Trust Stamp

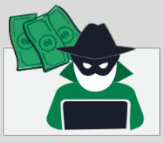
En colaboración con CWAG y la Alianza Estatal, Trust Stamp ha desarrollado un modelo de punta que opera entre los Procuradores Generales del Estado de Nuevo México, EE.UU. y el Estado de Guanajuato en México.

Este proyecto usa las **Coincidencias Faciales** de Trust Stamp y sus **Sistemas de Hashing**, para crear un medio por el cual ambas procuradurías generales puedan compartir hashes vinculados con víctimas del tráfico de personas. El mecanismo permite notificar a los investigadores de un "cotejo" sin las complicaciones que significa compartir información personalmente identificable. Este sistema de uso de hashes ha resuelto un problema de larga duración para las operaciones de las fuerzas del orden público con respecto a compartir datos inter-jurisdiccionales. Antes se requería obtener órdenes judiciales para compartir cualquier información, lo cual muchas veces causaba demoras o la necesidad de legislación específica en ciertas jurisdicciones. Al usar el hash biométrico, no se comparte información personal, y se conserva la privacidad y los protocolos relacionados con la seguridad de datos a través de las jurisdicciones. Éste es un modelo revolucionario, y el Procurador General del Estado de Nuevo México comparte esta opinión.

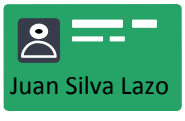
La tecnología fue anunciada por el General Balderas en la conferencia internacional del Instituto Biométrico en Nueva York en junio de 2018.

El enfoque principal de Trust Stamp ha sido desarrollar sistemas de autenticación de identidades, potenciados por la inteligencia artificial (IA) y enfocados en la biométrica facial.

Los gastos dedicados por Trust Stamp a la investigación y desarrollo se basan en la doble tesis que en los próximos 5 años la biométrica facial se transformará en la metodología dominante de autenticación para transacciones en línea y que, a medida que aumenta su uso, aumentará a la par la inversión ilícita en ataques contra estas metodologías.



En respuesta, han desarrollado y patentado múltiples enfoques de IA para identificar y defenderse contra ataques de presentación de imágenes fijas y videos. Una vez que han comprobado una imagen facial viva y no adulterada, usan los siguientes medios para conectar una identidad legal con un hash biométrico :



El análisis forense de escaneos de documentos de identidad emitidos por gobiernos.

Minado de datos de medios sociales.

Otros recursos en línea y de propiedad.

En forma paralela, Trust Stamp también ha patentado un hash biométrico permanente y encriptado que puede basarse en un **servidor** o en un **blockchain**, y funcionar como un ADN digital para la persona. El hash actualmente se produce de una fotografía fija o un video, extrapolando las medidas a partir de una máscara virtual en 3D creada por el software, pero puede evolucionar a través del tiempo y puede basarse, quedar incorporado, y/o ser punto de pivote con respecto a múltiples factores biométricos y otros datos individuales. Como hash, el dato jamás puede someterse a ingeniería de reversa, y no se considera información personalmente identificable con respecto a los EE.UU. y Reglamentos Generales de Protección de Datos (GDPR).

Un importante factor que distingue las metodologías de Trust Stamp es el hecho que su proceso de patentado de hashing les permite comparar cada hash biométrico nuevo con cada otro hash que hayan visto previamente, y su IA de propiedad calcula las probabilidades de que dos hashes hayan sido generados a partir del mismo rostro humano. A pesar de que los procedimientos KYC (conocer al cliente), tradicionalmente segregados, muchas veces "aceptan" identidades sintéticas y robadas, asociadas a documentos de crédito y de identidad, este proceso ha identificado numerosas identidades sintéticas (y falsificadores con múltiples identidades), y existe menos de una probabilidad entre mil millones de que el cotejo del hash coincida con más de un rostro.

Durante una segunda implementación en agosto, Trust Stamp incorporará personal en cada una de las oficinas de las Procuradurías en sistemas de comunicaciones biométricamente encriptadas, para permitirles intercambiar mensajes encriptados y archivos que sólo pueden desencriptarse con datos biométricos faciales en vivo de un usuario autorizado. El sistema no usa llaves privadas, nombres de usuarios o contraseñas, así eliminando oportunidades para el uso indebido.