ENCRYPTION OF EVENT CAMERA DATA FOR VISUAL LOCALISATION

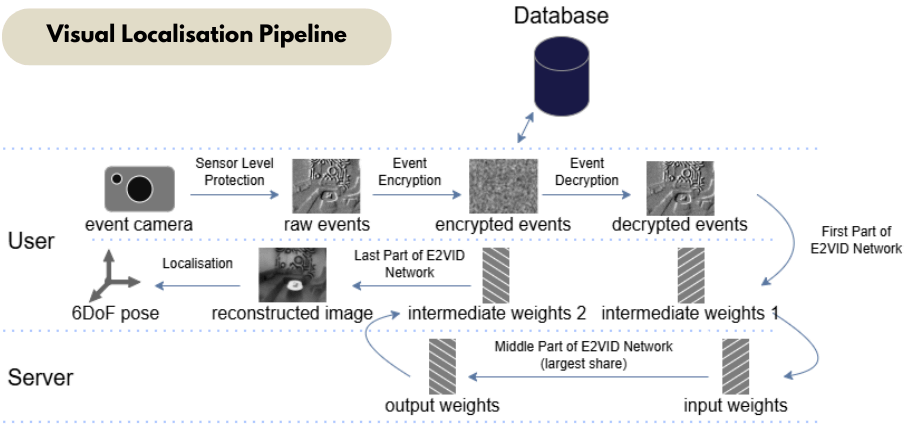
Author: Bink Boëtius | Supervisor: Tunahan Parlayici | Responsible Professor: Nergis Tömen | Examiner: Ricardo Marroquim | Faculty EEMCS, Delft University of Technology, The Netherlands

How can the encryption of raw event camera data be practically and effectively used for privacy protection in a visual localisation application?

Background & Motivation

Event-based vision is an emerging field that focuses on implementing computer vision using event cameras. In VR and AR applications, event-based vision can be used to localise the user in a pre-built environment. Earlier work by Kim et al. proposes a privacy-preserving client-server visual localisation method. Here, an honest-but-curious service provider is assumed, which only extracts visual information from data it has access to. Since other attackers might exploit this system, my research aims to enhance its security by encrypting the raw event data using the algorithm designed by Zhang et al.

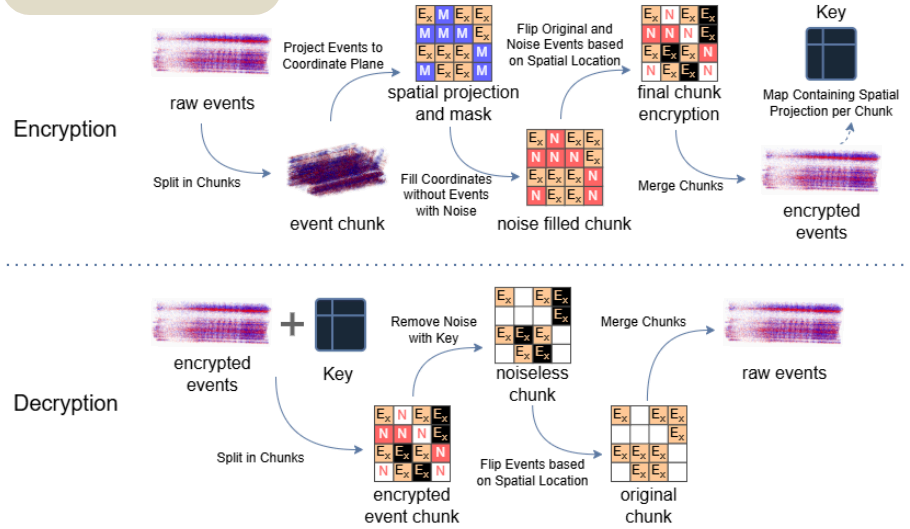
Visual Localisation Pipeline

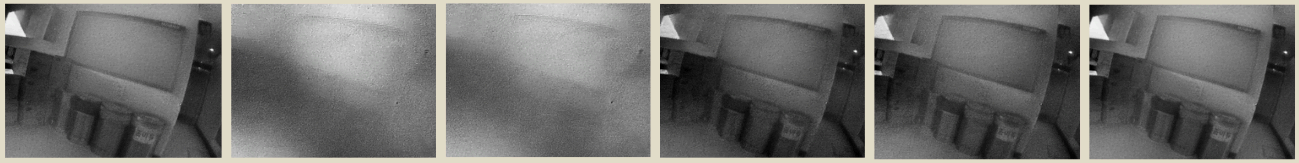


Methodology

1. The visual localisation codebase by Kim et al. was set up and slightly modified to suit the purpose of this research.
2. The average temporal event density and the average pixel intensity were calculated for all scenes in the EvRooms dataset
3. Four versions of the encryption algorithm were implemented: The original, one skipping the polarity-mapping step, one with modified noise creation, and one with both changes.
4. Privacy metrics were calculated for reconstructed images, see below, and localisation performance was measured for the original and decrypted events.
5. Differences in performance across encryption versions and relations between scene characteristics and performance were analysed.

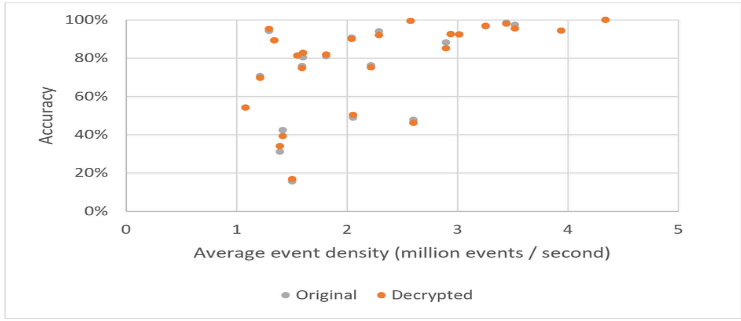
Encryption Pipeline





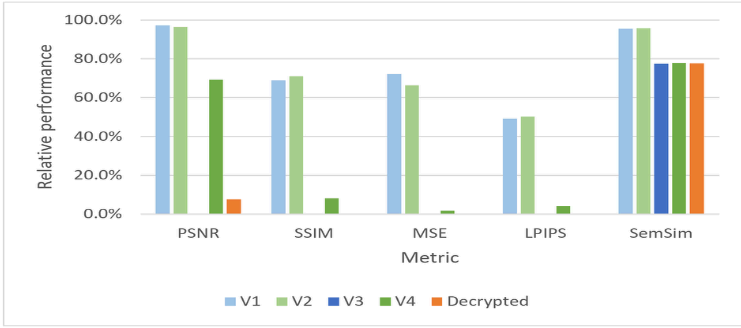
Localisation Performance

No significant difference was found between the localisation performance of the original and decrypted event streams. However, a significant influence of the average temporal event density on localisation performance was observed, as visualised below. No significant relation between the average pixel brightness and localisation performance was found.



Comparing Encryption Algorithms

The privacy measurements, shown below, demonstrate that versions of the algorithm that skip the polarity-mapping step perform considerably worse across all privacy metrics. Note that 0% is the performance of reconstructed images of the original events, and 100% is the performance of noise. Other significant differences are found, but those are relatively small. It should be noted that SemSim measurements are not taken with the intended model, which could explain the irregular results. The irregular PSNR results can be explained by the fact that infinite values are capped at 70.



Conclusion & Future Works

The encryption designed by Zhang et al. does not influence the localisation performance of the pipeline implemented by Kim et al. after decryption. The main part obscuring the data is the polarity-mapping step, which can be reversed by any attacker and therefore is not secure under Kerckhoffs's principle. Further research should explore whether raw event encryption can be achieved solely through key-dependent polarity mapping.