Submission Summary

Conference Name	11th International Conference on Computer Vision & Image Processing (CVIP 2026)
Track Name	CVIP2026-Phase-II
Paper ID	1001
Paper Title	Defense-in-Depth: Tamper Localization, Self-Recovery, and Attack-Type Classification for Meaningful Secret Sharing in Privacy-Preserving Face Recognition
Abstract	Visual secret sharing-based face recognition divides face data into secret shares that reveal no information about the individual. The recent VOIDFace framework employs patch-based secret sharing to store training faces across various institutions and to provide users with a Right-To-Be-Forgotten (RTBF) property. Two main constraints hinder VOIDFace's practical application. Firstly, VOIDFace shares resemble arbitrary noise and are consequently easily identifiable as ciphertext and thus prone to harvest-now-decrypt-later attacks. Secondly, VOIDFace shares lack integrity. An adversary can secretly compromise a share and corrupt the training. Even if the breach is identified, the only option would be to discard the share and retransmit it. The proposed technique solves these problems by making the framework more secure and self-recovering. Initially, the noisy shares are embedded into cover images. This renders the ciphertext unnoticeable. Similarly, the integrity of the embedded cover images is protected with a dual layer of a fragile cryptographic hash and a semi-fragile DWT spread-spectrum watermark. The proposed technique employs a redundant embedding scheme to reconstruct the tampered block without retransmission. Additionally, a lightweight classifier is added to read the localized tamper signature to separate malicious tampering from benign channel operations. Experiments using VGGFace2 combined with LFW, CALFW, and AgeDB-30 demonstrate indistinguishable embedding (PSNR >40dB, SSIM >0.95), robust tampering detection, self-recovery, and comparable accuracy to VOIDFace, all while preserving privacy and RTBF assurances.
Created	2026-07-31 17:24:40 WET
Last Modified	2026-10-20 13:23:16 WET
Authors	**Ajnas Muhammed** (University of Coimbra) <ajnas.muhammed@isr.uc.pt>

	Iurii Medvedev (University of Coimbra) <iurii.medvedev@isr.uc.pt> Nuno Gonçalves (University of Coimbra) <nunogon@deec.uc.pt>
Primary Subject Area	Image Biometrics/ Forensics
Secondary Subject Areas	Computer Vision/ Pattern Recognition
Submission Files	CVIP_final.pdf (1.3 Mb, 2026-07-31 18:26:52 WET)