ABSTRACT

Face Morphing Attacks pose a novel threat to the security of identification documents. The fusion of the face images of two or more – similarly looking – individuals during the application process for a new travel document (i.e., passport) or identity card enables both individuals to travel with the same document. In order to develop algorithms to detect morphing attacks, large data sets of morphed face images are needed, for which in turn many similarly looking individuals need to be paired.

The study at hand uses face embeddings of openly accessible face recognition models to describe similarity between individuals. It aims at finding appropriate face recognition models, metrics to quantify similarity, morphing algorithms to fuse facial images of paired individuals, and soft biometric characteristics to analyze the attack potential of face morphs.

Results demonstrate, that image pre-selection based on Cosine or Euclidean distances between face embeddings highly improves the attack potential of morphs. Especially ArcFace and MagFace provide valuable face embeddings to quantify similarity for pre-selection. Both open source, as well as Commercial Off-The-Shelf Face Recognition Systems get fooled by morphed faces. Landmark-based, closed source morphing algorithms pose high risk for any of the tested Face Recognition Systems. On the other hand, MagFace embeddings further emerge as valuable means to detect morphed face images. Soft biometrics characteristics however were only partially relevant to predict morph success, if morphing has been conducted within similar age, gender, and race groups.

The results emphasize that face embeddings are valuable instruments on both sides of the morphing attack, image pre-selection for face morphing and detection of morphed faces.

ZUSAMMENFASSUNG

Gesichtermorphing Angriffe stellen eine neue Gefahr für die Sicherheit von Idenditätsnachweisen dar. Die Verschmelzung zweier – sich ähnlich sehender – Lichtbilder zu einem Morph, der in der Antragsstellung für ein Identitätsdokument (Pass, Personalausweis) eingereicht wird, ermöglicht es beiden Beteiligten gleichermaßen mit dem ausgestellten Dokument zu reisen. Um Algorithmen für die Erkennung solcher Morphing Angriffe zu entwickeln werden große Mengen von Morphs benötogt, welche wiederum aus vielen – sich ähnlichen – Gesichter-Paaren zusammengesetzt sein müssen.

Die hier vorliegende Studie benutzt Gesichter-Embeddings von Open Source Gesichtserkennungs-Modellen um Ähnlichkeit zwischen Individuen zu beschreiben. Das Ziel ist, passende Gesichtserkennungs-Modelle, Ähnlichkeitsmaße, Morphing-Algorithmen, und Soft-Biometrische Eigenschaften zu analysieren, um das Angriffspotential von Morphs zu verbessern.

Die Ergebnisse zeigen, dass wenn die Cosinus-Distanz oder die Euklidische Distanz zwischen zwei Gesichtern als Ähnlichkeitsmaß für die Paarung von Lichtbildern genommen wird, das Angriffspotential der resultierenden Morphs erhöht wird. Speziell ArcFace und MagFace stellen geeignete Gesichter-Embeddings für die Berechnung dieser Ähnlichkeit bereit. Sowohl Open Source, als auch kommerzielle Gesichtserkennungssysteme werden von den resultierenden Gesichtermorphing Angriffen getäuscht. Landmarkbasierte, nicht-öffentliche Morphingalgorithmen generieren hochwertige Morphs, welche ein hohes Risiko für die getesteten Gesichtserkennungssysteme darstellen. Andererseits stellen sich vor allem MagFace Gesichter-Embeddings als nützliches Werkzeug für die Erkennung von gemorphten Gesichtern heraus. Soft-Biometrische Eigenschaften sind nur zum Teil für den Erfolg des Morph-Angriffs ausschlaggebend, zumindest wenn innerhalb bestimmter Alter-, Geschlechts- und Ethnizitätsgruppen gemorpht wurde.

Die Ergebnisse betonen die Wichtigkeit von Gesichter-Embeddings auf beiden Seiten des Angriffs. Zum einen können sie für die Paarfindung vor dem Morphing eingesetzt werden, zum anderen wiederum für die Erkennung von gemorphten Gesichtern.