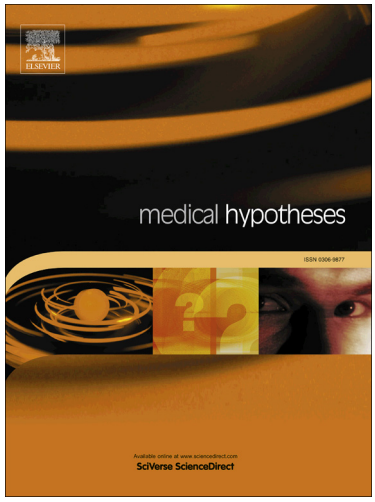

Medical information security in the era of artificial intelligence

Yufeng Wang, Liwei Wang, Chang-ao Xue

PII: S0306-9877(18)30223-8
DOI: https://doi.org/10.1016/j.mehy.2018.03.023
Reference: YMEHY 8841

To appear in: *Medical Hypotheses*

Received Date: 22 February 2018
Accepted Date: 23 March 2018

Please cite this article as: Y. Wang, L. Wang, C-a. Xue, Medical information security in the era of artificial intelligence, *Medical Hypotheses* (2018), doi: https://doi.org/10.1016/j.mehy.2018.03.023

Medical information security in the era of artificial intelligence

Yufeng Wang *a*, Liwei Wang *b*, Chang-ao Xue *a* ，*

a Department of Stomatology, Nanjing First Hospital, Nanjing Medical University, Jiangsu, 210006, China

b Department of Radiology, Nanjing First Hospital, Nanjing Medical University, Jiangsu, 210006, China

*Corresponding author.

E-mail addresses:njsdyyykqk@163.com

Yufeng Wang and Liwei Wang contributed equally to this work.

Abstract In recent years, biometric technologies, such as iris, facial, and finger vein recognition,have reached consumers and are being increasingly applied. However, it remains unknown whether these highly specific biometric technologies are as safe as declared by their manufacturers. As three-dimensional (3D) reconstruction based on medical imaging and 3D printing are being developed, these biometric technologies may face severe challenges.

Introduction

Biometrics is an identification technology that uses human biological traits and comprises fingerprint, face, iris, and finger vein recognition [1]. Most people believe that biometric technology, which has a high degree of uniqueness,is very advanced and secure. In fact, if some medical imaging materials typically used by physicians were made available, many biometric systems would be easy to crack.

The insecurity of fingerprinting identification is well known.Models for copying fingerprints to fake time attendance systems in universities and companies have even evolved into a small-scale industry [2]. Hence, iPhone X began using Face ID to replace Touch ID. Given the iPhone's tremendous consumer influence, facial recognition is likely to become a popular biometric technology in the coming years. However, whether facial recognition is as safe as we believe it is remains unknown. Facial three-dimensional (3D) reconstruction at various levels of precision can be accomplished via several methods, such as traditional computed tomography (CT), magnetic resonance imaging (MRI), cone-beam computed tomography (CBCT, used in dental scanning), and medical 3D scanner[3-5]. We are interested in learning whether reconstructing faces using these techniques can be 3D printed and used to crack facial recognition systems.

Hypothesis

Will medical imaging development threaten biometric technology?Accurately reconstructing the human face can be accomplished by using multiview imaging or medical 3D scanner and subsequently be printed on