WISE AI™

WISE LIVENESS

WHITEPAPER

Jan 2023

WISE AI™

Why KYC Matters

Customer data is extremely powerful. Take for example the banking industry, which was built on top of customer data well before the age of computers, and will continue to do so in the distant future. Through customer data, banks have kept track of their numerous accounts, assess credit risk, and issue out IOUs of the past -- which eventually became the dollars and cents we use today

A bank's success hinges heavily on how well they know its customers and how they act based on that information

However, the banking industry has also long battled against unscrupulous players exploiting weaknesses within the data-gathering process - such as identity fraud, forgeries, duplicate accounts, and others.

Medical institutions, telecommunication providers and government agencies have long struggled with these exploiters, and have thus relied on Know Your Customer (KYC) processes to verify customer identities

WISE AI™

WISE LIVENESS

As with any authentication solution, there will be fraudsters looking for ways to circumvent the security and verification system. WISE LIVENESS is a system that is able to detect impersonation attempts, be it a photo, or videos of facial mask spoofing methods

WISE LIVENESS uses state-of-the-art deep learning and convolutional neural networks, enabling liveness detection to be conducted passively

Passive liveness system requires the users to take selfie photos without the need to perform any action. This provides a simple and easy user experience, and less friction for the user side to get onboarded during the process

This is in contrast with active liveness detection, which requires users to blink, tilt or shake their heads according to on-screen instructions

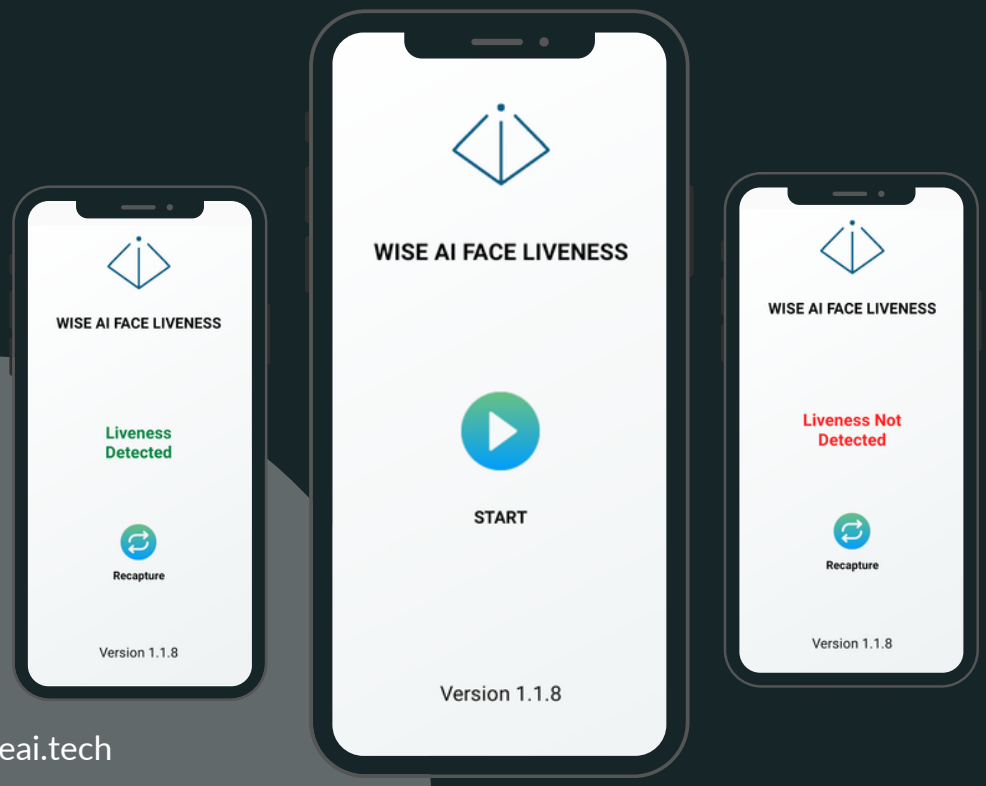
www.wiseai.tech

Mitigate Spoof Attacks

In order to bypass any liveness detection methods, you need to be equipped with resources. Most liveness detection systems are either active or passive systems that is able to reject some spoof cases

The table on the right shows popular spoofing attacks that an attacker might use to bypass the system

Attack	How to create it?	How to prevent it?
Print Attacks (any material)	Stolen personal documents or printed selfie photos	Liveness check or compare selfie with document
Replay Attacks (image or video)	Recording of a persons identity or selfie video	Active Liveness Detection to enable user participation
Face Mask	Purchase of any face mask or surgical mask	Human texture analysis and Passive Liveness Model trained to detect face masks



Example of WISE LIVENESS on mobile

WISE AI™

Model Training

The model is trained with more than a million images consisting of live and spoof facial images and validated on unseen samples. The training data is cleaned before being fed into the neural network to ensure that there is a visible face in every image and no occlusion or distortion in the face region.

The training data comes from different data sources to improve the generalizability of the trained model. In specifically our training data covers the most popular devices, different factors for face attributes such as skin colors and age, different lighting conditions such as indoor and outdoor. We constantly increase the training data and unseen samples to improve our model

In recent study, synthetic face data generate by GAN could be added to the training – this reduces the effort required to collect the data from multiple sources

WISE AI™

About Us

WISE AI, Known As The FACE OF ASEAN By Our Partners, Is Recognized As The Preferred Digital Identity Enabler In Southeast Asia Due To Our Laser Focus On Analyzing Southeast Asian Faces. WISE AI Has Developed The Industry's Leading Electronic Know-Your-Customer (EKYC), And Digital Identity Solutions That Help Enterprise Shortens The Customer Onboarding Process By Up To 95%.

Want to collaborate? Contact us.

www.wiseai.tech
sales.ekyc@wiseai.tech
+603-2770 0302