DOI: 10.3217/978-3-85125-603-1-17

# Depreciating Motivation and Empirical Security Analysis of Chaos-Based Image and Video Encryption

Mario Prieshuber[1], Thomas Hütter[1], Stefan Katzenbeisser[2], and Andreas Uhl[1]

### Abstract

Over the past years an enormous variety of different chaos-based image and video encryption algorithms have been proposed and published. While any algorithm published undergoes some more or less strict experimental security analysis, many of those schemes are being broken in subsequent publications. In this work we show that two main motivations for preferring chaos-based image encryption over classical strong cryptographic encryption, namely computational effort and security benefits, are highly questionable. We demonstrate that several statistical tests, commonly used to assess the security of chaos-based encryption schemes, are insufficient metrics for security analysis. We do this experimentally by constructing obviously insecure encryption schemes and demonstrating that they perform well and/or pass several of these tests. In conclusion, these tests can only give a necessary, but by no means a sufficient condition for security. As a consequence of this work, several security analyses in related work are questionable; further, methodologies for the security assessment for chaos-based encryption schemes need to be entirely reconsidered. For more details, we would like to refer to the original work [1].

## REFERENCES

[1] M. Preishuber, T. Hütter, S. Katzenbeisser, and A. Uhl, "Depreciating motivation and empirical security analysis of chaos-based image and video encryption," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 9, pp. 2137–2150, 2018. [Online]. Available: 10.1109/TIFS.2018.2812080

[1] University of Salzburg, Department of Computer Sciences {mpreis,thuetter,uhl}@cosy.sbg.ac.at
[2] University of Darmstadt katzenbeisser@seceng.informatik.tu-darmstadt.de