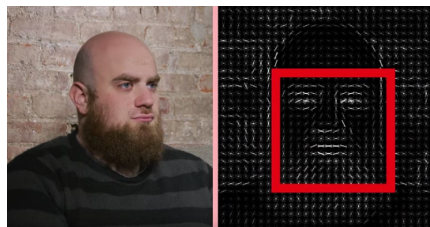


Cómo funciona el reconocimiento facial

En estos días, seguramente viste muchas fotos de amigos y familiares “avejentados” gracias a un software de tratamiento de imágenes. Luego sobrevino la duda: ¿Utilizarán esas fotos para reconocimiento facial de esos usuarios?

¿Cómo reconoce una máquina un rostro? ¿Qué detalles concretos busca y cómo los distingue? ¿De qué depende que se pueda reconocer a una persona concreta entre miles en una fotografía? Son cuestiones que, quien más quien menos, se ha preguntado alguna vez, especialmente ahora que tenemos sistemas de reconocimiento facial hasta en la sopa: Google Photos, Fotos para MacOS, Facebook... De hecho es difícil ver en acción estos sistemas «adivinando quién es quién» sin imaginar cómo son capaces de hacerlo.

Todo comienza por las imágenes digitalizadas que se convierten a blanco y negro y luego a un histograma de gradientes orientados que básicamente son vectores que indican hacia donde van las diferencias de brillo entre píxeles. Esto permite detectar los bordes de los objetos en la imagen. Con eso es relativamente fácil explorar con una especie de «plantillas» cada zona de la imagen, intentando identificar los llamados landmarks o puntos de referencia concretos: ojos, nariz, boca, etcétera, que se corresponden con círculos, trazos verticales/horizontales y demás. Se emplean hasta unos 68 de estos puntos normalmente. Cuando se tienen varios de ellos en la misma zona es porque probablemente hay un rostro humano a su alrededor.



El siguiente paso es asegurarse de que la orientación del rostro es correcta, porque la persona puede estar «mirando» en diferentes direcciones. Dado que se sabe dónde están los puntos de referencia se puede deformar la imagen en un proceso llamado normalización, estirándola hasta que encaje. Podría decirse que no queda muy bonito pero es muy práctico. De este modo se consigue que todas «miren de frente»... Más o menos.

El último paso en el reconocimiento para distinguir unas personas de otras es la clasificación. Para esto hay diferentes algoritmos. Por ejemplo el uso de redes neuronales convolucionales, que básicamente se entrenan mediante aprendizaje automático con muchas imágenes de personas distintas, a las que se suman las de la persona que se está intentando encontrar, ya de nuevo en color. Aquí hay una combinación de estadística (cuantificar las diferencias entre los puntos de referencia de dos rostros) y factor humano (confirmar al algoritmo si ha acertado o no), lo cual se hace durante la fase de entrenamiento.

Los resultados serán sólo tan buenos como bueno sea el entrenamiento y la variedad de imágenes. Todo esto puede sonar muy complicado, pero se obtiene un resultado final que cuando se trata de comparar dos rostros no es más que una puntuación en forma de porcentaje de similitud, que puede traducirse también a un «sí, son iguales» o en un «no, son diferentes».

Independientemente de lo exacto que parezca en las series de televisión, no hay espacio para el error, aunque la tecnología está mejorando. El Instituto de Estándares de Tecnología de EEUU estimó que las tasas de error declaradas están disminuyendo un 50% cada dos años y actualmente están alrededor del 0,8%. Eso es mejor que el reconocimiento de voz que tiene tasas de error superiores al 6%.

Privacidad

Pero el reconocimiento facial plantea problemas de privacidad. Una de las principales preocupaciones es que, al igual que el aumento de las bases de datos de ADN, los rasgos faciales y las fotos están siendo almacenadas por los gobiernos, que son capaces de rastrear gente, borrando cualquier noción de privacidad o anonimato.

Por otra parte, una nueva aplicación, FindFace, permite tomar fotos de una persona y usar el reconocimiento facial para encontrar sus cuentas de redes sociales. Pensada como un amanaera conveniente para conectar con amigos, la aplicación invita al mal uso. La gente puede utilizarla para exponer identidades y acosar a otros.