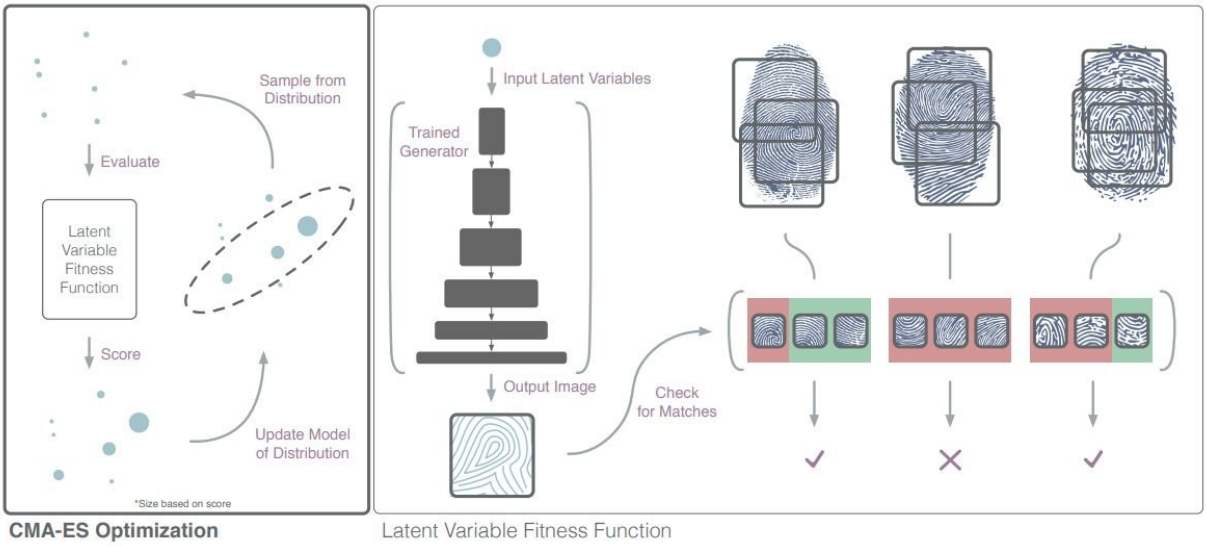
# Oh those GANs: Scanner finger technique could result in fake fingerprints

November 18 2018, by Nancy Owano




Latent Variable Evolution with a trained network. On the left is a high level overview of CMA-ES and the box on the right shows how the latent variables are evaluated. Credit: arXiv:1705.07386 [cs.CV] https://arxiv.org/abs/1705.07386

Biometric systems news: Fake fingerprints can imitate real ones. A neural network has managed to pull off fake fingerprints—those very fingerprints that are designed to work as master keys for your identification.

The work is by researchers, and they presented their paper at a

biometrics security conference in Los Angeles. "DeepMasterPrints: Generating MasterPrints for Dictionary Attacks via Latent Variable Evolution" is up on the arXiv server. Almost all author affiliations are from New York University with one other affiliation from Michigan State University. NVIDIA donated CPUs for their research.

At the heart of their research is a machine learning technique, DeepMasterPrints, which is what the fake prints are all about. The researchers wrote that "Experiments with three different fingerprint matchers and two different datasets show that the method is robust and not dependent on the artifacts of any particular fingerprint matcher or dataset."

So what paths to fakery did the researchers churn up?

Alex Hern, technology reporter for *The Guardian*, walked readers through the technique: most fingerprint readers do not read the entire finger at once, he said.

The readers do their imaging on a part of the finger that touches the scanner. Hern said the comparison takes place of the partial scan against the partial records. Here's the thing: "That means that an attacker has to match just one of tens or hundreds of saved partial fingerprint in order to be granted access."

Yet another element works in fakery attempts is in how some features of fingerprints are more common than others. "That means that a fake print that contains a lot of very common features is more likely to match with other fingerprints than pure chance would suggest," Hern said.

With those weaknesses, they used a technique that worked for their ends. The fakes that they created looked convincingly like a real fingerprint—to a human eye. This is notable because a previous

technique "created jagged, right-angled fingerprints that would fool a scanner but not a visual inspection," said Hern.

The machine learning technique was the Generative Adversarial Network. The technique succeeded in a creation of fingerprints that matched as many partial fingerprints as possible. (Prasad Ramesh in *Packt* : "A GAN network is trained over a dataset of fingerprints, then LVE searches the latent variables of the generator network for a fingerprint image that maximize the matching chance. This matching is only successful when a large number of different identities are involved, meaning specific individual attacks are not so likely.")

The method is compared to a "dictionary attack" against passwords, where a hacker runs a pre-generated list of common passwords against a security system.

As Hern pointed out, the attacks may be unable to break into specific accounts but "when used against accounts at scale, they generate enough successes to be worth the effort."

What do security sleuths say in reaction to their presentation: *Naked Security* said findings were a little worrying.

"If someone developed this into a working exploit, perhaps by printing the images with capacitive ink, it could present problems for many fingerprint recognition systems," said Danny Bradbury in *Naked Security*.

Yes, but that leads to the big question: Should we just dismiss fingerprints as an identification tool?

Sam Medley, *Notebookcheck*, would say, no, the research findings do not invalidate fingerprint scanners as a security measure. Medley wrote, "The researchers freely admit that while someone could eventually use

something like DeepMasterPrints to hack into something like a smartphone or computer, they would need to do a lot of work to optimize the AI for a specific system."

In fact, the authors themselves underscored the value of their approach. "Beyond the application of generating DeepMasterPrints, this paper successfully shows the usefulness of searching the latent space of a generator network for images, or other artifacts, that meet a given objective. This idea is surprisingly under-explored and could be useful in computational creativity research as well as other security domains."

**More information:** DeepMasterPrints: Generating MasterPrints for Dictionary Attacks via Latent Variable Evolution, arXiv:1705.07386 [cs.CV] arxiv.org/abs/1705.07386