Naif Arab University for Security Sciences
Arab Journal for Security Studies
المجلة العربية للدراسات الأمنية
https://journals.nauss.edu.sa/index.php/ajss
AJSS

Integrating Digital Fingerprinting and Artificial Intelligence: Modern Mechanisms for Analyzing Crime Scenes and Improving Digital Forensics Evidence

التكامل بين البصمة الرقمية والذكاء الاصطناعي: آليات حديثة لتحليل مسرح الجريمة وتحسين الأدلة الجنائية الرقمية

عمار ياسر زهير البابلي
أكاديمية الشرطة المصرية، جمهورية مصر العربية

Ammar Yasser Zuhair Al-Babli
Egyptian Police Academy, Arab Republic of Egypt

Received 03 Mar. 2025; accepted 29 Jul. 2025; available online 9 Dec. 2025

Abstract

This study examines the analysis of the digital fingerprint using artificial intelligence as one of the effective technological pillars for keeping pace with contemporary security challenges, analyzing the crime scene, and identifying forensic evidence, particularly in light of the rise of cybercrimes and their complexities, such as electronic intrusions, financial fraud, and identity theft. It highlights how the digital fingerprint—represented in unique data such as the IP address, digital device fingerprints, and browser logs—contributes to tracking unlawful activities and accurately identifying offenders, in addition to messages and digital evidence stored on various digital devices at the crime scene, whether purely forensic or digitally associated. This, in turn, enhances the efficiency of criminal investigations and accelerates judicial procedures by providing digital evidence admissible for judicial proof.

The study sheds light on the role of artificial intelligence in developing mechanisms for integrating digital fingerprints with biometric fingerprints (such as biological and voice prints), which enhances the accuracy of digital evidence analysis and strengthens the ability to detect complex

Keywords: *security studies, artificial intelligence, digital fingerprint, biometric fingerprint, forensic evidence, crime scene, criminal investigation*

المستخلص

تناولت هذه الدراسة تحليل البصمة الرقمية بالذكاء الاصطناعى كإحدى الركائز التكنولوجية الفاعلة في مواكبة التحديات الأمنية المعاصرة، وتحليل مسرح الجريمة والوقوف على الأدلة الجنائية، خاصة في ظل تنامي الجرائم السيبرانية وتعقيداتها، مثل: الاختراقات الإلكترونية والاحتيال المالي وانتحال الهوية، وتُبرز الدراسة كيف تُسهم البصمة الرقمية المتمثلة في بيانات فريدة كعنوان الIP وبصمات الأجهزة الرقمية وسجلات المتصفح في تعقب الأنشطة غير المشروعة، وتحديد هوية الجناة بدقة بخلاف الرسائل والأدلة الرقمية المسجلة على الأجهزة الرقمية المتعددة بمسرح الجريمة على حد سواء الجنائي والمقترن بالرقمي؛ مما يُعزز كفاءة التحقيقات الجنائية، ويُسرع إجراءات المحاكمة عبر تقديم أدلة رقمية قابلة للاستخدام في الإثبات القضائي.

وتُسلط الدراسة الضوء على دور الذكاء الاصطناعي في تطوير آليات تكامل البصمة الرقمية مع البصمات البيومترية (كالبصمة الحيوية والصوتية)، مما يُحسّن دقة تحليل الأدلة الرقمية، ويُعزز القدرة على رصد الأنماط الإجرامية المعقدة، مثل: تمويل الإرهاب

الكلمات المفتاحية: الدراسات الأمنية، الذكاء الاصطناعي، البصمة الرقمية، البصمة البيومترية، الأدلة الجنائية، مسرح الجريمة، التحقيق الجنائي

* Corresponding Author: *Ammar Yasser Zuhair Al-Babli*
Email: 3marelbably@gmail.com

doi: 10.26735/HDRW6833

أو الجرائم المالية المنظمة، كما تُناقش الإشكاليات القانونية المتعلقة بمشروعية استخدام هذه الأدلة في المحاكم، مع ضرورة تطوير أطر تشريعية تواكب التطور التكنولوجي وتضمن حقوق الأفراد في الخصوصية وتعتمد الدراسة على منهج وصفي لتحليل المفاهيم الأساسية وتقنيات البصمة الرقمية وتُوصي بضرورة تعزيز التعاون بين الدول لمواجهة الجرائم العابرة للحدود، وتبني سياسات أمنية متكاملة تدعم توثيق الأدلة الرقمية وحمايتها من التلاعب، إلى جانب تدريب الكوادر الأمنية والقضائية على استخدام الأدوات التكنولوجية المتقدمة.

criminal patterns, such as the financing of terrorism or organized financial crimes. It also discusses the legal issues related to the legitimacy of using such evidence in courts, emphasizing the necessity of developing legislative frameworks that keep pace with technological advancement and ensure individuals' rights to privacy.

The study relies on a descriptive approach to analyze fundamental concepts and digital fingerprint technologies. It recommends strengthening cooperation among states to confront transnational crimes, adopting integrated security policies that support the documentation of digital evidence and protect it from tampering, in addition to training security and judicial personnel on the use of advanced technological tools.

1. المقدمة

البصمة الرقمية بما تحويه من بيانات متعلقة بأنماط التصفح، وتفاعلات الحسابات، والاتصالات ذات الطابع المشفّر، والإحداثيات الافتراضية قد غدت بمثابة «دلائل معاصرة» في فضاء الجريمة، غير أن الأهمية الحقيقية لهذه البيانات لا تكمن في وجودها المجرد، بل في القدرة على تحليلها بعمق وربطها بشكل دقيق بالفاعل، وهو ما يستدعي أدوات تحليلية تتجاوز أطر العمل التقليدية، وهنا يظهر الذكاء الاصطناعي بقدراته غير المسبوقة في استيعاب ومعالجة الكم الهائل والمتنوع من البيانات، واكتشاف الترابطات المستترة، واستبصار الأنماط السلوكية المتكررة ضمن السياق الرقمي (Guo, et al. 2024).

ومن الجدير بالذكر أن الذكاء الاصطناعي يشكّل دعامة مركزية في تحليل البصمة الجنائية الرقمية، وهي تلك الآثار الفريدة والبيانات التي تُخلفها الأجهزة أو التطبيقات أو المستخدمون أثناء تفاعلهم مع البيئة الرقمية؛ إذ تُتيح قدرته الفائقة على معالجة الكم الهائل والمتشعّب من هذه البيانات، بسرعة ودقة غير مسبوقتين باستخدام تقنيات متقدمة؛ مثل: التعلم الآلي والتعلم العميق والخوارزميات؛ مما يتيح كشف الأنماط الخفية وغير القانونية، ورصد الشذوذ في السلوك الرقمي والجنائي، كذلك يُؤدي دورًا حاسمًا في مواجهة التزييف والهجمات الإلكترونية المعقدة من خلال التعرف على أدق التناقضات في البصمات الرقمية أو البيومترية، مُحدثًا بذلك ثورة في ميادين الأمن السيبراني والتحقيقات الرقمية؛ حيث يُعزز الكفاءات التحليلية لتُصبح أكثر سرعة، وعمقًا، واستباقية؛ مما يُفضي إلى الكشف المبكر عن التهديدات المتطورة، والتصدي لها بفاعليّة، وبناء بيئة رقمية أكثر أمنًا وموثوقية للجميع.

وعلى سبيل المثال، في إحدى قضايا الابتزاز الإلكتروني الدولي استطاع النظام الذكي تتبع بصمة رقمية مخفية مرتبطة بعنوان IP مشفر، ثم ربطه ببيانات جغرافية والإحداثيات الرقمية، وانتهى بكشف هوية الجاني وتحديد موقعه الفعلي رغم محاولات التمويه، كما أن تطبيقات الذكاء الاصطناعي؛ مثل: أنظمة التعرف على الوجه، وتحليل نمط الكتابة، والتقاط الكلمات المفتاحية التهديدية، وقد أسهمت في رفع جودة الأدلة الجنائية الرقمية وجعلها أكثر قبولًا أمام جهات التحقيق والقضاء، لكونها مدعومة بتحليل علمي متكامل، ولم يعد الاعتماد على مجرد وجود البصمة الرقمية كافيًا، بل أصبحت قدرتها على الصمود أمام التدقيق القانوني رهينة بتحليلها الذكي وربطها بسياق جنائي متكامل (Astrobotic's, 2025).

أهمية الدراسة

تكمن أهمية الدراسة فيما يأتي:

- على المستويين النظري والتطبيقي؛ إذ تُثري من الناحية النظرية المعرفة العلمية المتعلقة بتقنيات الذكاء الاصطناعي وتوظيفها ضمن مجالي الأمن السيبراني والتحقيق الجنائي وتحليل الأدلة الرقمية، عبر تسليط الضوء على الأسس النظرية الكامنة وراء خوارزميات التعلم الآلي وتحليل البيانات الضخمة، وما يرتبط بها من فهم وتحليل البصمة الرقمية والبيومترية.
- دراسة مفهوم البصمة الرقمية وأهميتها في التحقيقات الجنائية باعتبارها أداة حديثة وفعَّالة في التحقيقات الجنائية؛ حيث تُسهم في تحديد هوية الأفراد وتتبع أنشطتهم الإلكترونية، وتشمل البصمة الرقمية مجموعة من البيانات الفريدة التي تُترك عند استخدام الأجهزة الإلكترونية أو الإنترنت، مثل: عناوينIP، وملفات تعريف الارتباط (Cookies)، وسجلات المتصفح، وبصمات الجهاز.

مشكلة الدراسة

مع التحول الرقمي المتزايد، بات العنصر الرقمي حاضرًا في معظم الجرائم، سواء من خلال استخدام الوسائل الرقمية في ارتكاب الجريمة وإخفاء أو تدمير الأدلة الرقمية بالأجهزة المتواجدة بمسرح الجريمة؛ مما يؤدي إلى طمس البصمات الجنائية الخاصة بالجريمة، أو الجاني، أو المجنى عليه.

ومع ذلك، يواجه توظيف البصمة الرقمية في التحقيقات عدة معوقات تقنية وفنية، من بينها محدودية موثوقية بعض أنواع البيانات الرقمية، وصعوبة التحقق من هوية الجناة؛ نتيجة للجوء إلى تقنيات الإخفاء والتلاعب الرقمي، بالإضافة إلى نقص التقنيات المتقدمة، وغياب الأطر التشريعية الواضحة التي تُنظّم حجية الأدلة الرقمية في بعض الأنظمة القضائية، كذلك وجود اعتراضات قضائية على مشروعية الأدلة المستخلصة بالتقنيات الحديثة؛ مما يثير إشكالية قبولها كوسائل إثبات أمام القضاء الجنائي.

أهداف الدراسة

- توضيح مفهوم البصمة الرقمية وأهميتها في العصر الرقمي، وتحليل ماهية الجرائم السيبرانية وخصائص مسرح الجريمة الرقمي.
- دراسة التطبيقات الأمنية للذكاء الاصطناعي في تعزيز التحقيقات الجنائية وتحليل دور الذكاء الاصطناعي في تكامل البصمات البيومترية والرقمية لتحسين التحريات.
- تقييم استخدام الذكاء الاصطناعي في فحص الأدلة الجنائية الرقمية وعمليات المضاهاة.
- التعرف على أهمية البصمة الرقمية والبيومترية كأدلة في الإثبات الجنائي وتحليل دور البصمة الرقمية في تقديم أدلة دقيقة وموثوقة في المحاكم مع الأمثلة الحقيقية لقضايا مماثلة.

تساؤلات الدراسة

- ما إسهامات البصمة الرقمية والبيومترية في تعزيز التحقيقات الجنائية ومكافحة الجريمة السيبراني والتعرف على ماهية وأنواع البصمات الجنائية والرقمية.
- ما التطبيقات الأمنية المستخدمة من خلال الذكاء الاصطناعى لتتبع الأدلة الرقمية الجنائية، سواء الإجرامى أو الإرهابى؟ وما إسهامات البصمة الرقمية في تحسين كفاءة التحقيقات الجنائية؟

منهج الدراسة

- **المنهج الوصفي:** لتحليل مفهوم البصمة الرقمية وتقنياتها.
- **المنهج التحليلي:** لدراسة حالات واقعية لاستخدام البصمة الرقمية في التحقيقات الجنائية.

2. المبحث الأول: مفهوم البصمة الرقمية والبيومترية وتوظيفها الأمني

تأتى العلاقة بين البصمة الرقمية وهي الآثار الفريدة التي يتركها المستخدم في الفضاء الرقمي كعناوين الIP وسجلات الأجهزة وأنماط السلوك ومسرح الجريمة الرقمي (البيئة التي تحدث فيها الجريمة الإلكترونية؛ مثل: الخوادم أو الحسابات المخترقة) علاقة تكاملية؛ حيث تُعد البصمة الرقمية الأدلةَ الرئيسة التي يتم استخراجها من مسرح الجريمة لتحديد هوية الجاني وطريقة ارتكاب الفعل الإجرامي، من خلال تحليل بيانات مثل: سجلات الوصول أو الرسائل المشفرة أو البرمجيات الخبيثة، ويعتمد التحقيق الجنائي الرقمي على ربط هذه البصمات بالجهات أو الأفراد عبر أدوات مثل: التحليل الزمني أو مطابقة الأنماط، لكنه يواجه تحديات مثل: استخدام المجرمين أدوات إخفاء الهوية كـ(VPN) أو تشتت الأدلة عبر مساحات رقمية واسعة؛ مما يجعل جمع البصمات وتحليلها عملية معقدة تتطلب تقنيات متطورة لضمان فاعلية التحقيقات في كشف الجرائم الإلكترونية كالاختراقات أو التصيد الاحتيالي (Biswas, S, 2024).

2. 1. المطلب الأول: أهمية البصمة الرقمية والبيومترية

تعريف البصمة البيومترية

البصمة البيومترية هي تقنية تعتمد على استخدام الخصائص الحيوية أو السلوكية الفريدة لكل إنسان، مثل: بصمات الأصابع، ملامح الوجه، قزحية العين، الصوت، أو طريقة التوقيع والحركة، بهدف التحقق من الهوية أو التعرف على الأفراد بدقة وأمان، وتتميز هذه التقنية بصعوبة التزوير وسهولة الاستخدام؛ حيث تُستخدم في العديد من المجالات مثل: الهواتف الذكية، وأنظمة الحضور والانصراف، والمطارات، والخدمات الحكومية، وتُعد البصمة البيومترية وسيلة فعَّالة لتحقيق الأمان الرقمي وتقليل الاعتماد على كلمات المرور أو البطاقات التقليدية، رغم ما تثيره من تحديات تتعلق بالخصوصية وحماية البيانات (فتح الله، 2021).

وتُعدُّ البصمة البيومترية أداة محورية في التحقيقات الجنائية الحديثة؛ حيث تُستخدم لتحديد هوية المشتبه بهم أو الضحايا بدقة عالية، من خلال مقارنة الخصائص البيولوجية، مثل: بصمات الأصابع أو بصمة الوجه أو قزحية العين مع قواعد البيانات الجنائية. وتُسهم هذه

التقنية في ربط الأشخاص بمسرح الجريمة من خلال الآثار البيومترية التي يُمكن أن يتركها الجاني، مثل: بصمات على الأسطح أو تسجيلات كاميرات تستخدم التعرف على الوجوه، كما تُستخدم في مراقبة وتتبع المتهمين، والتحقق من الهوية أثناء التوقيف أو في السجون؛ مما يعزز من دقة الإجراءات العدلية ويُسرّع الوصول إلى الحقيقة.

تعريف البصمة الإلكترونية (الرقمية)

البيانات الهائلة التي يوفرها المستخدمون تشكل ما يعرف بالبصمة الرقمية، وهي كل السجلات والآثار والأنشطة التي يتركها مستخدم الإنترنت، مثل: المشاركات والصور والتدوينات وسجل دخول المواقع، واستقبال رسائل بالبريد الإلكتروني والبحث من خلال محركات الإنترنت؛ حيث تسجل بصمة رقمية لكل مستخدم مختلفة عن الآخر، وهي تتشكل كلما تم استخدام الإنترنت، وتحتوي على كل ما ينشر من تعليقات وأخبار وآراء وصور، وفيديوهات وكل ما يكتب ويسجل على لوحة مفاتيح الحاسب الآلي، وهي تُعبر عن أثر الأنشطة التي تتم على الإنترنت، والتي يصعب التخلص منها (الغثبر، 2024).

والبصمة الرقمية (Digital Footprint) هي مجموعة البيانات والأنشطة والسلوكيات والتفاعلات الخاصة بشخص ما التي يتم تسجيلها في البيئة الرقمية، فكل ما يتم على الهاتف الذكي أو اللوحي عبر الإنترنت أو يتم مشاهدته أو البحث عنه أو يتم تحميلة أو رفعه من الإنترنت داخل أوعية المعلومات بالأنظمة الإلكترونية المختلفة، ويتم تسجيله وتحليله، وفي كثير من الأحيان يصعب حذفه.

البصمة الرقمية كدليل جنائي

تُعدُّ البصمة الرقمية أداةً حاسمة في البحث الجنائي الحديث؛ حيث تُسهم في كشف الجرائم الإلكترونية والتقليدية على حد سواء. وتشمل البصمة الرقمية الآثار التي يتركها الأفراد أثناء استخدامهم للإنترنت أو الأجهزة الذكية، مثل: عناوينIP، وبيانات الموقع الجغرافي، وسجلات البحث، وأنماط السلوك الرقمي، وفي البحث الجنائي، تُستخدم هذه البيانات لتتبع هويات المشتبه بهم، وتحليل تحركاتهم، والكشف عن مصادر الهجمات الإلكترونية، وتعزيز الأدلة في المحاكم. على سبيل المثال، يمكن تحليل رسائل البريد الإلكتروني أو سجلات الهواتف الذكية لإثبات تورط شخص ما في جريمة (قاسم، 2024).

وتطوير الإثبات الجنائي يُعد ركيزة أساسية في تعزيز النظم الجنائية والأمنية لمكافحة الجرائم السيبرانية، وتحقيق العدالة الناجزة، ومع تزايد تعقيد الجرائم الإلكترونية، أصبحت الحاجة ملحة لاعتماد أدلة رقمية متطورة مثل: البصمات الرقمية والبيومترية، وتحليل البيانات الضخمة، وتقنيات الذكاء الاصطناعي، وهذه الأدوات تُسهم في تسريع التحقيقات، وتحسين دقة الأدلة، وتحديد هوية الجناة بفاعليَّة أكبر (السبكي، 2024).

ويرى الباحث أن البصمة الرقمية تتميز بقدرتها على تقديم معلومات دقيقة عن الزمان والمكان وسلوك المستخدم؛ مما يجعلها دليلًا قويًّا في الإثبات أو النفي أمام الجهات القضائية.

أهمية البصمة الرقمية والبيومترية واستخدامها كدليل جنائي

تُعدُّ كل من البصمة الرقمية والبصمة البيومترية من الأدوات الجوهرية ضمن منظومة التحقيقات الجنائية الحديثة، ولا سيما مع التصاعد المستمر في وتيرة الجرائم الإلكترونية والتطور التقني المتسارع في آليات تنفيذها، وتكمن العلاقة بين هذين النوعين من البصمات في طبيعتهما التكاملية، إذ تُتيح البصمة الرقمية إمكانية تتبع مسارات الجريمة في الفضاء الإلكتروني، بينما تُوفّر البصمة البيومترية الوسيلة الدقيقة وغير القابلة للطعن في إثبات هوية الجاني.

وفي مثال آخر يُجسّد بصورة أوضح التفاعل بين هذين النوعين، فقد تمكّنت السلطات البريطانية في عام 2018 من حل جريمة قتل، اعتمادًا على بصمة وجه تم التقاطها باستخدام تقنيات التعرف على الوجوه عبر كاميرات المراقبة، والتي تمت مطابقتها مع قواعد بيانات حكومية، وبالتوازي، استُخدمت البصمة الرقمية المأخوذة من هاتف المجني عليه، وسجلات الرسائل، لتحديد آخر تواصل معه؛ ما قاد إلى تحديد مكان المشتبه به واعتقاله (Wyzykowski & Jain, 2023).

وقد أدت كل من البصمات الرقمية والبيومترية دورًا محوريًّا في التعامل مع قضايا الإرهاب، كما في هجمات باريس في 13 نوفمبر 2015 وكانت سلسلة من الاعتداءات الإرهابية المنسقة التي نفذها مسلحون وانتحاريون من تنظيم داعش، واستهدفت مواقع متعددة في العاصمة الفرنسية، أبرزها مسرح باتاكلان ومحيط ملعب «ستاد دو فرانس» وعدة مقاهٍ ومطاعم، وأسفرت عن مقتل 130 شخصًا وإصابة المئات، حيث جرى تتبع الأجهزة الإلكترونية المستخدمة من قبل الجناة، وتحليل سجلات المواقع الجغرافية والاتصالات، في حين استُخدمت البصمات البيومترية لتأكيد هوياتهم بعد الوفاة، من خلال مطابقة البيانات مع قواعد أمنية أوروبية.

وأدت التقنيات الحديثة دورًا حاسمًا في كشف ملابسات الهجمات؛ حيث استخدم المحققون تحليل الهواتف المحمولة وسجلات الاتصالات لتحديد هوية المهاجمين وتتبع تحركاتهم، كما

استعانوا بالبيانات المستخرجة من الشبكات الاجتماعية وتطبيقات التواصل؛ مثل: Telegram وWhatsApp التي استُخدمت للتنسيق بين المنفذين، بالإضافة إلى مراجعة تسجيلات كاميرات المراقبة في المواقع المستهدفة ومحيطها؛ مما ساعد على رسم مسار تحركات المنفذين قبل وأثناء تنفيذ الهجمات وتحديد أماكن اختبائهم وشبكات الدعم التي تواصلوا معها.

2. 2. المطلب الثاني: التوظيف الأمني للبصمة الرقمية في تعقب الأنشطة الإجرامية والإرهابية

تُشكِّل البصمة الرقمية سلاحًا إستراتيجيًّا في مواجهة الجريمة المنظمة والإرهاب في العصر الرقمي؛ حيث تعتمد الحكومات والجهات الأمنية على تحليل الآثار الرقمية التي يتركها الأفراد والجماعات عبر أنشطتهم الإلكترونية، بدءًا من الاتصالات المشفرة على منصات؛ مثل: «تيليجرام» أو «سجنال»، ومرورًا بتحركاتهم على الشبكة المظلمة (Dark Web)، ووصولًا إلى استخدام العملات الرقمية في تمويل العمليات الإرهابية (عبد الجواد، 2023).

والبصمة الرقمية لم تعد مجرد أداة تكميلية، بل غدت عَصَب التحقيقات الجنائية، خاصةً في الجرائم التي تعتمد على التخطيط الذكي أو التعتيم المادي، فهي تُمكِّن المحققين من سد الثغرات في الأدلة التقليدية، وتحويل الهواتف والأجهزة الذكية إلى «شهود إلكترونيين» صامتين يُعيدون بناء تفاصيل الجريمة بدقةٍ مذهلة ومع ذلك، يظل التحدي الأكبر هو تحقيق التوازن بين مصلحة العدالة وحقوق الخصوصية، في عالمٍ تُهدد فيه التكنولوجيا باختراق الحميمية الإنسانية.

أهمية البصمة الرقمية في فحص مسرح الجريمة

أصبحت البصمة الرقمية أداةً حاسمةً في تحقيقات الجرائم التقليدية؛ حيث تُوفِّر أدلةً غير مسبوقة تربط الجناة بمسرح الجريمة، حتى في الحالات التي تبدو خاليةً من الأدلة المادية وفيما يلي تفصيل لدورها في أنواع الجرائم المختلفة كجرائم القتل؛ حيث تحديد تحركات الجاني من خلال تحليل بيانات الموقع الجغرافي (GPS) من الهواتف أو السيارات الذكية لإثبات وجود المشتبه به في مكان الجريمة وقت حدوثها، وتتبع سجلات المكالمات أو الرسائل النصية مع المجني عليه قبل الحادث لرصد تهديدات أو تخطيط سابق، والكشف عن الدوافع بفحص سجل البحث على الإنترنت (مثل: البحث عن طرق القتل، أو شراء أدوات مشبوهة) وتحليل محادثات تطبيقات المراسلة المشفرة (مثل: واتساب أو تيليجرام) لاكتشاف نوايا إجرامية.

في إحدى قضايا القتل في الولايات المتحدة (2022)، تم ربط الجاني بالجريمة عبر بيانات هاتف المجني عليه التي سجلت اتصالًا وثيقًا بهاتف المشتبه به قبل ساعات من الحادث، بالإضافة إلى صور التقطتها كاميرات مراقبة ذكية رُبطت ببيانات الموقع الجغرافي للهاتف (Alzahrani & et al. 2023) جرائم الاغتصاب والتحرش الجنسي بجمع أدلة رقمية واستعادة الصور أو الفيديوهات المحذوفة من أجهزة الجاني عبر تقنيات الطب الشرعي الرقمي وتحليل البيانات الوصفية (Metadata) للصور المُرسلة لإثبات وقت ومكان التقاطها، وتتبع الأنشطة الإلكترونية بكشف حسابات وهمية استُخدمت لاستدراج الضحايا على منصات المواعدة أو التواصل الاجتماعي.

وفي الهند (2021)، أدَّت بيانات الموقع الجغرافي من تطبيق أوبر إلى إدانة متهم بالاغتصاب، حيث أثبتت تواجده مع المجني عليه في مكان معزول وقت الحادث (Pfeuffer, 2019) ونتناول دراسة قضية ولاية دلهي ضد راجيش كومار (State of Delhi v. Rajesh Ku-mar2021) كالتالي:

بتاريخ 30 سبتمبر 2021، صدر بحق راجيش كومار (32 عامًا) حكمٌ بالسجن لمدة 20 عامًا دون إمكانية الإفراج المشروط، بالإضافة إلى غرامة مالية قدرها 400،000 روبية، وذلك استنادًا إلى المادة 376 من القانون الجنائي الهندي (§ 376 IPC)، والمادة 66E من قانون تكنولوجيا المعلومات (§ 66E IT Act)، عقب ثبوت قيامة بارتكاب جريمة اغتصاب بحق ضحية تبلغ من العمر 22 عامًا، حيث استُدرجت المجني عليها عبر حساب وهمي على تطبيق «تندر Tinder»، أنشأه المتهم من هوية مزيفة تحت اسم «أرون سينغ»، واستدرجها إلى مزرعة مهجورة في جنوب دلهي بتاريخ 15 يناير 2021 وقد بُنيت الإدانة على تكامل أدلة رقمية ذات طابع حاسم على النحو الآتي:

- بيانات تطبيق «أوبر»، أظهرت تواجد المتهم برفقة المجني عليها في الموقع المعزول خلال الفترة الزمنية الممتدة بين 20:30 و22:03 (لمدة 93 دقيقة).
- التحليل الجنائي الرقمي لهاتف المتهم (Samsung Gal-axy S20)، أتاح استرجاع 4 صور وفيديو محذوف، يظهر فيه المجني عليها فاقدة للوعي، وقد أكدت البيانات الوصفية (Metadata) تطابق توقيت التقاط الصور (21:17) وإحداثيات الموقع مع بيانات تطبيق «أوبر».
- تقرير وحدة الجرائم الإلكترونية (Cyber Cell)، الذي كشف عن تشغيل المتهم لثلاثة حسابات وهمية على منصتي «تندر» و«إنستجرام»، استُخدمت لاستدراج عدة ضحايا، من بينهم المجني عليها محل الواقعة؛ حيث عُثر على رسالة نصية

موجَّهة إليها جاء فيها: «نلتقي في مكان هادئ لجلسة يوغا»، فضلًا عن استعادة رسالة واتساب محذوفة، أرسلها المتهم إلى صديقه.

- وقد أصدرت المحكمة في دلهي بدولة الهند حكمها، مؤكدة أن التكامل القائم بين الأدلة الرقمية وبيانات الموقع اللحظي، الميتاداتا، والسلوك الإلكتروني يُشكِّل منظومة إثبات مغلقة تُقصي الشك المعقول في قضايا العنف الجنسي، بما يتماشى مع نتائج دراسة Pfeuffer (2019)، التي أشارت إلى أن 92% من قضايا الاغتصاب في الهند (2018-2023) تعتمد على الأدلة الرقمية لتعزيز دقة الإثبات بنسبة 78%. وعلاوةً على ذلك، أضحت هذه القضية بمثابة سابقة قضائية، مع اعتمادها كمرجع في 13 قضية لاحقة حتى عام 2023، مؤسِّسةً بذلك معيارًا جديدًا للاعتماد على بيانات التطبيقات الذكية كأدلة دامغة (§ 65B IT Act).

ويرى الباحث أن التوجّه القضائي المتنامي نحو الاعتماد على الأدلة الرقمية، ولا سيما المستخلصة من التحليل الفني للبيانات وفحص الأجهزة الإلكترونية من قِبل جهات إنفاذ القانون، يمثل خطوة رشيدة تُعزز من موثوقية الإثبات في ميدان العدالة الجنائية الرقمية كما يؤكد ضرورة تعميم هذا النهج بين مختلف الهيئات القضائية والاستشارية؛ لما يتيحه من وسائل فعَّالة لتوثيق الأدلة الرقمية الخاصة بالاتهام، بما يُسهِم في تحقيق العدالة وتظلّ الوسائل التقنية قادرة في نهاية المطاف على كشف الحقيقة، رغم محاولات مرتكبي هذه الجرائم التخفّي.

أهمية البصمة الرقمية في مسرح الجريمة الرقمي

تُشكِّل البصمة الرقمية عنصرًا حاسمًا في التحقيقات الجنائية الحديثة؛ حيث تعمل على كشف الأدلة الخفية عبر تتبع الآثار الرقمية التي يخلِّفها الجناة، مثل: عناوين الIP، وبيانات الأجهزة كـ IMEI أو MAC Address، والبيانات الوصفية (Metadata) التي تُسجل توقيت وموقع النشاط الإلكتروني، وتُساعد هذه التقنية في ربط المشتبه بهم بجرائم متنوعة، بدءًا من الجرائم السيبرانية كالاختراقات وهجمات الفدية، ووصولًا إلى الجرائم المادية التي تترك آثارًا رقمية كاتصالات هاتفية أو سجلات مراقبة.

كما تُسهم في إعادة بناء مسرح الجريمة افتراضيًّا عبر تحليل أنماط الاتصالات والتحويلات المالية المشبوهة، أو حتى تحديد هويات مجهولة عبر منصات مُشفَّرة كالتالي:

1. كشف الشبكات الإجرامية والإرهابية

تعتمد أجهزة الاستخبارات الأمنية على تتبع البيانات الوصفية (Metadata) مثل: توقيت الاتصالات ومواقع الأجهزة، حتى لو كانت المحادثات مشفرة؛ مما يساعد في رسم خرائط علاقات المشتبه بهم وعلى سبيل المثال، أسهمت تحليلات البصمة الرقمية في تفكيك خلايا إرهابية عبر ربط حسابات وهمية على وسائل التواصل بتحركات ميدانية (خليفة، 2020).

2. مواجهة الجرائم السيبرانية المتطورة

مع تصاعد هجمات الRansomware والاختراقات الاستهدافية، تُستخدم البصمة الرقمية لتحديد مصادر الهجمات عبر تحليل عناوين الIP المزَيَّفة، أو أنماط البرمجيات الخبيثة، أو حتى التوقيعات الرقمية الفريدة للمتسللين.

3. مكافحة التمويل الإرهابي

أصبحت العملات المشفرة أداةً رئيسة لتمويل الإرهاب، لكن تقنيات مثل: Blockchain Analysis التي توفرها شركة Chain-alysis تتعقب التدفقات المالية المشبوهة عبر تحليل سجلات المعاملات الرقمية؛ مما أسهم في تجميد أصول جماعات إرهابية (البهي، 2021) ونتناولها كالتالي:

أ. رصد عمليات تمويل الإرهاب يعتمد بشكل متزايد على القنوات الرقمية؛ مما يجعل البصمة الرقمية أداة لا غنى عنها في تعقب هذه الأنشطة وتفكيك الشبكات المالية المرتبطة بالجماعات الإرهابية.

ب. مراقبة المحافظ الإلكترونية والعملات المشفرة: تُستخدم المحافظ الرقمية والعملات المشفرة مثل: «Bitcoin» لنقل الأموال بسرية، ولكن البصمة الرقمية تتيح تتبع حركات المحافظ المشبوهة وتحليل سلاسل العمليات، باستخدام أدوات تحليل Blockchain وربطها بهويات حقيقية.

ج. رصد التبرعات المشبوهة: بعض التنظيمات الإرهابية تستخدم واجهات خيرية أو دينية لجمع التبرعات عبر البصمة الرقمية ويمكن تحليل أنماط التبرع، وعلاقات المتبرعين بالجهة المستلمة، واكتشاف حملات تمويل مشبوهة أو متكررة (Farber, S. 2025).

د. كشفت التقارير عن استخدام البصمة الرقمية في تفكيك شبكة إرهابية في أوروبا واعتمدت على تطبيقات مراسلة مُشفَّرة، حيث تم ربط حسابات وهمية بتحركات ميدانية عبر بيانات الموقع الجغرافي وفي آسيا تم تعقب هجمات إلكترونية على البنية التحتية الحيوية مرتبطة بدول معادية، عبر تحليل شفرات برمجية فريدة (Reedy, 2023).

أمثلة حقيقية على استخدام البصمة الرقمية في مكافحة الجريمة والإرهاب

من أبرز الأمثلة على ذلك تفكيك شبكة «EncroChat» في عام 2020 التي كانت تُستخدم كمنصة اتصالات مشفرة من قبل عصابات المخدرات والجرائم المنظمة في أوروبا وتمكنت الشرطة الفرنسية والهولندية من اختراق خوادم الشبكة واعتراض ملايين الرسائل المشفرة؛ وذلك من خلال تتبع البصمات الرقمية للأجهزة مثل: الـ IMEI «بصمة الجهاز الرقمي والتليفون الذكي» وأدى ذلك إلى اعتقال أكثر من 800 شخص، ومصادرة أطنان من المخدرات والأسلحة، وإسقاط شبكة إجرامية دولية (الجمل، 2024).

وفي سياق موازٍ، جرى توظيف البصمة الرقمية في عام 2021 لتعقّب عمليات تمويل تنظيم «داعش» التي تمت عبر العملات المشفّرة، حيث كان التنظيم يعتمد على عملة «البيتكوين» في تمويل أنشطته داخل سوريا والعراق.

ومن خلال تحليل سلاسل الكتل (Blockchain)، باستخدام تقنيات طُوّرت من قِبل شركات متخصصة مثل: Chain lysis، تمكّن المحققون من تتبّع التحويلات المشبوهة التي وصلت إلى محافظ رقمية مرتبطة بالتنظيم؛ بما أسفر عن تجميد أصول رقمية تُقدّر قيمتها بملايين الدولارات، وهو ما مثّل عرقلة فعّالة لتمويل العمليات الإرهابية.

أما في عام 2022، فقد كُشف النقاب عن هجوم إلكتروني استهدف شبكة «Colonial Pipeline»، التي تُعدّ أكبر شبكة أنابيب لنقل الوقود في الولايات المتحدة، وقد أدّى الهجوم إلى تعطيل واسع في توزيع الوقود بشرق البلاد، ومن خلال تتبع البصمة الرقمية المرتبطة بالبرمجيات الخبيثة (Malware)، أمكن ربط هذا الهجوم بمجموعة «Darkside»، وهي مجموعة إجرامية تنشط في روسيا، وذلك استنادًا إلى تحليل الشفرات البرمجية الفريدة وعناوين بروتوكول الإنترنت (IP) المُقنَّعة.

وأسفرت التحقيقات عن استعادة جزء كبير من مبلغ الفدية الذي بلغ 4.4 مليون دولار، إلى جانب فرض عقوبات على الأطراف الضالعة في الهجوم (رمضان، 2022).

وفي تطور آخر خلال عام 2023، استُخدمت البصمة الرقمية في التصدي لعمليات تجنيد عناصر إرهابية عبر تطبيق «تليجرام»، حيث استغلت بعض الجماعات المتطرفة القنوات المتاحة على التطبيق لاستقطاب أعضاء جدد في مناطق متعددة من الشرق الأوسط وأوروبا.

ومن خلال تحليل البيانات الوصفية (Metadata)، بما في ذلك توقيت النشر والروابط المتبادلة، أمكن التعرف على المشرفين على تلك القنوات، وربط هوياتهم بحسابات على منصات أخرى مثل: «فيسبوك»، عبر تتبع بصمات الأجهزة، وقد أدّى هذا الجهد إلى إغلاق عشرات القنوات، بالإضافة إلى اعتقال 60 عنصرًا متطرفًا في كل من ألمانيا وفرنسا (كردمان، 2024).

3. المبحث الثاني: تطبيقات الذكاء الاصطناعي التوليدي في تكامل البصمات وتحسين كفاءة التحقيقات الجنائية في القضايا الكبرى

تُعدُّ البصمة الرقمية أداةً محوريةً في تعزيز البحث الجنائي الحديث؛ حيث تعتمد على رصد الآثار الرقمية التي يخلّفها الأفراد عبر تفاعلاتهم الإلكترونية، كعناوين الIP، وبيانات الأجهزة، وأنماط استخدام المنصات الرقمية، والبيانات الوصفية (metadata)؛ مما يُسهم في الكشف عن أدلة تربط المشتبهين بجرائم متنوعة كالاختراقات والاحتيال، أو حتى الجرائم التقليدية ذات البصمة الرقمية وتوفِّر هذه التقنية للمحققين دقةً عاليةً في تتبُّع مسارات البيانات وتحليلها؛ بما يعزز مصداقية الأدلة في المحاكم، خاصةً مع تعقُّد الجرائم السيبرانية (القحطاني، 2020).

ونتناول هذا المبحث من خلال مطلبين، وذلك على النحو التالي:

3. 1. المطلب الأول: أثر تطبيقات الذكاء الاصطناعي التوليدي في تكامل البصمات وإعادة بنائها

يشكّل التكامل بين البصمة الرقمية وتقنيات الذكاء الاصطناعي إحدى الركائز الحديثة في تطوير أدوات التحليل الجنائي الرقمي؛ حيث تُسهم هذه المنظومة المتقدمة في تعزيز قدرات أجهزة إنفاذ القانون على تحليل مسرح الجريمة الإلكتروني بدقة متناهية وسرعة فائقة.

فمن خلال خوارزميات الذكاء الاصطناعي، يمكن رصد وتحليل الأنماط السلوكية، وتتبع الأثر الرقمي للمشتبه بهم، واستخراج القرائن الرقمية القابلة للاعتماد القضائي، حتى في البيئات المشفّرة أو عالية التمويه (Farber, S. 2025).

كما تُمكّن هذه التقنيات من إعادة بناء تسلسل الأحداث الجنائية بشكل لحظي، وربط الأدلة الموزعة على منصات متعددة ضمن شبكة جنائية واحدة، وهذا التكامل لا يُعزز فقط فاعليَّة التحريات، بل يُسهم بشكل مباشر في دعم سرعة وكفاءة إجراءات العدالة الجنائية الناجزة، وضمان دقة القرار الأمني والقضائي، بما يتماشى مع معايير الأمن السيبراني، وحماية الخصوصية، ومتطلبات الملاحقة القانونية في الجرائم العابرة للحدود (كتهريب المخدرات والأسلحة غير المرخصة وتهريب المهاجرين وعمليات الاتجار بالبشر).

تعريف الذكاء الاصطناعي الأمني والتوليدي

الذكاء الاصطناعي (AI) هو استخدام أنظمة حاسوبية قادرة على محاكاة الذكاء البشري لتحليل البيانات، وتعلم الأنماط، واتخاذ

قرارات أو تنبؤات بدقة عالية، وفي سياق إنفاذ القانون، يُطبَّق AI لتحسين الكفاءة في منع الجرائم، وتحقيق الأمن، ومكافحة الأنشطة الإجرامية المعقدة، خاصةً غير التقليدية مثل: الجرائم الإلكترونية، والاحتيال المالي، والإرهاب الرقمي، والجرائم الرقمية والجرائم المنظمة (قاموس Webster, 2024).

يُقصد بالذكاء الاصطناعي التوليدي (Generative AI) من منظور أجهزة إنفاذ القانون توظيف النماذج والخوارزميات القادرة على إنتاج محتوى جديد (نصوص، صور، أصوات، مقاطع فيديو، بيانات محاكاة) استنادًا إلى أنماط سابقة في البيانات، بهدف تحليل الأدلة، وإعادة بناء مسارح الجريمة، والتنبؤ بالتهديدات، وتوليد سيناريوهات تحقيق افتراضية تدعم اتخاذ القرار الأمني.

ويُعدُّ الذكاء الاصطناعي منظومة متكاملة تعتمد على مكونات حاسمة مثل: التعلم الآلي (ML) والتعلم العميق (Deep Learning) ومعالجة اللغة الطبيعية (NLP)، مدعومة بخوارزميات متطورة كالشبكات العصبونية التلافيفية CNNs للصور، والذاكرة الطويلة قصيرة المدى LSTMs للسلاسل الزمنية) وهذه المكونات تُحدث ثورة في التحليل الجنائي الرقمي عبر معالجة البيانات الجنائية الضخمة (مثل: سجلات الشبكة، ومحتوى الاتصالات المشفرة، ومسارات الهجمات الإلكترونية) بسرعة ودقة غير مسبوقة فخوارزميات التعلم الآلي تُحلل الأنماط (Brown, T & Narayanan, A. 2024).

تطبيقات الذكاء الاصطناعي التوليدي في محاكاة وتتبع البصمات الرقمية: رؤية علمية متعمقة

- يمثل الذكاء الاصطناعي التوليدي (Generative AI) نقطة تحوّل في فهم وتحليل البصمة الرقمية الجنائية، إذ لم يعد التعاطي مع هذه الأخيرة مقتصرًا على جمع وتتبع الأثر الرقمي للمستخدم، بل توسّع ليشمل توليد تمثيلات رقمية تركيبية تحاكي الواقع كمسارح الجريمة المتعددة، وتُستخدم لاستقراء سلوكيات، أو كشف تزوير، أو التنبؤ بمخاطر رقمية مستقبلية (Chen, L. & Kumar, V. 2024).
- تقوم هذه التقنية على نماذج رياضية عميقة مثل: الشبكات الخصومية التوليدية (GANs) التي تُمكّن من إنتاج بيانات اصطناعية تحاكي المرور الشبكي، وسلوكيات المستخدمين، وتوقيعات البرمجيات الخبيثة بدقة شبه تامة، وكذلك النماذج اللغوية الضخمة (LLMs) مثل GPT-5 التي تستوعب السياقات المعقدة في النصوص الرقمية وتحلل الرسائل المشفرة لاستنباط النوايا المحتملة. كما تُستخدم نماذج المعالجة التوليدية للغة الطبيعية في تحليل الأنماط الخفية داخل المحتوى الرقمي واكتشاف التغيرات الدقيقة التي قد تشير إلى سلوك إجرامي أو نشاط ارهابي.
- يُستخدم في محاكاة سيناريوهات جنائية مستقبلية، بما يمكّن جهات التحقيق من بناء فرضيات ديناميكية قائمة على بيانات تركيبية تتفاعل مع أنماط السلوك المحتملة للجناة أو الضحايا؛ حيث تسهم هذه النماذج في كشف التزوير العميق وعمليات الاحتيال الرقمي (Deepfakes) من خلال توليد بصمات رقمية مضادة تستند إلى تحليل التشوهات الإحصائية الدقيقة داخل الصور والفيديو والصوت، الأمر الذي يسمح بكشف التلاعب الذي يصعب على الوسائل التقليدية اكتشافه (Torres, M, & Al Jameel, 2025).

التطابق والتنبؤ في تعقُّب الجرائم من خلال مضاهاة البصمة الرقمية والبيومترية

يمثل دمج البصمة البيومترية (مثل: بصمات الأصابع أو ملامح الوجه) مع البصمة الرقمية (مثل: أنماط استخدام الأجهزة أو عناوين IP) تطورًا نوعيًّا في أساليب مكافحة الجرائم الحديثة، سواء أكانت مادية أم إلكترونية، وتعتمد هذه المنظومة المتكاملة على توظيف تقنيات الذكاء الاصطناعي ضمن أنظمة المراقبة والتحليل الأمني، بهدف رصد السلوكيات المشبوهة واتخاذ إجراءات استباقية قبل وقوع الجريمة، فعلى سبيل المثال، يمكن لنظام ذكي أن يربط بين صورة وجه التُقطت بكاميرا مراقبة في موقع جريمة، وبين نشاط رقمي مشبوه صادر من الجهاز الخاص بنفس الشخص؛ مما يعزز من قوة الأدلة الجنائية ويُسرّع مسار التحقيق.

وفي سياق التحقق من الهويات، تسمح هذه التكنولوجيا بالكشف عن الهويات المزيفة أو المسروقة عبر مقارنة البصمة الحيوية للفرد (كمسح قزحية العين) مع بصمته الرقمية المخزنة في قواعد البيانات الحكومية. إذا حاول شخص استخدام هوية مزورة، سيكشف النظام التناقض بين البيانات الحيوية الفعلية؛ وتلك المرتبطة بالهوية الرقمية؛ مما يحد من جرائم الاحتيال كما تُستخدم أنظمة التعرف متعدد العوامل في المؤسسات الحساسة كالبنوك؛ حيث يتطلب الوصول مزامنةً بين مسح حيوي (كبصمة الإصبع) وتوافق الجهاز مع بصمة رقمية مسجلة سلفًا (B.G.B., & Q.L Artificial Intelligence. 2024).

أما في مجال الوقاية التنبئية، فيُستخدم الذكاء الاصطناعي لتحليل البيانات التاريخية والأنماط السلوكية للتنبؤ بالجرائم المحتملة وعلى سبيل المثال، إذا أظهر شخص ذو سجل إجرامي أنماطًا رقمية

مشبوهة (كشراء مواد خطرة عبر الإنترنت) وتواجدًا متكررًا في مناطق حساسة (مُسجل عبر كاميرات التعرف على الوجه)، يُصنف كنشاط عالي الخطورة، وتُتخذ إجراءات وقائية، والجدير بالذكر أن هذه النماذج على خوارزميات التعلم الآلي التي تربط بين مصادر البيانات المتباينة لاستنتاج التهديدات الخفية.

وعلى مستوى الأمن القومي والأمن الجنائي، تساعد هذه الأنظمة في ملاحقة الإرهابيين والمجرمين الخطرين عبر ربط الأدلة الحيوية (كالحمض النووي من مسرح الجريمة) بالبصمات الرقمية (كتحركات الهواتف المحمولة) ففي مطارات السعودية والإمارات والولايات المتحدة الأمريكية وألمانيا وإنجلترا مثلًا، يُستخدم مسح الوجه مع تحليل بيانات السفر الإلكترونية لتحديد المسافرين المطلوبين أثناء عبورهم المنافذ، إلا أن هذه التكنولوجيا تواجه تحديات كبيرة، أبرزها مخاوف الخصوصية، حيث يمكن لاستخدامها التعسفي انتهاك الحقوق الفردية، كما أن الأخطاء في التعرف على البصمات الحيوية (خاصةً مع التحيز العرقي في بعض الخوارزميات) قد تؤدي إلى اتهامات خاطئة.

مكونات ومضمون البصمة الرقمية ودورها في مكافحة الجرائم

- سجلات الاتصالات الهاتفية والرسائل النصية ومحادثات الإنترنت وتطبيقات التواصل الاجتماعي.
- بيانات كاميرات المراقبة والأجهزة الرقمية المتصلة بالإنترنت.
- سجلات أنظمة الدخول الذكية أو المفاتيح الإلكترونية.
- السجلات المالية والرقمية وكروت الائتمان وموزعات الاتصال.
- مواقع GPS للأجهزة المحمولة والبيانات الخلوية والاتصال من خلال الأقمار الاصطناعية.

وفي مكافحة الجرائم التقليدية، تُستخدم البصمة الرقمية لتحديد أماكن وجود المشتبه بهم، وتتبع تحركاتهم، وربطهم بمسرح الجريمة من خلال تحليل الاتصالات الرقمية والبيانات المسجلة. وهذه الأدلة توفر للمحققين أدلة موثوقة تُستخدم لتأكيد أو نفي تورط الأشخاص في الجرائم.

مفهوم البصمة البيومترية واستخداماتها الأمنية

البصمة البيومترية تعتمد على السمات الجسدية الفريدة لكل فرد ومن أبرز أشكالها: بصمة الأصابع لربط الجناة بجرائم سابقة، وتستخدم المطارات أنظمة التعرف على بصمة الوجه لرصد المطلوبين، بينما توفر بصمة قزحية العين حماية قصوى للمنشآت الحساسة، وتعتمد الأجهزة الأمنية على بصمة الصوت لتحديد هوية المتحدثين في التحقيقات والمكالمات، في حين تسمح بصمة الحركة عبر كاميرات المراقبة الذكية بتتبع الأفراد دون تلامس مباشر، مما يعزز قدرة الرصد الوقائي.

وتسهم هذه البصمات في تحديد هوية المجرمين بدقة عالية، مما يقلل من فرص الانتحال أو الإنكار أثناء التحقيقات الجنائية (World Economic Forum. 2024).

التكامل بين البصمتين الرقمية والبيومترية في مكافحة الجرائم

تُحقق النظم الأمنية أعلى مستويات الدقة والفاعليَّة من خلال الدمج بين البصمة الرقمية والبيومترية.

وهذا التكامل يسمح برصد النشاط الإجرامي من زوايا متعددة منها:

- **التتبع والتحقق**: عند العثور على بصمة رقمية في مسرح الجريمة، يمكن استخدامها لتحديد هوية المشتبه به من خلال مقارنتها بالبيانات البيومترية المسجلة في قواعد البيانات الأمنية.
- **كشف الأنشطة المشبوهة**: توفر البصمة الرقمية سجلًا كاملًا لتحركات واتصالات الجاني، بينما تؤكد البصمة البيومترية هوية الفاعل؛ مما يوفر أدلة دامغة أمام القضاء.
- **منع التهرب أو الانتحال**: يعزز استخدام البصمتين من صعوبة التهرب من العدالة، خاصة في الجرائم التي تعتمد على التنكر أو تزوير الهوية.

تطبيقات البصمة الرقمية والبيومترية في أنواع الجرائم المختلفة

- **الجرائم الجنائية التقليدية**: مثل: القتل أو السرقة، حيث تُستخدم بصمات الأصابع والوجه لتحديد هوية الجناة، مع تتبع أنشطتهم الرقمية لمعرفة تحركاتهم قبل وبعد ارتكاب الجريمة.
- **الجرائم الإرهابية**: تسهم البصمتان في رصد شبكات التواصل بين الأفراد، والتحقق من هويات المشتبه بهم في المنافذ الحدودية.
- **الجرائم المالية**: مثل: الاحتيال أو غسل الأموال، حيث تُستخدم البصمات الرقمية في تتبع الحسابات البنكية والتحويلات المالية المشبوهة، مع التحقق من هوية الفاعلين من خلال البيانات البيومترية (عبد العظيم، 2020).
- **الجرائم الإلكترونية**: يتم تتبع الهجمات السيبرانية باستخدام البصمات الرقمية وتحليل هوية الجناة المحتملين باستخدام أدوات بيومترية لتعزيز دقة تحديد المجرمين (اليوسف، 2022).

ويمثل الدمج بين البصمة الرقمية والبيومترية عبر تقنيات الذكاء الاصطناعي تحولًا إستراتيجيًّا في التحقيقات الجنائية، ولا سيما في قضايا الجنايات الكبرى، والإرهاب، والجرائم السيبرانية، حيث تتيح هذه المنظومة الذكية إنشاء نموذج موحد ومتعدد الأبعاد يُحلل سلوك الأفراد رقميًّا (مثل: سجلات التصفح، والحسابات، والموقع الجغرافي، ونمط الكتابة) ويطابقه مع السمات البيومترية (كالوجه، والبصمة، والصوت، وقزحية العين) بشكل آلي وفعّال، حتى في حالات التمويه أو انتحال الهوية.

وتتميز البصمة الرقمية بأنها دليل خفي لكنه قوي، حيث يمكن جمعه دون معرفة المستخدم؛ مما يجعله أداة فعّالة في تعقب الجرائم الرقمية ومع ذلك، فإن التحدي الأساسي الذي يواجه المحققين هو أن المجرمين يستخدمون تقنيات إخفاء الهوية مثل: الشبكات الافتراضية الخاصة (VPN)، وأدوات تشفير البيانات، والمتصفحات التي تمنع التتبع؛ مما يجعل من الصعب تحديد مصدر النشاط الإجرامي (أحمد، 2020).

3. 2. المطلب الثاني: التكامل الأمني الذكي بين البصمات الرقمية والبيومترية

3. 2. 1. المخرجات والدلائل الأمنية الناتجة عن دمج البصمات الرقمية والبيومترية بالذكاء الاصطناعي في التحقيقات الجنائية

- حيث تتيح الخوارزميات الذكية تحليل أنماط السلوك الرقمي ومطابقتها تلقائيًّا مع الهوية البيومترية للأفراد، مما يمكّن جهات التحقيق من التعرف بدقة عالية على الجناة حتى عند تخفيهم أو انتحالهم لهويات مزيفة (Parkinson, S, & Khan, 2024).
- أدلة تقنية موثوقة وعدالة ناجزة: لما يُنتجه هذا التكامل من أدلة جنائية رقمية - بيومترية مركبة تتمتع بقوة إثباتية عالية أمام القضاء؛ حيث يجمع بين دلائل رقمية (مثل: سجلات الاتصالات وبيانات التصفح) والبصمات الحيوية (مثل: بصمات الأصابع أو التعرف على الوجه وقرنية العين) بطريقة مدعومة بالذكاء الاصطناعي وهذه الأدلة المزدوجة تعزز موثوقيتها القانونية، وتسد الثغرات التي قد يستغلها المجرمون في تمويه هويتهم، وبذلك يتعاظم أثر إنفاذ القانون من خلال رفع كفاءة التحقيقات وتسريع وتيرة تحقيق العدالة الجنائية الناجزة بأعلى درجات الدقة والاحتراف (Reedy, 2023).
- يمثل الدمج بين البصمة الرقمية (الأنشطة الإلكترونية، بيانات المواقع، الحسابات المشبوهة) والبصمة البيومترية (مثل: بصمة الإصبع، التعرف على الوجه، الصوت) من خلال تقنيات الذكاء الاصطناعي أحد المرتكزات الحديثة في التحقيقات الجنائية المتقدمة، وهذا التكامل يسمح بربط السلوك الافتراضي بالهوية الفيزيائية بدقة؛ مما يُعزز قدرة أجهزة إنفاذ القانون على كشف المجرمين حتى في أكثر البيئات التقنية تعقيدًا، خاصة في الملفات ذات الطابع الإرهابي والسيبراني، وذلك كما يأتي:

1. الربط بين الهوية الرقمية والبيومترية: في الجرائم الإرهابية على شبكات الإنترنت لنشر مواد تحريضية أو تنسيق عمليات عن بُعد باستخدام أسماء مستعارة وهويات رقمية مزيفة وعلى سبيل المثال، قد ينشر أحد الأشخاص مقاطع مصورة تُحرض على العنف باسم مستعار، مستخدمًا أدوات تشفير مثل «Tor» أو تطبيقات تراسل آمنة عبر الذكاء الاصطناعي، يتم تحليل النمط السلوكي الرقمي (لغة الكتابة، وتوقيت النشر، والموقع الجغرافي)، ثم تتم مطابقته مع صور التتبع البيومتري (من كاميرات مراقبة، مطارات، أو بوابات إلكترونية)؛ مما يؤدي إلى تحديد هوية الفاعل بدقة فمثلًا في إحدى العمليات بأوروبا، تم القبض على عنصر متطرف بعد أن طابقت خوارزميات أمنية حديثة صوته في تسجيل تحريضي مع بصمة صوتية مسجلة له أثناء عبوره أحد المعابر الحدودية. (Evarts, H 2024).
2. **في الجنايات والقضايا الكبرى:** ففي الجرائم التقليدية ذات البعد التقني، مثل: القتل أو الخطف، قد يترك الجاني أدلة مادية بصمة إصبع أوDNA، لكن الجديد هو تتبع أنشطته قبل الجريمة عبر بصمته الرقمية، فمثلًا في إحدى قضايا القتل، رُفعت بصمة إصبع من أداة الجريمة، ولكن تأكيد التورط جاء بعد اكتشاف أن الهاتف المحمول الخاص بالجاني كان متصلًا بالشبكة قرب موقع الجريمة، وسجل محادثات بحث عن «كيفية محو الأدلة الجنائية» وهذه المعطيات، بعد معالجتها عبر منظومة AI، شكلت دليلًا مركبًا ساعد في الإدانة؛ لأنه ربط بين الزمان والمكان والنية والسلوك، بدلًا من الاعتماد على عنصر واحد فقط (Casey, E.2025).

3. 2. 2. دور خوارزميات الذكاء الاصطناعي في إعادة بناء وتحليل البصمات

1. تمثّل الخوارزميات في مجال الذكاء الاصطناعي الأمني إعادة بناء الأدلة البيومترية، مثل: البصمات الرقمية، التي قد تكون جزئية أو تالفة أو مطموسة.

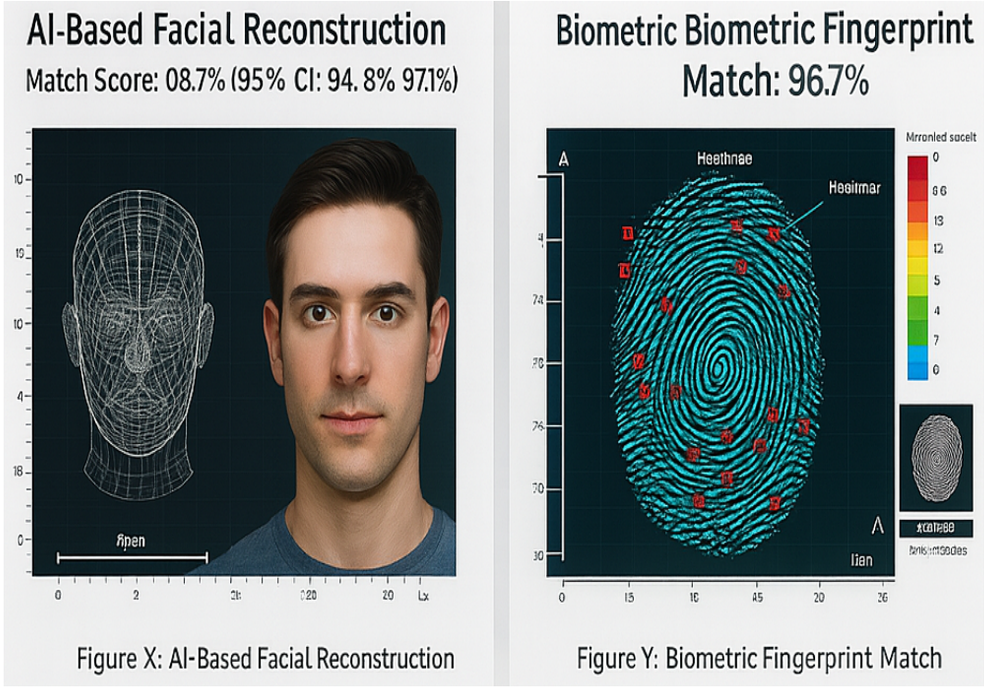
2. يعتمد الذكاء الاصطناعي في هذه الحالات على خوارزميات «التعلم العميق» (Deep Learning) المستندة إلى الشبكات العصبية التلافيفية (CNNs)، والتي يتم تدريبها على قواعد بيانات ضخمة من البصمات أو الصور الجنائية؛ مما يسمح لها بالتعرف على الأنماط وإعادة توليد الأجزاء الناقصة بدقة، كما تُستخدم هذه الخوارزميات في تحليل مسرح الجريمة الرقمي، من خلال نماذج خوارزمية تتبع المسارات الحركية، وتحليل الصور من الكاميرات الحرارية أو المرئية، والتقاط التسلسلات الزمنية للحدث من الأدلة الرقمية (log data, metadata) (2020.Yoon, S, Feng K).
3. أتاحت خوارزميات التعلم العميق القدرة على معالجة كميات ضخمة من البصمات في ثوانٍ، واستخلاص سمات دقيقة من الصور منخفضة الجودة أو الجزئية. ومن أبرز الابتكارات الحديثة، ما أعلنته شرطة نيو ساوث ويلز بأستراليا؛ حيث تم تطوير نظام ذكاء اصطناعي قادر على مطابقة البصمات من مناطق غير تقليدية في اليد مثل: الphalange، ما أدى إلى إعادة فتح قضايا جنائية قديمة بعد اكتشاف تطابقات لم تكن ممكنة بالنظم التقليدية.
4. ظهرت تقنيات غير تلامسية حديثة مثل: نماذج TipSegNet وG-MSGINet، التي تستخدم خوارزميات عميقة لتقسيم أطراف الأصابع من صور RGB عادية دون ملامسة، مع تسجيل معدلات دقة تتجاوز 99%؛ مما يجعلها مناسبة للاستخدام في الأماكن عالية الحساسية؛ مثل: المطارات والمؤسسات الأمنية.
5. كما تشهد نظم ما بعد المعالجة تطورًا نوعيًّا باستخدام الذكاء الاصطناعي التوليدي (Generative AI) لإعادة بناء البصمات التالفة، إلى جانب استخدام التشفير الكامل (FHE) لدمج البصمة مع قزحية العين وبصمة الصوت داخل إطار واحد مشفر وآمن.
6. قامت شرطة مدينة بوني بالهند في عام 2024 بإطلاق وحدة متنقلة تعتمد على الذكاء الاصطناعي لجمع البيانات البيومترية الكاملة (بصمة، قزحية، صورة متعددة الزوايا) من المشتبه بهم وتحليلها لحظيًا، حتى في حال تغيير المتهم لهيئته الخارجية كذلك، يُستخدم الذكاء الاصطناعي في أنظمة الحماية البيومترية في البنوك والمطارات، مع الاعتماد المتزايد على الذكاء الاصطناعي على الحافة

شكل 1

توليد نموذج ثلاثي الأبعاد تقريبي لوجه المشتبه به بدرجة تطابق عالية

Figure 1

Generating an approximate 3D model of the suspect's face with a high degree of accuracy



جدول 1

آليات الرصد والمطابقة الرقمية

Table 1

Digital monitoring and verification mechanisms

النوع	آليات الرصد الفني وجمع البصمات	آليات المطابقة و التحقق وربطها بالقضية	التطبيق الأمني في القضايا الإرهابية والجنائية
البصمة البيومترية	▪ تبدأ عملية الرصد عبر أجهزة استشعار عالية الدقة، مثل: الماسحات الضوئية لبصمات الأصابع وكاميرات القزحية والوجه، حيث يتم التقاط البيانات البيولوجية الخام ▪ تُجرى معالجة ثلاثية الأبعاد للصور والبيانات لتقليل التشويش الناجم عن الإضاءة أو التلف البيولوجي. ▪ ثم تقوم خوارزميات الذكاء الاصطناعي باستخراج النقاط المميزة والفريدة لكل شخص.	▪ بمجرد جمع البيانات، يتم إدخالها في أنظمة المطابقة الجنائية مثل: FBI - INTERPOL AFIS، حيث تُجرى مقارنة آنية مع ملايين السجلات وتُستخدم خوارزميات تعلم عميق تُحدّث باستمرار. ▪ ما يسمح بتحسين النتائج التلقائية مع كل مطابقة جديدة، وتقليل نسب الخطأ إلى حد كبير.	▪ تُستخدم هذه الآليات في تحديد هوية الإرهابيين والمطلوبين عبر المنافذ والمطارات. ▪ كما تُسهم في التعرف على الجثث مجهولة الهوية في العمليات الإرهابية. ▪ ربط بصمات الأصابع أو الوجه بالأدوات المستخدمة في جرائم مثل: التفجيرات والاغتيالات.
البصمة الرقمية	▪ تبدأ بعملية استخراج وتحليل البيانات الوصفية (Metadata) للصور والفيديوهات والملفات المضبوطة، والتي تكشف توقيت الالتقاط والموقع الجغرافي. ▪ ثم يتم تحليل السمات التقنية للأجهزة، مثل: عنوان الIP، نظام التشغيل، المتصفح، دقة الشاشة. ▪ إضافة إلى مراقبة الاتصالات عبر تحليل الشبكات والبروتوكولات خاصة في الشبكة المظلمة.	▪ بعد جمع هذه البيانات، تُجرى مطابقة عكسية مع قواعد بيانات الجرائم الإلكترونية باستخدام أنظمة، مثل: Palantir أو تقنيات التتبع العكسي، حتى لو استُخدمت أدوات إخفاء الهوية، مثل Tor وVPN ▪ كما يتم تطبيق تحليل السلوك الرقمي للكشف عن الأنماط الإجرامية أو الإرهابية وربطها بأشخاص محددين.	▪ تُسهم هذه الآليات في تتبع اتصالات الشبكات الإرهابية وتمويلها الإلكتروني، وكشف مخططات التفجيرات أو التجنيد عبر الإنترنت ▪ كما يمكن ربط الأجهزة الرقمية المضبوطة بمحتويات إجرامية (مثل: مخططات المتفجرات أو ملفات تمويل غير مشروع) ▪ مثل ما حدث في قضايا مثل: Silk Road وعمليات «إنترنت الظلام».
بصمة المخ	▪ تُجمع الإشارات العصبية بواسطة أجهزة تخطيط الدماغ (EEG) أو fNIRS بطريقة غير جراحية. ▪ تُحلل الموجات العصبية (مثل: P300، N200) الناتجة عن التعرف على صور أو معلومات متعلقة بالجريمة. ▪ تُعالج الإشارات لإزالة الضوضاء وتحليل الأنماط الترددية والزمنية.	▪ تُحوّل الإشارات إلى قوالب رقمية مميّزة وتُخزّن مشفرّة. ▪ تُستخدم خوارزميات تعلم عميق (مثل: CNN وSVM) لاستخراج نمط إدراكي فريد وربطه بالمشتبه به. ▪ يمكن دمج نتائجها مع البصمات الأخرى لرفع مستوى الثقة في تحديد الهوية أو الارتباط بالجريمة.	▪ تُستخدم لاكتشاف ما إذا كان المشتبه يتعرّف على عناصر مسرح الجريمة (اختبار المعرفة الخفية - Concealed Information Test). ▪ تُوظف في القضايا الإرهابية المعقدة لتأكيد أو نفي ارتباط المتهمين بأماكن أو أشخاص محددين. ▪ تساعد في كشف الأكاذيب الإدراكية أو استرجاع المعلومات المرتبطة بالذاكرة الإجرامية.

(Edge AI) «ويقصد به تشغيل خوارزميات الذكاء الاصطناعي مباشرة على الأجهزة الطرفية (Edge Devices)»، مما يُتيح زمن استجابة فوري دون الحاجة إلى الاعتماد على الخوادم السحابية (Guo, G& Xu, W.2024).

7. جمع الأدلة وتحليلها مثل: تحليل الحمض النووي (DNA) والطب الشرعي الرقمي تُسهم في كشف هوية الجناة عبر مطابقة العينات البيولوجية أو فحص الأجهزة الإلكترونية للضحية أو المشتبه به، كما تُستخدم كاميرات المراقبة ذات الدقة العالية لإعادة بناء خط سير الجاني قبل وبعد ارتكاب الجريمة في حالات القتل الغامضة؛ حيث تساعد تقنيات الواقع الافتراضي (VR) في إعادة تمثيل مسرح الجريمة لفهم تفاصيلها بدقة؛ مما يعزز فرص كشف الحقيقة.

3. 2. 3. الذكاء الاصطناعي التوليدي في تحسين البصمات البيومترية اثناء التحقيق في القضايا والحوادث

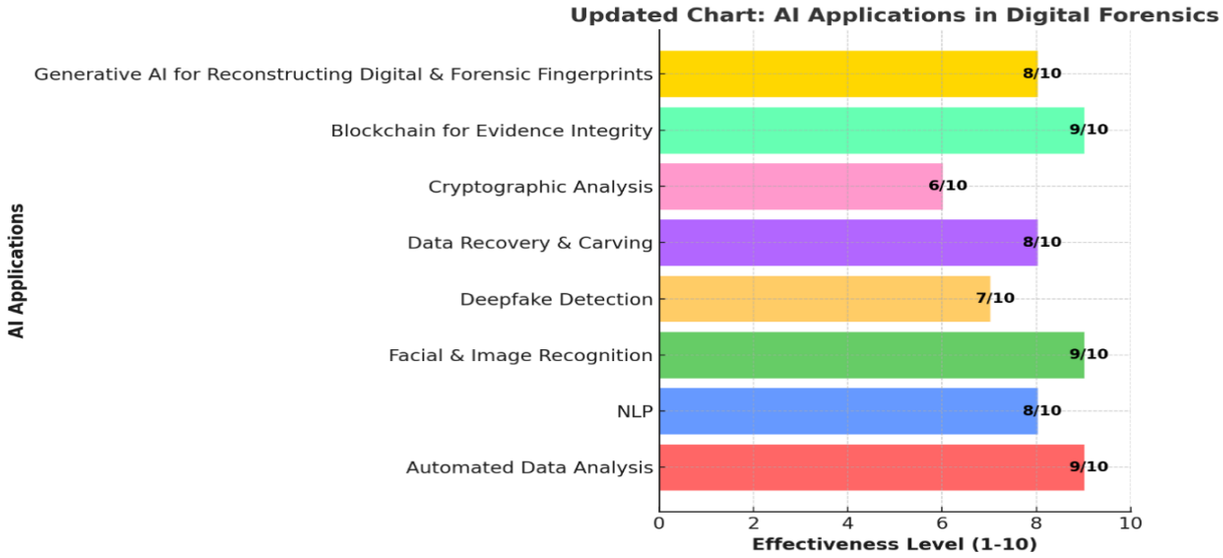
أدت التقنيات الحديثة مثل: البلوك تشين والذكاء الاصطناعي التوليدي إلى تحول جذري في عالم التحقيقات فتقنيات البلوك تشين تُوثق الأدلة الجنائية بشكل غير قابل للتلاعب؛ مما يضمن مصداقيتها

شكل 2

دور الذكاء الاصطناعي في رفع دقة التعرف على البصمات البيومترية والبيولوجية

Figure 2

The role of artificial intelligence in improving the accuracy of biometric and biological fingerprint recognition.



في المحاكم، فيُستخدم لمحاكاة سيناريوهات الجرائم الافتراضية لفهم سلوك المجرمين أو حتى توليد صور مشتبه بهم بناءً على أوصاف الضحايا ومع ذلك، فإن هذه التقنيات تُثير مخاوف أخلاقية، مثل: إمكانية إنشاء أدلة وهمية أو انتهاك الخصوصية عبر تحليل البيانات الحساسة.

ويمثل الذكاء الاصطناعي التوليدي نقلة نوعية في تحسين كفاءة وفاعليَّة البصمات البيومترية خلال مراحل التحقيق في القضايا الجنائية والحوادث الكبرى؛ حيث تسهم تقنياته في رفع جودة البيانات البيومترية وتحليلها بدقة فائقة، حتى في ظروف ميدانية معقدة أو في حال تضرر أو تشوّه البصمة المادية فمن خلال خوارزميات الذكاء الاصطناعي وتعلم الآلة، يمكن للنظام تصحيح صور الوجه المشوشة، وتحسين جودة بصمات الأصابع غير الكاملة أو المسوحة جزئيًّا، واستعادة ملامح الوجوه من تسجيلات كاميرات منخفضة الدقة، ما يُساعد فرق التحقيق في استخلاص أدلة دقيقة يمكن الاعتماد عليها قضائيًّا.

كما تسمح هذه التقنيات بمقارنة البصمة المستخرجة من مسرح الجريمة مع ملايين السجلات في قواعد البيانات البيومترية خلال ثوانٍ، مع تقديم نسب تطابق مدعومة بتحليل إحصائي ذكي وفي القضايا المعقدة كحوادث الحرائق أو التفجيرات، يُمكن للذكاء الاصطناعي تحليل بقايا السمات البيولوجية أو رسم نماذج ثلاثية الأبعاد للوجوه من أجزاء غير مكتملة؛ مما يُعزز من قدرة جهات التحقيق على تحديد هوية المجني عليه أو الجاني حتى في أصعب السيناريوهات (Horsman, & Iqbal, F 2025).

وفي إحدى القضايا الأمنية المعقدة، وقع تفجير في محطة نقل عامة، أسفر عن عدد من الضحايا وتشوه بعض الأدلة الفيزيائية في الموقع، ومن ذلك كاميرات المراقبة وبقايا بصمات بيومترية متناثرة وواجه المحققون صعوبة في تحديد هوية الجاني نتيجة رداءة جودة تسجيل الفيديو وعدم وضوح ملامح الوجه، بالإضافة إلى تلف جزئي في البصمات المرفوعة من قطعة معدنية استُخدمت في التفجير.

وتم استدعاء وحدة التحليل التقني المتقدم التي تعمل بتقنيات الذكاء الاصطناعي، حيث استخدمت خوارزميات تعزيز الصور (AI-based Facial Reconstruction) لاستعادة تفاصيل الوجه من اللقطات المشوشة، فتم توليد نموذج ثلاثي الأبعاد تقريبي لوجه المشتبه به بدرجة تطابق عالية وبالتوازي، كما هو موضح بشكل رقم (1) ففي تفجير مترو سانت بطرسبرغ في 2017 وانفجار ميناء الشهيد رجائي في جنوب إيران - إبريل 2025 «نموذجًا» تمت معالجة البصمة المسوحة جزئيًا بواسطة خوارزميات «تحسين النمط البيومتري» (Biometric Pattern Enhancement)، والتي نجحت في استكمال الفراغات بدقة تنبئية ومقارنتها مع قاعدة بيانات وطنية وبعد أقل من 6 ساعات، حدد النظام هوية المشتبه به بدقة تفوق 98%، وتم إصدار أمر ضبط وإحضار عاجل؛ حيث أُلقي القبض عليه

واعترف لاحقًا بتخطيط وتنفيذ العملية؛ ما يُظهر كيف أسهم الذكاء الاصطناعي في تحويل أدلة أولية ضعيفة إلى قرائن حاسمة في كشف الجريمة (Casey, E. 2025).

3. 2. 4. آليات الرصد الفني والمطابقة لكل من البصمات البيومترية والرقمية وبصمة المخ (p 300) في الحوادث والقضايا الإرهابية والجنائية

تعتمد الأجهزة الأمنية والعدلية على مجموعة من الآليات التقنية المتقدمة في رصد ومطابقة البصمات البيومترية والرقمية، خاصة في سياق التحقيق في قضايا الإرهاب والجرائم الخطيرة وفيما يخص البصمات البيومترية (Evarts، H. 2024)، وقد اشتمل الجدول السابق على آليات الرصد والمطابقة.

3. 2. 5. درجة فاعلية نجاح تطبيقات الذكاء الاصطناعي في الأدلة الجنائية الرقمية

يتمتع الذكاء الاصطناعي بدرجة عالية من الفاعلية في مجال الأدلة الجنائية الرقمية وإعادة بناء الأدلة الحيوية والبصمات بمختلف أنواعها. ففي مجال الأدلة الرقمية، تصل فاعلية تطبيقات التحليل الآلي للبيانات الضخمة إلى مستويات مرتفعة تتراوح بين 85% و95%، بفضل قدرتها على اكتشاف الأنماط الخفية وربط الأدلة ببعضها بشكل سريع ودقيق. أما في مجال إعادة بناء البصمات الرقمية (مثل: بصمات التصفح أو البصمة السلوكية الرقمية)، فتُقدَّر فاعلية الذكاء الاصطناعي التوليدي بما يقارب 80% - 90%، حيث يستطيع إعادة بناء البصمات المشوهة أو المسوحة جزئيًا اعتمادًا على خوارزميات التعلم العميق والنماذج التنبئية (Ahmed et al., 2022).

وفيما يتعلق بالبصمات البيومترية، مثل: بصمة الوجه والصوت والقزحية، فإن أنظمة الذكاء الاصطناعي، وخصوصًا الشبكات العصبية العميقة (Deep Neural Networks)، تحقق معدلات دقة تصل إلى 95% - 98% في التعرف والمطابقة، حتى في ظل ظروف إضاءة ضعيفة أو زوايا تصوير غير مثالية. أما في إعادة بناء البصمات البيولوجية، مثل: تحليل الحمض النووي (DNA) أو البصمات الوراثية، فقد ساعد الذكاء الاصطناعي في تسريع عمليات التسلسل الجيني (Genome Sequencing) وتحليل عينات الحمض النووي بشكل يصل إلى فاعلية تقارب 90% في تحديد الهوية وربطها بالأدلة المادية (Budowle et al., 2020)؛ (Al Awadhi & Fadhel, 2023) كما هو مشار إليه في الشكل رقم (2).

4. الخاتمة

أصبحت البصمة الرقمية، مدعومة بتقنيات الذكاء الاصطناعي، ركيزةً أساسية في تطوير النظم الجنائية والأمنية، حيث أسهمت في إحداث نقلة نوعية في آليات كشف الجرائم، سواء السيبرانية أو التقليدية ذات الامتداد الرقمي. فمن خلال تتبّع الآثار الرقمية وتحليل أنماط السلوك وتحركات المستخدمين، يمكن إعادة بناء مسار الجريمة بدقة، مما يُعزز فاعليَّة الإثبات القضائي عبر تقديم أدلة رقمية موثوقة يصعب دحضها. وتُبرز تقنيات التعلم الآلي وتحليل البيانات المتقدمة قدرة الأنظمة الأمنية على رصد الهويات الافتراضية والأنماط الخفية والتنبؤ بالسلوك الإجرامي، بل وإعادة بناء سيناريوهات الجريمة في بيئات مشفّرة أو معقّدة. ومع تزايد تعقيد الجرائم العابرة للحدود والمرتبطة بالإرهاب أو الاحتيال الرقمي، بات لزامًا على الجهات القضائية والأمنية تطوير قدراتها البشرية والتشريعية والتقنية، لتواكب هذا التطور وتُحقق عدالة ناجزة قائمة على الأدلة الرقمية والتحليل الذكي.

وقد توصل الباحث من خلال الدراسة إلى عدد من النتائج والتوصيات أهمها:

النتائج

توصلت الدراسة إلى أن التكامل بين الذكاء الاصطناعي والبصمة الرقمية، سواء أكانت رقمية أو بيومترية، أحدث تحولًا نوعيًا في أساليب التحري والتحليل الجنائي، إذ مكَّن أجهزة إنفاذ القانون من فهم الجرائم المعقدة، خصوصًا الجرائم السيبرانية والإرهاب الإلكتروني، بدرجة دقة وكفاءة تفوق الطرق التقليدية، من خلال تحليل البيانات غير المنظمة واستنباط الروابط السلوكية بين الوقائع والمشتبه بهم، وتحويل البصمة الرقمية إلى دليل جنائي حاسم يُعتمد عليه في تحديد الجناة وإثبات الوقائع أمام القضاء. كما بينت النتائج أهمية التحليل الاستخباري للشبكات الاجتماعية في الكشف المبكر عن الأنشطة الإرهابية وحملات التضليل، ودوره في تفكيك شبكات التجنيد وتهديدات الأمن القومي، في حين كشفت الدراسة عن التحديات التقنية والتشريعية المرتبطة بحفظ الأدلة الرقمية وتعدد مصادرها، وأظهرت كيف أسهم الذكاء الاصطناعي في تجاوزها عبر تطوير أدوات ذكية لاسترجاع البيانات وتتبع تسلسل الحيازة وتوحيد صيغ الأدلة. وأكدت النتائج في الختام أن الذكاء الاصطناعي أصبح ركيزة جوهرية لتحليل الأنماط الجُرمية والكشف عن الجرائم المنفذة عبر الطبقات المظلمة للإنترنت، وأن توظيفه الفعّال يمثل نقلة إستراتيجية نحو عدالة جنائية رقمية أكثر دقة وموثوقية وشمولًا.

التوصيات

- توصي الدراسة بإنشاء منظومة أمنية وطنية متكاملة لتحليل البصمات الرقمية بالذكاء الاصطناعي، تهدف إلى دعم أجهزة إنفاذ القانون في الرصد الوقائي والتعقب الاستخباري والتحقيق الجنائي، من خلال إنشاء مركز عمليات أمنية موحّد (AI Security Fusion Center) يدمج بين بيانات البصمات الرقمية والبيومترية وسجلات الجرائم الإلكترونية، ويعمل بخوارزميات تعلم عميق قادرة على تحليل الأنماط الإجرامية والتنبؤ بالتهديدات قبل وقوعها. وتشمل آليات التنفيذ: تطوير بنية تحتية رقمية مؤمنة تعتمد على أنظمة تحليل فوري (Real-Time Forensics) وتعلّم اتحادي يحافظ على سرية البيانات، وتدريب الكوادر الأمنية والقضائية على أدوات الذكاء الاصطناعي والتحليل التنبئي، وإنشاء تشريعات متخصصة تنظم استخدام الأدلة الرقمية والبيومترية وتضمن حجيتها القانونية، بما يحقق التكامل بين الأمن الوقائي والعدالة الجنائية الرقمية في مواجهة الجرائم السيبرانية والإرهاب الإلكتروني.
- إنشاء وحدات متخصصة في «الاستجابة الرقمية السريعة» داخل مراكز الشرطة أمرٌ ضروريٌّ، بحيث تضم هذه الوحدات خبراء في الأدلة الجنائية الرقمية، ومحللي بيانات، ومهندسي نظم، قادرين على فحص الأجهزة الرقمية ميدانيًا كتحليل الأدلة الجينية، والتحليل الرقمي للصور والفيديو، وتحليل البيانات الرقمية بالذكاء الاصطناعي ويمكن أن يساعد هذا في تقديم أدلة قوية في القضايا الجنائية وتقديم التقارير الفنية ذات الدقة العالية للمحكمة واستخلاص الأدلة في اللحظة ذاتها، مما يقلل من فرص ضياع الأدلة أو تزييفها، ويسرع في إصدار أوامر التوقيف والاستدعاء.
- تطوير تشريعات جنائية رقمية حديثة تُنظم إجراءات جمع وتحليل وتقديم البصمات الرقمية والبيومترية، بما يضمن مشروعيتها أمام القضاء، ويحمي في الوقت ذاته الخصوصية الرقمية للأفراد. فلا جدوى من التوسع في استخدام هذه الأدلة دون وجود إطار قانوني واضح يحدد معايير قبولها في مراحل التحقيق والاستدلال والمحاكمة، ويضمن الالتزام بسلسلة الحفظ الرقمية (Chain of Cus-tody) التي تضمن عدم التلاعب بها.

الإفصاح عن تضارب المصالح

يعلن المؤلف أنه ليس له أي تضارب في المصالح للمقالة المنشورة.

الإفصاح عن تمويل البحث

يعلن المؤلف بأن البحث المنشور لم يتلقَ أي منحة ماليَّة، من أي جهة تمويل في القطاعات الحكوميَّة، أو التجاريَّة، أو المؤسسات غير الربحية.

المراجع

المراجع العربية

أحمد، بن مالك. (2020). البصمة الوراثية ودورها في الإثبات الجنائي، مجلة آفاق علمية، م22(ع40)، ص 58.

البهي، رغدة. (2021). الردع السيبراني: المفهوم والإشكاليات والمتطلبات، المركز الديمقراطي العربي، جامعة القاهرة، مجلة العلوم السياسية والقانون، ع1، ص 66.

الجمل، أحمد. (2024). البصمة الوراثية ودورها في الإثبات الجنائي، المجلة القومية الجنائية، المركز القومي للبحوث الجنائية والاجتماعية، القاهرة، م 46(ع3)، ص 85.

ابن خليفة، إلهام صالح. (2014). دور البصمات والآثار العادية في الإثبات الجنائي، ط1، (الأردن، دار الثقافة).

رمضان، شريف عبد الحميد حسن. (2022). الحرب السيبرانية ومدي ملاءمتها مع القانون الدولي الإنساني، مجلة كلية الشريعة والأنظمة، جامعة الطائف، المملكة العربية السعودية، ص 33.

السبكي، هاني. (2024). التقنيات الحديثة في مكافحة عمليات الاتجار بالبشر، القاهرة، دار الفكر الجامعي.

عبد الجواد، أميمة جمال. (2023). دور التكنولوجيا في الإثبات الجنائي) البصمة الوراثية - الدليل الرقمي (المؤتمر العلمي الدولي الثامن التكنولوجيا والقانون)، جامعة طنطا، ص 107.

عبد العظيم، أميرة. (2023). المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مجلة الشريعة والقانون، القاهرة، (ع 35)، ص 124.

الغثبر، خالد سليمان، القحطاني، محمد عبد الله. (2024). أمن المعلومات بلغة ميسرة، ط1، الرياض، مركز التميز لأمن المعلومات.

فتح الله، محمود رجب. (2021). البصمة الرقمية ودورها في الإثبات الجنائي: دراسة تطبيقية مقارنة، الإسكندرية، دار الجامعة الجديدة، ص 33.

قاسم، إبراهيم. (2024). اعتماد الأدلة الرقمية في الإثبات الجنائي وفقًا لقانون مكافحة الجرائم الإلكترونية، تقرير جريدة اليوم السابع المصرية https://www.youm7.com/story/2024/10/10

قاموس Webster من خلال الموقع الإلكتروني التالي: https://www.merriam-webster.com تاريخ زيارة الموقع 14/3/2024.

كردمان، أفضال السيد صديق. (2024). البصمات الجنائية ودورها في مسرح الجريمة، بحث محكم، مجلة الدراسات القانونية والاقتصادية، م 10(ع4)، ص 63.

محمد، آمنة على البشير. (2023). الأمن السيبراني في ضوء مقاصد الشريعة، المجلد الأول، مجلة كلية الدراسات الإسلامية والعربية، بالإسكندرية، م1(ع37)، ص 54.

محيي الدين، أسامة حسين. (2021). حجية الدليل الرقمي في الإثبات الجنائي للجرائم المعلوماتية دراسة تحليلية مقارنة، مجلة البحوث القانوني

المراجع الأجنبية

Ahmed, M., Islam, M. R., & Kabir, M. (2022). Generative adversarial networks (GANs) in forensic science: Re-constructing missing and damaged digital evidence. Forensic Science International: Digital Investiga-tion, 41, 301429. https://doi.org/10.1016/j.fsidi.2022.301429

AI governance in cybersecurity: Principles for managing generative AI risks. Geneva: WEF

Al Awadhi, A., & Fadhel, F (2023). Artificial intelligence in forensic science: Applications, challenges, and fu-ture directions. Forensic Science International: Synergy, 8, 100266. https://doi.org/10.1016/j.fsisyn.2023.100266

B.G.B., & Q.L. (2024). Artificial Intelligence in Social Media Forensics: A Comprehensive Survey and Analysis. Electronics, 13(9), 1671. https://www.mdpi.com/2079-9292/13/9/1671MDPI

Budowle, B., Schmedes, S. E., & Wendt, F R. (2020). Advances in forensic DNA analysis using machine learning and AI. Forensic Science International: Genetics, 48, 102336. https://doi.org/10.1016/j.fsigen.2020.102336

Casey, E. (2025). Digital evidence and computer crime: Forensic science, computers, and the internet (4th ed.). Academic Press.

Chen, L., & Kumar, V. (2024).

CHI. (2019). Proceedings of the Human Factors Conference in Computing Systems, Glasgow, Scotland, Uk, pp. 1-12.

Deepfake forensics in the era of generative AI: Detection and counter-generation. ACM Transactions on Mul-timedia Computing, 20(2), 1-21.

Digital forensics and generative AI in GCC security frameworks: A review. Arab Journal of Information Secu-rity, 5(2), 71-89.

EncroChat and the future of digital forensics in Europe. Journal of Law, Technology and Policy, 14(1), 88-112.

European Union Agency for Cybersecurity (ENISA). (2024).

Evarts, H. (2024, January 10). AI discovers that not every fingerprint is unique. ScienceDaily. Retrieved from https://www.sciencedaily.com/releases/2024/01/240110120225.htmScienceDaily

Evarts, H. (2024, January 10). AI Discovers That Not Every Fingerprint Is Unique. Columbia Engineering. Re-trieved from https://www.engineering.columbia.edu/about/news/ai-discovers-not-every-fingerprint-uniqueColumbia Engineering

Farber, S. (2025). AI as a decision support tool in forensic image analysis: A pilot study on integrating large language models into crime scene investigation workflows. Journal of Forensic Sciences, 70(5), 932-943. https://doi.org/10.1111/1556-4029.70035PMC+1University of Haifa+1

Farber, S. (2025). AI as a decision support tool in forensic image analysis: A pilot study on integrating large language models into crime scene investigation workflows. Journal of Forensic Sciences, 70(5), 932-943. https://doi.org/10.1111/1556-4029.70035

Generative AI in cybercrime investigations: Trends, techniques, and ethical dilemmas. Computers & Securi-ty, 132, 103225.

Guo, G., et al. (2024). AI Discovers That Not Every Fingerprint Is Unique. Columbia Engineering. Retrieved from https://www.engineering.columbia.edu/about/news/ai-discovers-not-every-fingerprint-uniqueelectropages.com+2Columbia Engineering+2Criminal Legal News+2

forensics and cyber crime. Springer. https://doi.org/10.1007/978-3-030-54809-9

Schulz, M., & Gerlach, T. (2023). EncroChat and the admissibility of digital evidence in criminal trials: A Ger-man perspective. European Criminal Law Review, 13(1), 45–62.

Torres, M., & Al Jameel, M. (2025).

U.S. Attorney's Office, Middle District of Florida. (2025, February 11). The California teenager sentenced to 48 months for nationwide swatting spree. https://www.justice.gov/usao-mdfl/pr/california-teenager-sentenced-48-months-nationwide-swatting-spree

Wyzykowski, A. B. V., & Jain, A. K. (2023). A universal latent fingerprint enhancer using transformers. arXiv preprint arXiv:2306.00231. https://arxiv.org/abs/2306.00231arXiv

Yoon, S., Feng, J., & Jain, A. K. (2020). Deep learning-based latent fingerprint matching: Recent progress. IEEE Transactions on Information Forensics and Security, 15, 3620–3634.

Horsman, G., & Iqbal, F (2025). Artificial intelligence and the investigation of crime: Promises, perils, and pos-sibilities. Forensic Science International: Digital Investigation, 43, 301477. https://doi.org/10.1016/j.fsidi.2025.301477

Interpol. (2023). Biometric Hub. Retrieved from https://www.interpol.int/en/How-we-work/Forensics/Biometric-HubInterpol

Parkinson, S., & Khan, S. (2024). The role of Artificial Intelligence in digital forensics: Case studies and future directions. Assessment & Development Matters, 16(1), 42–47. https://doi.org/10.53841/bpsadm.2024.16.1.42

Pfeuffer, K., Geiger MJ, Prange S, Mecke L, Buschek D, Alt F (2019) Behavioural biometrics in vr: identifying people from body motion and relations in virtual.

Rogers, M. K., & Seigfried-Spellar, K. C. (2021). Digital forensics and cyber crime. Springer. https://doi.org/10.1007/978-3-030-54809-9

Rogers, M. K., & Seigfried-Spellar, K. C. (2021). Digital