SOPHIE NIGHTINGALE

IDENTITY FRAUD IN THE DIGITAL AGE

Advances in technology are bringing new problems to the task of detecting identity fraud, including the relatively new phenomenon of face-morphing and the synthesis of facial images.

We rely on biometric information, such as face, fingerprint, and voice, to provide a strong and permanent link between an individual and their identity. Yet this information can become compromised — sometimes unintentionally, but other times as part of an attempt to steal another person's identity. Identity fraud is a societal problem that presents a significant threat to national security. Although not a new problem, technological advances allow for increasingly sophisticated means to commit identity fraud.

Consider how a known criminal on a government watch list might attempt to travel into a different country undetected. In the past they might have created a fake passport or had a similar-looking accomplice (who is legally able to travel) submit a renewal application using their photo. Now, the fraudster can rely on the relatively new phenomenon of face-morphing. Morphing enables a fraudster to digitally combine their face with that of their accomplice in a single image. The morphed image is submitted with the accomplice's passport application. If successful, the fraudster is issued a fraudulently obtained but genuine (FOG) passport; a real document that will bypass any counterfeit detection measures in place. It is now the task of the border control officials or automatic face recognition systems to detect the manipulated photo.

In applied settings, such as border security, it is important to accurately match faces of individuals unfamiliar to us with their photo-ID, yet people show surprisingly poor unfamiliar face-matching performance (Bruce et al., 1999). The morphing technique further complicates matters because the morphed image contains some of the fraudster's facial features thus making the ID-checkers' task even more difficult. Worryingly, there is growing evidence suggesting that accurate detection of these so-called 'morphing attacks' is limited, especially for high-quality morphs, and that training attempts have little effect on accuracy (Kramer et al., 2019; Nightingale et al., 2021; Robertson et al., 2017, 2018). Face recognition systems have also been shown to be vulnerable to morphing attacks (Nightingale et al., 2021; Scherhag et al., 2019).

> **...the morphed image contains some of the fraudster's facial features making the ID-checkers' task even more difficult.**

HOW CAN WE IMPROVE PEOPLE'S ABILITY TO DETECT FACE-MORPHING?

Borrowing from facial recognition studies, it has been shown that expert forensic facial examiners and untrained super-recognisers achieve higher accuracy on challenging face identification tasks than members of the general public (Phillips et al., 2018). Research has also shown that adopting a feature-by-feature comparison strategy can improve unfamiliar face-matching (Towler et al. 2017). These lines of research suggest that human face 'specialists' might show greater accuracy in morph detection tasks, and a featural rather than holistic approach might translate to improved accuracy in the task of face morph detection. These two possibilities remain to be tested.

Another possible solution is to modify the passport-issuance process. Researchers have suggested that the best solution to the face morphing problem is to have government officials acquire photos at the place of issuance (Ferrara et al., 2014). This live enrolment approach is already used in some countries and has recently been implemented in others in response to the threat of face morphing. Although this approach would solve the problem of digital face morphing, it still does not deal with the issue of physical identity fraud techniques, such as the use of hyperrealistic silicon masks (Robertson et al., 2020).

Adapted from @Art Huntington / Unsplash.com

CAN ARTIFICIAL INTELLIGENCE HELP?

The successful application of machine learning to develop an algorithm that can accurately discriminate morphed faces from real faces remains somewhat limited, in part because of the manual effort required to generate a high-quality landmark-based morph. Therefore, training sets typically consist of relatively small numbers of morphs.

One potential way to improve the capability of machine learning for detecting morphs is to draw on a popular artificial intelligence (AI) mechanism for synthesising content: generative adversarial networks (GANs) (e.g., MorGAN; Damer et al., 2018). A GAN consists of two neural networks — a generator and a discriminator — that are pitted against one another in a game-like scenario. The generator's task is to synthesise a facial image that the discriminator accepts as 'real'. The discriminator's task is to distinguish between real faces and those synthesised by the generator. Initially, the generator produces a random array of pixels and passes this to the discriminator. If the image is distinguishable from a real face, then the generator is penalised and over many iterations, it learns to synthesise increasingly realistic faces until the discriminator is no longer able to distinguish the synthetic from the real faces. Of course, this ability to synthesise content (so-called deep fakes) brings a unique set of threats to society (Nightingale & Farid, 2022); however, it also provides the infrastructure to produce high-quality face morphs at scale and, in turn, generate a substantial training set that could be used to train human facial examiners and to improve the accuracy of computational classification of morphed and non-morphed faces.

THE ARMS RACE CONTINUES

Rapid advances in technology continue to make it easier than ever to create sophisticated and compelling fakes. Although in a technological sense, these advances are exciting and an incredible achievement, inevitably there will be individuals who use these developments for harm. Therefore, we must work to keep these threats at bay.

Dr Sophie Nightingale is a lecturer in Psychology at Lancaster University. Her research examines the challenges and opportunities posed by digital technology, especially in relation to security and forensic identification processes.