitigation of video-based denial-of-service attacks through source-level filtering; (4) secure forensic archiving of analog footage with verifiable origin; (5) lawful or military deployments where source attribution is mandatory.

The proposed signal source authentication method relies on embedding an encrypted and cryptographically signed metadata into the analog signal path at the transmission side. The system architecture includes a source-side cryptographic module that encrypts metadata using receiver public key and generates digital signatures for the data packet, which are then injected into predefined intervals of the signal using amplitude or timing modulation techniques. On the receiver side, the verification unit extracts the metadata, decrypts the payload using receiver private key, and validates the signature using a stored transmitter public key, without the need for two-way communication or direct fixed key sharing. The method is designed to be platform-independent and suitable for integration with existing analog transmission chains. Further technical details, including data encoding formats, error correction methods, synchronization schemes, packet segmentation,

noise resistance and reliability under interference and signal distortion are subjects of ongoing research.

REFERENCES

1. Malyi O., Vlasenko P. The Need of Advanced Analog Video Scrambling Methods for Mission-Critical Unmanned Vehicles Applications. Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій: тези доповідей XII Міжнародної науково-практичної конференції (10–12 грудня 2024 р., м. Запоріжжя). Запоріжжя: НУ «Запорізька політехніка», 2024. С. 22–23. ISBN 978-617-529-487-1.
2. Macrovision Corporation. Analog Protection System: A Presentation to the Analog Reconversion Discussion Group. March 5, 2003. Available at: https://w2.eff.org/IP/DMCA/Macrovision_v_321Studios/20030320_Macrovision_APS.pdf
3. US7162146B2 – System and method for the assertion and identification of rights information in an analog video signal. U.S. Patent. Issued January 9, 2007.
4. Yang C.-H. Design and Implementation of Cryptographic Systems Using 68HC05 Microcontrollers. Proceedings of the APCMTA 2000. Taiwan: National Kaohsiung First University of Science and Technology, 2000. P. 1–4.
5. ISO/IEC 13818-1:2018. Information technology – Generic coding of moving pictures and associated audio information – Part 1: Systems.
6. ISO/IEC 9798-2:2019. Information technology – Security techniques – Entity authentication – Part 2: Mechanisms using symmetric encipherment algorithms.