أكاديمية طويق
Tuwaiq Academy

هاكاثون
أبشر طويق

SAFEFACE

EYES ON SAFETY

أعضاء الفريق

ديمه الصيني

لمار براشي

ساره باحشوان

المحتويات

01 المشكلة

02 الحل

03 البيانات المستخدمة

04 التقنيات المستخدمة

05 وصف الفكرة

06 توفير البيانات

07 العرض التوضيحى

08 التحديات والخطط المستقبلية

المشكلة

تعتمد الأنظمة الأمنية الحالية بشكل كبير على الملاحظة البشرية وأساليب المراقبة التقليدية، والتي قد تفشل في اكتشاف العلامات السلوكية الدقيقة للتوتر أو الإكراه أو النوايا المشبوهة. وفي البيئات عالية الخطورة مثل مراكز الخدمات الحكومية ونقاط التفتيش، قد تؤدي هذه المحدودية إلى تأخير الاستجابة وزيادة التهديدات الأمنية.

الحل

SafeFace هو نظام مدعوم بالذكاء الاصطناعي يقوم بتحليل تعابير الوجه الدقيقة بشكل فوري لاكتشاف مستويات التوتر غير الطبيعية والسلوك المريب. يوفّر تنبيهات فورية لرجال الأمن مع الحفاظ على خصوصية المستخدم من خلال عدم تخزين الصور. يساهم هذا النهج الاستباقي في دعم التدخل المبكر وتعزيز السلامة العامة.

البيانات المستخدمة

- الكشف الفوري لنقاط الوجه (Real-time Facial Landmark Detection)
- محرّك تحليل تعابير الوجه الدقيقة (Micro-Expression Analysis Engine)
- خوارزمية تقييم مستوى الخطورة (Risk Scoring Algorithm)
- نظام التنبيهات والإشعارات الأمنية
- واجهة لوحة تحكم أمنية تفاعلية (Security Dashboard)
- وحدة حماية الخصوصية مع عدم تخزين أي بيانات أو صور

Expected Returns:

تعزيز الوعي الظرفي وتحسين القدرة على اتخاذ القرار

تسريع زمن الاستجابة للحالات الأمنية

تقليل عمليات انتحال الهوية

التقنيات المستخدمة

Python & TensorFlow / PyTorch
لتدريب نماذج الذكاء الاصطناعي وتحليل السلوك

MediaPipe Face Mesh
تقنية لاستخراج نقاط الوجه الدقيقة وتحليل تعابير الوجه بشكل فوري

FastAPI Backend
لربط النظام ومعالجة البيانات بشكل آمن وسريع

React Frontend Dashboard
لتصميم واجهة لوحة التحكم الأمنية التفاعلية

WebSocket for real-time alerts
لإرسال التنبيهات اللحظية في الوقت الحقيقي

ONNX/TFLite for optimized deployment
لنشر النموذج وتحسين الأداء وتقليل زمن الاستجابة

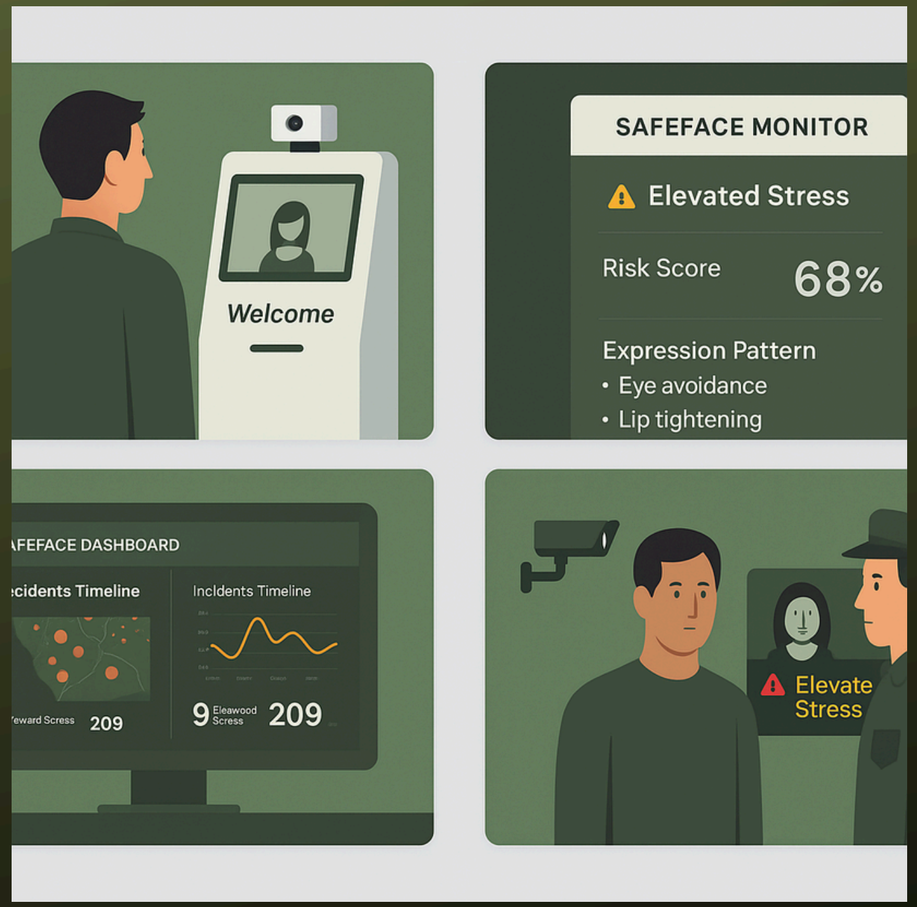
Infrastructure: البنية التحتية

الحوسبة الطرفية (Edge Computing)
لضمان أداء لحظي عالي

تكامل مع الشبكة الحكومية الآمنة

معالجة سحابية للذكاء الاصطناعي

وصف الفكرة



SafeFace هو نظام أمني مدعوم بالذكاء الاصطناعي يقوم بتحليل تعابير الوجه الدقيقة (Micro-Expressions) في الوقت الحقيقي، بهدف اكتشاف حالات التوتر غير الطبيعي والسلوكيات المريبة التي قد تشير إلى خطر محتمل أو محاولة إخفاء نية معينة.

يعتمد SafeFace على تتبّع نقاط الوجه وتحليل الأنماط الدقيقة للحركات الانفعالية التي يصعب ملاحظتها بالعين البشرية. يقوم النظام بتحويل هذه الإشارات إلى درجة خطورة (Risk Score)، ويرسل تنبيهًا فوريًا لرجال الأمن دون أن يشعر المستخدم أو يتأثر بتجربته.

يتميّز SafeFace بأنه يحافظ على الخصوصية بالكامل، حيث يتم تحليل الصورة لحظيًا دون تخزين أي بيانات شخصية أو صور للمستخدمين. يهدف النظام إلى دعم الجهات الأمنية في اتخاذ قرارات أسرع وأكثر دقة، وتقليل حالات انتحال الهوية، وتعزيز السلامة داخل مراكز الخدمات الحكومية ونقاط التفتيش.

مواءمة الفكرة :

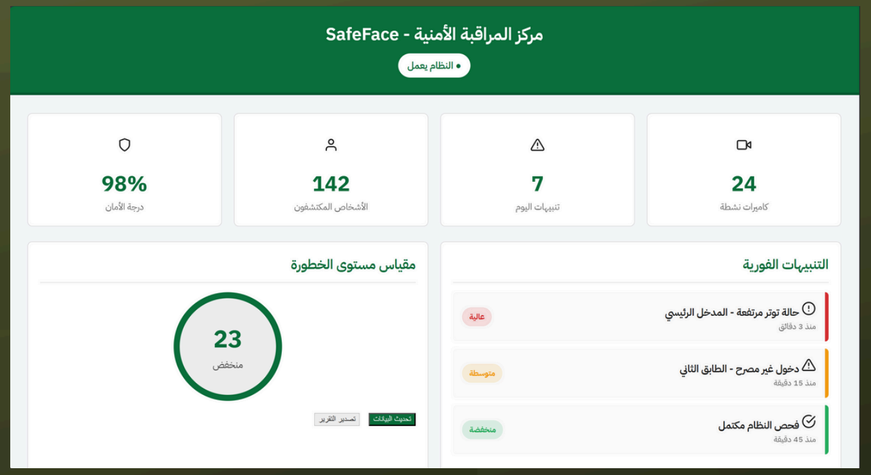
تتوافق فكرة SafeFace مع أهداف هاكاثون أبشر من خلال تقديم حل تقني مبتكر يُسهم في تعزيز المنظومة الأمنية عبر استخدام تقنيات الذكاء الاصطناعي في تحليل السلوك البشري بشكل آني، بما يرفع من كفاءة الإجراءات الأمنية ويُسهم في دعم الخدمات الحكومية الرقمية بصورة استباقية وفعّالة.

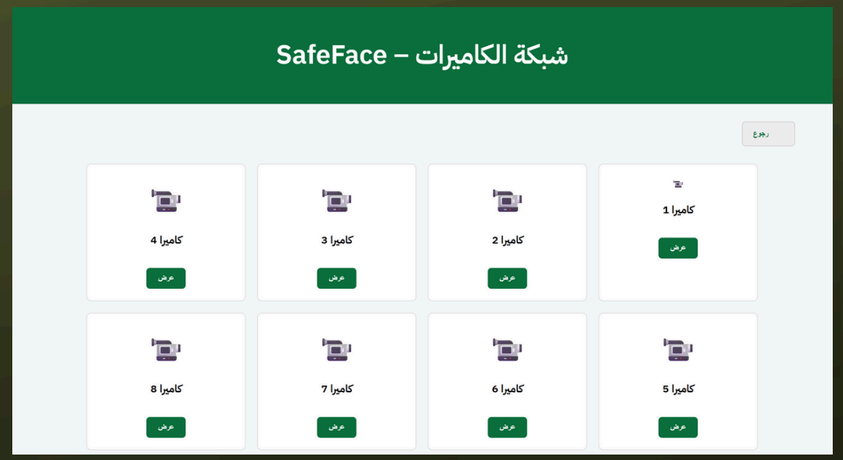
كما تنسجم الفكرة بصورة مباشرة مع رؤية المملكة 2030 التي تولي اهتمامًا كبيرًا بتطوير البنية التحتية الرقمية واعتماد حلول الذكاء الاصطناعي في القطاعين الأمني والحكومي. ويعزز SafeFace أهداف الرؤية في:

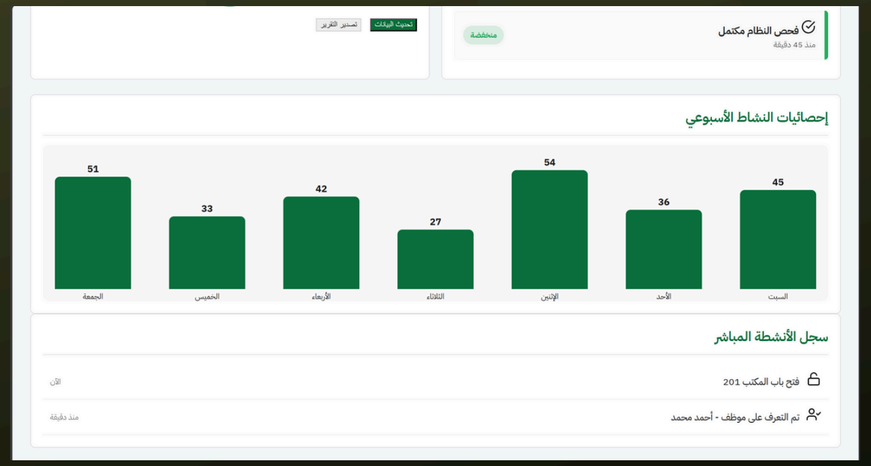
- رفع مستوى الأمان الوطني
- تحسين جودة الخدمات المقدمة للمواطنين والمقيمين
- تمكين التحول الرقمي
- دعم اتخاذ القرار عبر أنظمة ذكية دقيقة وموثوقة

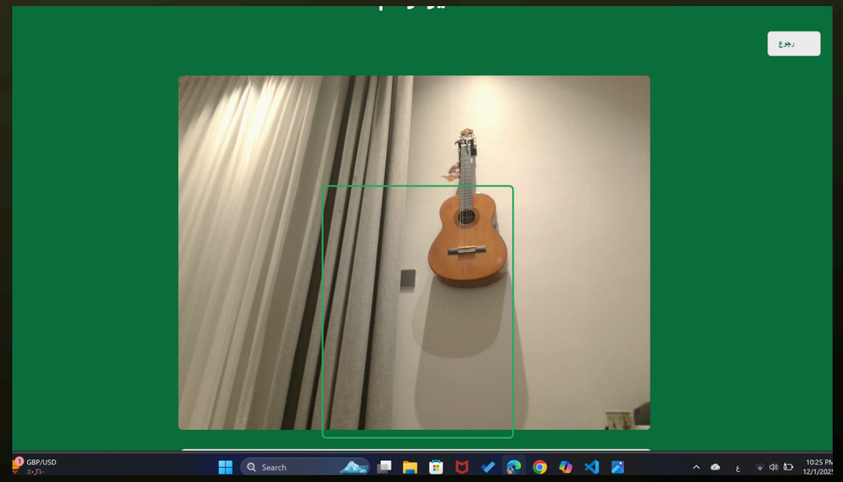
ويمثل SafeFace نموذجًا عمليًا لتبني تقنيات متقدمة تسهم في تطوير الخدمات الأمنية والحكومية وفق أعلى معايير الكفاءة والخصوصية.

العرض التوضيحي:









التحديات والخطط المستقبلية

التحديات:

- ضبط النموذج وتقليل الانحياز: يتطلّب النظام معالجة دقيقة لتجنّب أي تحيّز في تحليل السلوك.
- أداء النظام في الزمن الحقيقي: ضمان سرعة تحليل عالية دون التأثير على تجربة المستخدم أو عمل الأنظمة الأمنية.
- التكامل مع الأنظمة الحكومية: يحتاج النظام إلى توافق تقني وأمني مع منظومة أبشر والجهات ذات العلاقة.
- الاعتبارات الأخلاقية والخصوصية: الحفاظ على خصوصية الأفراد وعدم تخزين البيانات هو تحدٍّ يستلزم التزامًا صارمًا بالمعايير.

ما تحتاج إلى المساعدة فيه:

- إتاحة واجهات برمجية (APIs) وبيئات اختبار لتجربة التكامل مع أنظمة أبشر أو الجهات الأمنية ذات العلاقة.
- إرشاد فني من خبراء الأمن السيبراني والذكاء الاصطناعي لضمان الامتثال للمعايير الحكومية.

العمل المستقبلي:

العمل المستقبلي يركّز خلال الأسبوعين القادمين على تحسين دقة نموذج تحليل تعابير الوجه وتطوير خوارزمية تقييم مستوى الخطورة، إضافة إلى استكمال بناء لوحة التحكم وربط النموذج بنظام تنبيهات لحظي لضمان الجاهزية التشغيلية. وبعد ذلك سيتم العمل على استكمال 70% من المشروع من خلال تعزيز حماية الخصوصية، ودعم الحوسبة الطرفية، وتجهيز نسخة تجريبية قابلة للتكامل مع منصة أبشر والأنظمة الحكومية، وصولًا إلى نسخة شبه نهائية جاهزة للاختبار الميداني.

Timeline

المرحلة 1
الأسبوع الحالي

- إنجاز رسم الواجهات الأساسية وتصميم النموذج الأولي للواجهة (Prototype).
- بناء نسخة اختبارية بسيطة لواجهة المستخدم لإظهار الفكرة بصريًا.

المرحلة 2
الأسبوع المقبل

- تطوير النموذج التجريبي لتحليل تعابير الوجه الدقيقة باستخدام بيانات مفتوحة.
- تحسين التعرف على نقاط الوجه (Landmarks) وتجهيز بيئة الاختبار.

المرحلة 3
الأسبوع الثاني و الثالث

- إربط النموذج المبدئي مع الواجهة التجريبية (Integration MVP).
- تفعيل نظام التنبيهات اللحظي (Real-time Alerts).
- إجراء اختبارات مبسطة على سيناريوهات توتر وسلوك طبيعي

المرحلة 4
الأسبوع الرابع

- إعداد نسخة أولية جاهزة للعرض (Functional MVP).
- تجهيز Dashboard مبسطة لعرض نتائج النظام.
- تجهيز خطة التكامل الأولي مع منصّة أبشر.

العمل المستقبلي يهدف إلى تحسين دقة النموذج ورفع كفاءته في تحليل تعابير الوجه، وربط النظام بالكامل بالواجهة التجريبية مع تفعيل التنبيهات اللحظية. كما سيتم تعزيز الخصوصية ودعم الحوسبة الطرفية، ثم تجهيز نسخة تجريبية قابلة للتكامل مع منصة أبشر لإجراء الاختبارات الميدانية قبل التوسع في التطبيق.

Thank you

أكاديمية طويق
Tuwaiq Academy