

Fake Hands: Spoofing Hand Geometry Systems

Hong Chen¹, Hamed Valizadegan¹, Carrie Jackson², Shannon Soltysiak² and Anil K. Jain¹

¹Department of Computer Science and Engineering

²Forensic Science Program, Department of Criminal Justice

Michigan State University

East Lansing, Michigan 48824

chenhon2@cse.msu.edu, valizade@cse.msu.edu, jacks735@msu.edu, soltysi3@msu.edu, jain@cse.msu.edu

Hand geometry systems are widely used for attendance monitoring, access control and identity verification [1-3]. Features extracted from a presented hand shape are matched against stored genuine templates for the purpose of verification. Due to the inherent similarity of hand shapes, the hand geometry systems are not appropriate for identification and unattended high-security applications. While the idea of making fake hands to spoof hand geometry systems has been proposed [4, 5], to our knowledge, it has not been implemented in practice. In this paper, we present two simple approaches for making fake hands. Using these fake hands, we were successful in attacking a HandKey II system, produced by Recognition Systems®.

The first approach utilizes plaster for making fake hands [6]. The material used includes molding alginate, casting plaster and a peg board, on which the pegs are laid out in exactly the same fashion as in the HandKey II system. The first step is to make a molding container, which has the peg board as its bottom surface (Fig. 1(a)). After fixing the pose of a real hand according to the pegs, a mixture of alginate and water is poured into the container (Fig. 1 (b)). The solidification process takes 2 to 7 minutes, and the real hand can then be pulled out of the alginate mold without breaking it (Fig. 1 (c)). The next step is to fill the mold with mixer of plaster powder and water. Depending on the ratio of the plaster and water, it takes from 30 minutes to 24 hours for the plaster to solidify (Fig. 1 (d)). Fig. 1(e) shows how a fake hand is presented to the HandKey II system and how it gets verified by the system.

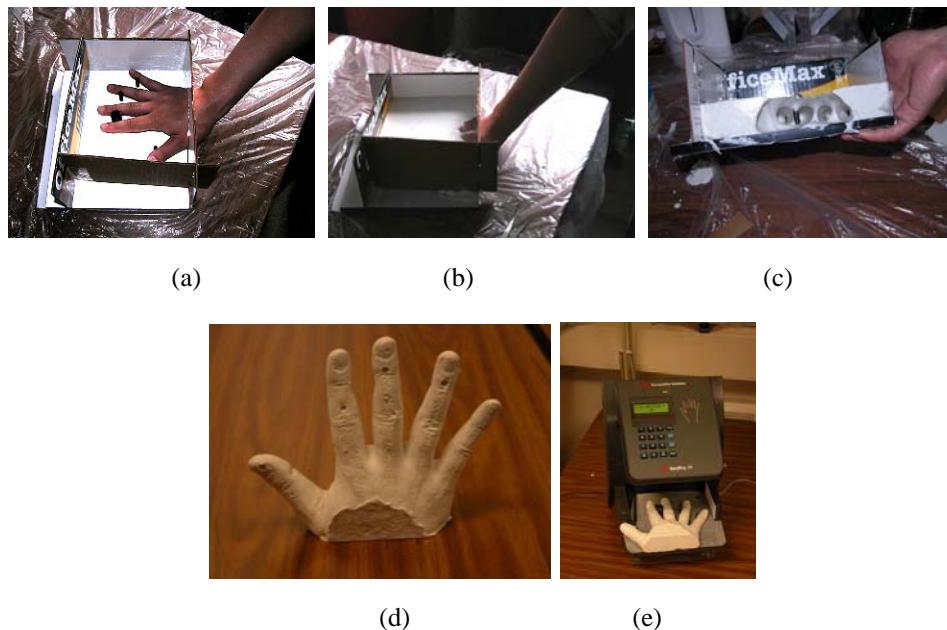


Figure 1. Making a plaster fake hand. (a) Place the hand in the correct posture; (b) fill in molding material; (c) solidified mold; (d) a plaster hand; (e) a plaster hand is presented to the hand geometry system.

The second approach makes a fake hand out of silhouette images captured by the hand geometry system and stored in an affiliate PC. An example of the silhouette images is shown in Fig. 2 (a). Although the images are distorted by scaling, they can be inversely scaled to the correct size (Fig. 2 (b)). This fake hand is made on a 2D paper card, so when presenting the card hand to the hand geometry systems, the hand should not touch the surface of the peg board. This way the system measures the distance from the card to the board and regards it as the thickness of the hand. Our experiments show that the hand geometry system is insensitive to the changes in the thickness of the hand. Fig. 3 shows that a card hand gets verified at the system.

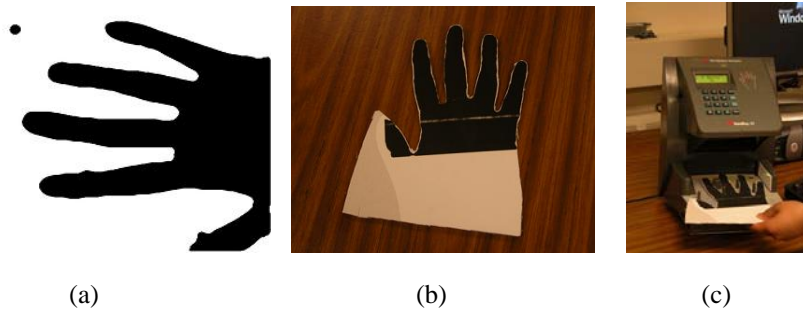


Figure 2. Making a card fake hand. (a) The silhouette of a genuine hand stored in the administrator's computer; (b) A card fake hand; (c) Presenting the fake hand to the hand geometry system.

We attempted to spoof 5 different users (hands) with the two proposed approaches. For the first approach, since the fake hands are exact duplicates of real hand shapes, they get correctly verified by the HandKey II system. While the system threshold on the matching distance is 100 for verification purpose, the actual matching distances are ~60 for the first trial, and they then decreased to 1 over the course of 10 trials, as the HandKey II system updates the matching templates incrementally. For the second approach, the matching distances decreased from ~70 to 10, as the stored templates were updated.

Although hand geometry systems are friendly to users, they are vulnerable to spoof attacks. Our experiments have shown that fake hands can be made with or without the knowledge of the genuine user (e.g., from the hand silhouette image stored in the template database). Our future work includes making a verifiable fake hand out of an arbitrarily posed hand image, which can be captured in a photo, or grabbed from a video. We are also addressing the anti-spoofing mechanism, such as liveness detection.

References

- [1] Recognition Systems Inc. <http://www.recogsys.com/index.shtml>
- [2] A.K. Jain, A. Ross and S. Pankanti, "A Prototype Hand Geometry-based Verification System", 2nd Int'l Conference on Audio- and Video-based Biometric Person Authentication (AVBPA), Washington D.C., pp. 166-171, March 22-24, 1999.
- [3] Arun Ross. "A Prototype Hand Geometry-based Verification System", M.S. Project Report, Department of Computer Science & Engineering, Michigan State University, 1999.
- [4] Benjamin Miller, Vital Signs of Identity, IEEE Spectrum, Vol. 31(2), pp. 22-30,
- [5] Dave Sims, Biometric Recognition: Our Hands, Eyes, and Faces Give Us Away, IEEE Computer Graphics and Applications, Vol. 14 (5), pp. 14-15
- [6] Life Casting, <http://www.artmolds.com>