MSU Unconstraint Smartphone Spoof Attack Release Agreement

The MSU Unconstraint Smartphone Spoof Attack Database (MSU USSA) is released only for academic researches. Any researcher from educational institute is allowed to use this database freely for non-commercial purpose. Please read and sign your agreement to the following regulations before getting access to this database.

Regulations

Users must obey the following regulations when using this database:

- Without the permission of MSU PRIP lab, any of, but not limited to, the following behaviors will be considered illegal: redistribution, modification, commercial usage of this database, in any way or form, either entirely or partially.
- For the sake of privacy, images of all subjects in this database are only allowed for demonstration in academic publications and presentations.
- As to acknowledgement, any publications using this database should acknowledge the MSU USSA Database by citing the following reference:
  - K. Patel, H. Han and A. K. Jain, "Secure Face Unlock: Spoof Detection on Smartphones", to appear in the *IEEE Transactions on Information Forensics and Security*, 2016.
- All users using the database agree to indemnify, defend and hold harmless MSU and its officers, employees and agents, individually and collectively, from any and all losses, expenses, damages. If any, users shall pay all damages, claims, judgments or expenses caused by misuse of MSU USSA database.

Your agreement

By filling out the blanks below, you have accepted the rules above. Please send the scanned copy of this agreement to: debdebay@msu.edu. After your application is approved, you will be emailed a download link of the database, which will be valid for 72 hours.

Name (should be the supervisor/PI of the research lab):

Signature:

Organization:

Address:

Email:

Date: