
Information technology — Biometric presentation attack detection —

Part 1: Framework

*Technologies de l'information — Détection d'attaque de présentation
en biométrie —*

Partie 1: Structure





COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2023

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Characterization of presentation attacks	3
4.1 General.....	3
4.2 Presentation attack instruments.....	3
5 Framework for presentation attack detection methods	4
5.1 Types of presentation attack detection.....	4
5.2 The role of challenge-response.....	5
5.2.1 General.....	5
5.2.2 Challenge-response related to liveness detection.....	6
5.2.3 Liveness detection not related to challenge-response.....	6
5.2.4 Challenge-response not related to biometrics.....	6
5.3 Presentation attack detection process.....	6
5.4 Presentation attack detection within biometric system architecture.....	7
5.4.1 Overview in terms of the generalized biometric framework.....	7
5.4.2 PAD processing considerations relative to the other biometric subsystems.....	8
5.4.3 PAD location implications regarding data interchange.....	9
6 Obstacles to biometric impostor presentation attacks in a biometric system	9
Bibliography	11