

عنوان البحث

تحليل فعالية أنظمة كاميرات المراقبة في تعزيز أمن المؤسسات المصرفية: دراسة تطبيقية على
البنك العربي الوطني

إعداد الطالب/

محمد عبد المحسن القحطاني

إشراف/

د. الفیصل عبد الحمید

د. فايز جراد

العام الدراسي:

1446هـ - 2025 م

الفصل الأول: الإطار العام للدراسة

1.1 مقدمة:

تعتبر المؤسسات المصرفية من الأهداف الرئيسية للتهديدات الأمنية المتنوعة، بدءاً من عمليات السطو المسلح وصولاً إلى الاحتيالات المالية، فضلاً عن الاختراقات الرقمية وسرقة البيانات. في ظل اعتماد البيئة المصرفية على الثقة كأساس لاستمرارية علاقاتها مع العملاء، يصبح من الضروري تعزيز الإجراءات الأمنية كجزء من الاستراتيجية المؤسسية. تعد أنظمة كاميرات المراقبة بالفيديو من بين أبرز الأدوات المستخدمة عالمياً في هذا السياق، حيث شهدت تطورات ملحوظة في الكفاءة والتعقيد بفضل تقدم تقنيات الذكاء الاصطناعي والتعلم العميق (Al-Ghamdi, Al- (Mutairi, & Al-Harbi, 2024).

تشير الدراسات المعاصرة إلى أن أنظمة المراقبة في البنوك لم تعد مقتصرة على التسجيل والتحقق، بل أصبحت قادرة على تنفيذ مهام تحليلية متقدمة، مثل التعرف على السلوكيات المشبوهة واكتشاف الأنماط غير المعتادة والتفاعل الفوري مع الأحداث (Al-powered threat detection In surveillance systems, 2024). وقد أصبحت هذه الأنظمة قادرة على معالجة كميات ضخمة من البيانات المرئية وتحليلها باستخدام خوارزميات التعلم العميق للكشف الاستباقي عن التهديدات (Intelligence Video Surveillance Using Deep Learning, 2024).

أثبتت العديد من الدراسات فعالية أنظمة المراقبة الذكية في الردع المباشر وغير المباشر للجرائم المصرفية. على سبيل المثال، أظهرت دراسة (Intelligence Surveillance System for Bank Security Against Robbery, 2024) أن البنوك التي تعتمد أنظمة مراقبة مدعومة بالذكاء الاصطناعي قد شهدت انخفاضاً ملحوظاً في حوادث السطو والاحتيال مقارنة بتلك التي لا تستخدم هذه الأنظمة.

مع تطور البنية التحتية الرقمية، بدأت البنوك في تبني نظم مراقبة متعددة الطبقات تجمع بين الفيديو المباشر والتحليلات الزمنية، بالإضافة إلى ربطها بأنظمة الأمن السيبراني، مما يعزز من قدرتها على إدارة الحوادث والتهديدات (Bank Surveillance System: Multi-Layered Security Strategy, 2024). وقد أظهرت التقارير الأمنية

أن التحليل الفوري للفيديوهات باستخدام خوارزميات الذكاء الاصطناعي يمكن البنوك من رصد التحركات غير الاعتيادية، خصوصاً حول أجهزة الصراف الآلي (IoT-Based ATM Surveillance, 2020).

من جهة أخرى، تشير الأدلة التطبيقية إلى أن فعالية هذه الأنظمة تعتمد على تكاملها مع أنظمة إدارة الفيديو (VMS)، حيث توضح الورقة البيضاء الصادرة عن (Saudi National Cybersecurity Authority, 2023). أن دمج التحليلات المتقدمة والمسرعات الذكية في أنظمة VMS يعزز من قدرة النظام على الاستجابة للتهديدات الأمنية بنسبة تفوق 85%. وقد أكد تقرير (Central Bank of Saudi Arabia, 2024). أن معظم البنوك التي اعتمدت أنظمة VMS الحديثة شهدت تحسناً كبيراً في مؤشرات الأمان الداخلي.

استناداً إلى ما سبق، يتضح الحاجة الملحة لتقييم فعالية أنظمة كاميرات المراقبة الذكية في السياق المحلي، خصوصاً في بيئة مصرفية حساسة مثل المملكة العربية السعودية، حيث يُعتبر "البنك العربي الوطني" من أبرز الكيانات المصرفية التي تستثمر في الحلول الأمنية المتقدمة. لذا، تنطلق هذه الدراسة لتحليل فعالية هذه الأنظمة داخل البنك من خلال دراسة تطبيقية ميدانية، تستند إلى معايير أمنية وفنية متقدمة، بهدف تقديم تصور علمي وعملي يعكس واقع الاستخدام، ونقاط القوة، ومواطن القصور، ومقترحات التطوير.

1.2 مشكلة الدراسة:

رغم التطورات الكبيرة التي شهدتها القطاع المصرفي في المملكة العربية السعودية نحو التحول الرقمي، وزيادة الاعتماد على أنظمة الكاميرات الذكية لتعزيز الأمن المؤسسي، إلا أن فعالية هذه الأنظمة في تقديم حماية شاملة لا تزال بحاجة إلى دراسة تفصيلية. تشير التقارير إلى أن الربط المباشر لكاميرات المراقبة بالإنترنت يمكن أن يخلق مخاطر اجتماعية وأمنية، خاصة إذا كانت الإعدادات الافتراضية غير محمية، مما يعرض سرية البيانات المصرفية للخطر (Ministry of Communications and Information Technology, KSA, 2023).

على مستوى المملكة، تعتبر السوق السعودية من الأسواق النامية بقوة في مجال أنظمة المراقبة بالفيديو، وذلك بفعل مبادرات رؤية 2030 والمشاريع الكبرى. حيث بلغ حجم هذا السوق حوالي 690.5 مليون دولار في 2024، ومن المتوقع أن يتجاوز 2 مليار دولار بحلول عام 2033، مع تسجيل نمو سنوي مركب يقدر بـ 13% نتيجة لتبني تقنيات الذكاء الاصطناعي وإنترنت الأشياء (Saudi Authority for Data and Artificial Intelligence, 2024).

كما تسعى الأجهزة الأمنية السعودية، مثل "سدايا"، إلى دمج الذكاء الاصطناعي مع أنظمة المراقبة لرصد السرقات والمشاجرات، فضلاً عن مراقبة حركة المرور، مما يعكس توجهاً نحو تحقيق الأمن الذي المتكامل. ومع ذلك، تفتقر الأبحاث التطبيقية إلى فحص مستوى التكامل الفعلي بين هذه الأنظمة في البنوك، وقدرتها على الكشف المبكر عن التهديدات وتحليلها والتفاعل معها ضمن نظام أمني شامل يضم الأمن السيبراني وأنظمة إدارة الفيديو (Boukerche et al., 2023).

يعد البنك العربي الوطني مثالاً حياً على بنك سعودي متقدم تقنياً، حيث يستثمر في التحول الرقمي وتطوير الخدمات المصرفية الرقمية المبتكرة، بما يتماشى مع رؤية المملكة 2030 وتوجهات البنك المركزي السعودي (ساما)، وقد حصل البنك على جائزة "البنك الأكثر ابتكاراً في الشرق الأوسط لعام 2023" تقديرًا لدوره الريادي في قطاع التقنية المالية (البنك العربي الوطني، 2023). ومع ذلك، يظل السؤال مطروحاً حول مدى فعالية أنظمة كاميرات المراقبة الذكية في تحقيق الحماية الفعلية للبنوك، وهو موضوع يشغل بال العديد من المؤسسات المالية (Monetary Authority of Saudi Arabia, 2023).

ومما سبق يمكننا تلخيص مشكلة الدراسة في الإجابة على التساؤل التالي:

ما مدى فعالية أنظمة كاميرات المراقبة في تعزيز أمن المؤسسات المصرفية، وكيف تساهم هذه الأنظمة في حماية

البنك العربي الوطني من التهديدات الأمنية المختلفة؟

1.3 أهمية الدراسة:

تتزايد التهديدات الأمنية التي تواجه المؤسسات المصرفية، مما يعكس الحاجة الملحة لتعزيز استراتيجيات الأمن. في هذا السياق، تلعب أنظمة كاميرات المراقبة دوراً محورياً في حماية الأصول والمعلومات الحساسة. تهدف هذه الدراسة إلى تحليل فعالية هذه الأنظمة في تعزيز الأمن بالمؤسسات المصرفية، مع التركيز على تجربة البنك العربي الوطني.

• الأهمية العلمية:

تساهم هذه الدراسة في إثراء الأدبيات الأكاديمية المتعلقة بأمن المعلومات في القطاع المصرفي، من خلال تقديم تحليل مفصل لفعالية أنظمة كاميرات المراقبة. كما توفر البيانات والمعلومات الضرورية لفهم كيفية استخدام التكنولوجيا الحديثة، مثل الذكاء الاصطناعي، في تحسين مستوى الأمان. من خلال تقديم رؤى جديدة، تعزز الدراسة الفهم النظري لتكامل أنظمة المراقبة مع استراتيجيات الأمن السيبراني.

• الأهمية العملية:

من الناحية العملية، تقدم الدراسة توصيات قابلة للتنفيذ للمؤسسات المصرفية لتحسين استراتيجياتها الأمنية. من خلال تحليل الحالة العملية للبنك العربي الوطني، يمكن للجهات المعنية تحديد نقاط القوة والقصور في أنظمة المراقبة الحالية، مما يساعد في تطوير حلول أكثر فعالية لمواجهة التهديدات الأمنية. كما تعزز الدراسة من ثقة العملاء في المؤسسات المصرفية من خلال تحسين مستويات الأمان وحماية المعلومات.

1.4 أهداف الدراسة:

- يهدف البحث الحالي إلى تحليل فعالية أنظمة كاميرات المراقبة في تعزيز أمن المؤسسات المصرفية، مع التركيز على تجربة البنك العربي الوطني. ويتفرع من الهدف الرئيسي مجموعة من الأهداف الفرعية التي تتمثل في:
- التعرف على مدى فعالية أنظمة كاميرات المراقبة في تعزيز الأمن داخل البنك العربي الوطني وتأثيرها على تقليل المخاطر الأمنية.
 - استكشاف الأنظمة التكنولوجية الحديثة المستخدمة في كاميرات المراقبة وقياس دورها في تحسين مستوى الأمان داخل المؤسسة.
 - تقييم أداء كاميرات المراقبة في كشف التهديدات الأمنية وتحليل البيانات المرتبطة بالأحداث بشكل فعال.
 - التعرف على التحديات التي يواجهها البنك العربي الوطني في تطبيق أنظمة كاميرات المراقبة الذكية وكيفية التغلب عليها.

- تقديم توصيات عملية لتحسين استراتيجيات الأمان في البنك، مما يساهم في تعزيز ثقة العملاء والحد من الجرائم المصرفية.

1.5 تساؤلات الدراسة:

السؤال الرئيسي: ما مدى فعالية أنظمة كاميرات المراقبة في تعزيز أمن المؤسسات المصرفية، وكيف تساهم هذه الأنظمة في حماية البنك العربي الوطني من التهديدات الأمنية المختلفة؟

ويتفرع من السؤال الرئيسي مجموعة من الأسئلة الفرعية التي تتمثل فيما يلي:

- السؤال الفرعي الأول: ما هي الأنظمة التكنولوجية الحديثة المستخدمة في كاميرات المراقبة لدى البنك العربي الوطني، وكيف تؤثر على مستوى الأمن؟

- السؤال الفرعي الثاني: كيف يتم تقييم فعالية كاميرات المراقبة في كشف التهديدات الأمنية داخل البنك؟

- السؤال الفرعي الثالث: ما هي التحديات التي يواجهها البنك العربي الوطني في تطبيق أنظمة كاميرات المراقبة الذكية؟

- السؤال الفرعي الرابع: هل هناك بيانات تشير إلى تأثير استخدام أنظمة المراقبة على تقليل حوادث الجرائم المصرفية في البنك؟

1.6 فروض الدراسة:

لتحقيق أهداف الدراسة وتحقيقها، فقد اعتمد الباحث على مجموعة من الفروض تتمثل في:

الفرضية الرئيسية: لا يوجد أثر ذو دلالة إحصائية عند مستوى $(\alpha = 0.05)$ لأنظمة كاميرات المراقبة في تعزيز أمن المؤسسات المصرفية، وخاصة في البنك العربي الوطني.

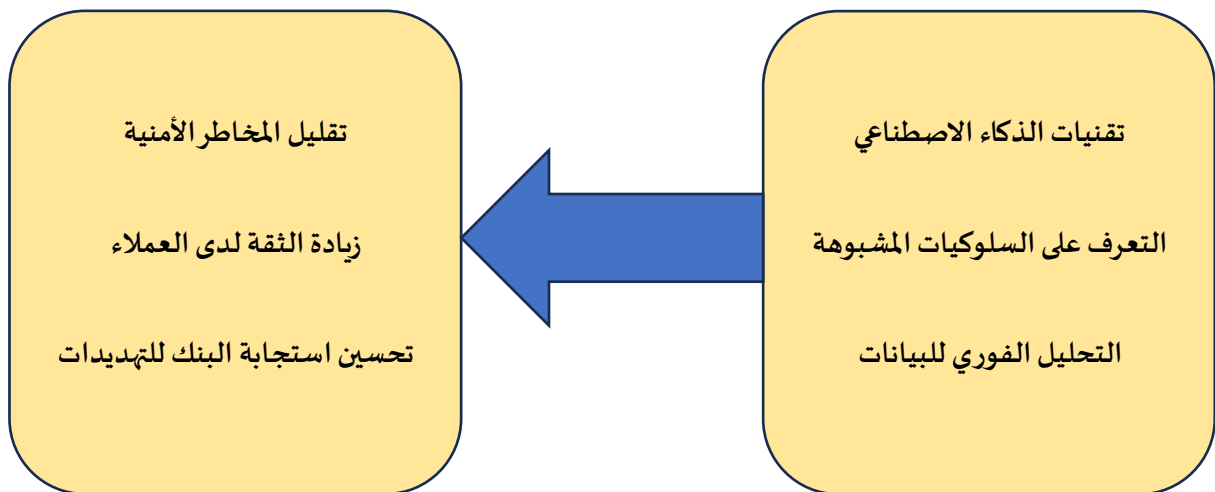
ويتفرع منها مجموعة من الفرضيات الفرعية التي تتمثل فيما يلي:

- الفرضية الفرعية الأولى: لا يوجد أثر ذو دلالة إحصائية عند مستوى $(\alpha = 0.05)$ لتأثير الأنظمة التكنولوجية الحديثة المستخدمة في كاميرات المراقبة على مستوى الأمن داخل البنك العربي الوطني.

- الفرضية الفرعية الثانية: لا يوجد أثر ذو دلالة إحصائية عند مستوى $(\alpha = 0.05)$ لفعالية كاميرات المراقبة في كشف التهديدات الأمنية داخل البنك العربي الوطني.
- الفرضية الفرعية الثالثة: لا يوجد أثر ذو دلالة إحصائية عند مستوى $(\alpha = 0.05)$ للتحديات التي يواجهها البنك العربي الوطني في تطبيق أنظمة كاميرات المراقبة الذكية على فعالية هذه الأنظمة في تعزيز الأمن.
- الفرضية الفرعية الرابعة: لا يوجد أثر ذو دلالة إحصائية عند مستوى $(\alpha = 0.05)$ لاستخدام أنظمة المراقبة على تقليل حوادث الجرائم المصرفية في البنك العربي الوطني.

1.7 نموذج الدراسة:

- يهدف هذا النموذج إلى التعرف على أثر أنظمة كاميرات المراقبة على تعزيز أمن المؤسسات المصرفية، بالتطبيق على البنك العربي الوطني في المملكة العربية السعودية.
- المتغير المستقل: أنظمة كاميرات المراقبة، وتتضمن (تقنيات الذكاء الاصطناعي، التعرف على السلوكيات المشبوهة، التحليل الفوري للبيانات).
 - المتغير التابع: تعزيز أمن المؤسسات المصرفية، والذي يشمل (تقليل المخاطر الأمنية، زيادة الثقة لدى العملاء، تحسين استجابة البنك للتهديدات).



شكل (١) متغيرات الدراسة

(المصدر : إعداد الباحث)

1.8 مصطلحات الدراسة:

1. أنظمة كاميرات المراقبة (CCTV Systems):

"هياكل تقنية متكاملة تشمل كاميرات ذكية، أنظمة تخزين سحابية، وخوارزميات تحليل فيديو قائمة على الذكاء الاصطناعي للكشف التلقائي عن التهديدات" (Al-Hadhrani et al., 2022, p. 34; Saudi National Cybersecurity Authority, 2023). ("Authority", 2023).

2. فعالية المراقبة (Surveillance Effectiveness):

"مدى تحقيق الأنظمة لأهدافها الأمنية عبر مؤشرات: دقة الكشف عن التهديدات، زمن الاستجابة، وتقليل الجرائم" (Alshammari & Alwan, 2023, p. 8; "Interpol", 2024).

3. الأمن المصرفي (Bank Security):

"الإطار المتكامل لحماية الأصول المالية والبيانات عبر تقنيات الذكاء الاصطناعي، البيوميتري، وأنظمة إدارة الفيديو" (SAMA, 2023, p. 41; "Boukerche et al.", 2023). (VMS).

4. أنظمة إدارة الفيديو (Video Management Systems – VMS):

"منصات برمجية لمراقبة الفيديو الحي، تحليل البيانات، ودمجها مع أنظمة الأمن السيبراني لتعزيز الاستجابة للتهديدات" (Saudi National Cybersecurity Authority, 2023, p. 12).

5. التهديدات الأمنية (Security Threats):

"أي فعل أو حدث يُهدد أصول البنك: السطو المسلح، الاحتيال المالي، الاختراقات الرقمية، أو سرقة البيانات" (Monetary Authority of Saudi Arabia, 2023, p. 9).

6. الذكاء الاصطناعي في المراقبة (AI-Powered Surveillance):

"استخدام خوارزميات التعلم العميق لتحليل الفيديو تلقائياً، الكشف عن السلوكيات المشبوهة، والتنبيه بالتهديدات"

(Al-Ghamdi et al., 2024, p. 5; *SDAIA*, 2024).

7. البنك العربي الوطني (Alinma Bank):

"مؤسسة مالية سعودية رائدة حاصلة على جائزة الابتكار 2023، وتمثل حالة الدراسة في هذا البحث" (Alinma Bank)

(Annual Report, 2023, p. 7).

8. تعزيز الأمن (Security Enhancement):

"التحسين القابل للقياس في مؤشرات الأمان: انخفاض حوادث الجرائم، تحسين زمن الاستجابة، وزيادة ثقة العملاء"

(Interpol, 2024, p. 16).

الفصل الثاني: الإطار النظري والدراسات السابقة.

تمهيد

يستعرض الفصل الثاني من البحث أنظمة كاميرات المراقبة وأهميتها في تعزيز أمن المؤسسات المصرفية، خاصة في ظل التحديات الأمنية المتزايدة. يتم تعريف أنظمة المراقبة كمنظومات تضم كاميرات وأجهزة تسجيل وشاشات عرض تهدف إلى توثيق الأحداث الأمنية وتعزيز الردع.

يتناول الفصل تاريخ تطور هذه الأنظمة من الأجهزة التناظرية إلى الرقمية، مع التركيز على تقنيات الذكاء الاصطناعي التي تحسن كفاءة المراقبة. كما يُستعرض الإطار التنظيمي في السعودية الذي يحدد معايير استخدام هذه الأنظمة، وأهمية التكامل مع الأمن السيبراني.

يتناول الفصل أيضاً التحديات المتعلقة بالخصوصية وحماية البيانات، ويبرز الحاجة إلى التقييم الفعال لفعالية الأنظمة، مستنداً إلى دراسات سابقة تدعم البحث الحالي وتساهم في تطوير استراتيجيات أمنية تعزز الأمان وثقة العملاء.

2.1 مقدمة عن أنظمة كاميرات المراقبة:

2.1.1 تعريف أنظمة كاميرات المراقبة:

تشير أنظمة المراقبة بالفيديو (CCTV) إلى منظومات متكاملة تتألف من:

تتألف أنظمة المراقبة بالفيديو من كاميرات رقمية/تناظرية، أجهزة تسجيل (DVR/NVR)، شبكات اتصالات، وشاشات عرض (Saudi Ministry of Interior, 2022).

من الناحية الوظيفية تقوم هذه الأنظمة بتوثيق الأحداث الأمنية مباشرةً وتحليلها لاحقاً لتعزيز الأمن والردع (مباشر، 2022).

ومن الناحية التكنولوجية تم دمج خوارزميات الذكاء الاصطناعي ورؤية الحاسوب لاكتشاف التهديدات في الوقت الفعلي كالتعدي على المناطق المحظورة أو السلوك غير الطبيعي (الزهاوي وشعلان، 2023).

وقانونياً تخضع في السعودية لللائحة أنظمة الكاميرات (القرار الملكي M/34) ومعايير الهيئة الوطنية للأمن السيبراني لضمان مشروعية البيانات المجمعة (Almarshad et al., 2024; المملكة العربية السعودية، 2025)

تعد أنظمة كاميرات المراقبة أدوات وقائية تعزز الوعي الظرفي في المؤسسات المالية، وتوفر أدلة جنائية قابلة للتدقيق وفق متطلبات البنك المركزي السعودي (SAMA). (Saudi National Cybersecurity Authority, 2022)

2.1.2 تاريخ وتطور أنظمة المراقبة:

مع تطور متطلبات الأمن والسلامة، شهدت أنظمة كاميرات المراقبة تحولاً جذرياً في بنيتها التقنية ووظائفها التشغيلية. فمنذ بداياتها الأولى كأدوات بسيطة للمراقبة البصرية، تطورت هذه الأنظمة لتصبح جزءاً أساسياً من البنية التحتية الأمنية في المؤسسات العامة والخاصة، وعلى وجه الخصوص في القطاع المصرفي الذي يعد من أكثر القطاعات حساسية من حيث أمن المعلومات والأصول. وقد واکب هذا التطور التقدم في مجالات التصوير الرقمي، والاتصالات، وتحليل البيانات. وفي المملكة العربية السعودية، حظيت أنظمة المراقبة باهتمام كبير على المستوى التنظيمي والتقني، خاصةً بعد صدور نظام استخدام كاميرات المراقبة الأمنية عام 2022، الذي يهدف إلى ضبط آليات استخدامها وضمان تكاملها مع جهود حفظ الأمن في المؤسسات المختلفة، بما فيها المؤسسات المصرفية.

أ- المرحلة التناظرية (Analog):

كانت البداية بأنظمة تناظرية تعتمد كاميرات تقليدية مرتبطة بأجهزة DVR لتسجيل الفيديو بجودة منخفضة، لكنها كانت تتميز بتكلفة تركيب منخفضة وسهولة الإعداد (مباشر، 2022).

ب- الانتقال إلى الرقمية (IP):

مع ظهور تكنولوجيا IP وNVR، أصبحت الكاميرات توفر جودة عالية ويمكن مراقبتها عن بُعد عبر الشبكات، مع إمكانية دمجها في البنية التحتية للشبكات المحلية (Almarshad et al., 2024).

ت- دمج الذكاء الاصطناعي:

شهدت أنظمة المراقبة تطورًا ملحوظًا بإدخال تقنيات الذكاء الاصطناعي، مثل التعرف على الوجوه، وكشف الحركات، والتنبهات الفورية، جنبًا إلى جنب مع تشفير التسجيلات (AES) لضمان حماية البيانات (Alwatan, 2022).

ث- الإطار التنظيمي في السعودية:

في 3 أكتوبر 2022، صدر مرسوم ملكي ونظام استخدام كاميرات المراقبة الأمنية (مرسوم م/34) لضبط تركيب وتشغيل هذه الأنظمة بما يتناسب مع التصنيفات الأمنية للأماكن (عالية، متوسطة، منخفضة الحساسية)، مع اشتراط الربط بغرف العمليات، والحفاظ على التسجيلات، وحظر النشر أو التعديل إلا بناءً على طلب رسمي أو أمر قضائي (Saudi Legal Portal, 2022; Almarshad et al., 2024).

يفرض النظام التزامات صارمة تشمل عدم التصنيع أو الاستيراد أو التشغيل دون رخصة، وتحديد أماكن محددة لحظر الكاميرات مثل غرف التنويم والحمامات، ووضع إشارات واضحة تُعلم الأشخاص بوجود مراقبة (Saudi Ministry of Interior, 2022; Alwatan, 2022; Aleqtisadiya, 2022).

2.2 أهمية أنظمة كاميرات المراقبة في المؤسسات المصرفية:

2.2.1 دور أنظمة المراقبة في تعزيز الأمان:

تلعب أنظمة كاميرات المراقبة دوراً محورياً في تعزيز أمن المؤسسات المصرفية من خلال مجموعة من الوظائف الحيوية:

1. ردع الجرائم والاحتيال: تُعد الكاميرات أداة فعّالة للردع، حيث يقلل وجودها المرئي من احتمالية وقوع السرقات

أو الاعتداءات داخل الفروع وأجهزة الصرف الآلي (Khan et al., 2023).

2. المراقبة اللحظية والاستجابة السريعة: تمكّن الكاميرات الشبكية (IP) المزودة بتحليل ذكي للصور فرق الحماية

من مراقبة الأحداث مباشرة واتخاذ الإجراءات الفورية عند رصد سلوك مريب (Alom et al., 2019).

3. توثيق ومعالجة الصور كأدلة قضائية: تقديم صور واضحة للوجه والأماكن وتعقب لحظات الجرائم يساعد في

التحقيقات وتقديم الأدلة إلى الجهات الرسمية (Khan et al., 2023).

4. زيادة ثقة العملاء والموظفين: توفر الكاميرات بيئة آمنة للموظفين والعملاء، مما يعزز الثقة بالمؤسسة ويحسن تجربتهم التفاعلية داخل البنك (Khan et al., 2023).

2.2.2 التهديدات الأمنية التي تواجه المؤسسات المصرفية:

تتعرض المؤسسات المصرفية لمجموعة متنوعة من التهديدات، تشمل:

1. السرقات والاعتداءات الخارجية: مثل سرقات الصناديق والفروع وعمليات الاعتداء في أجهزة الصراف الآلي، وتسهيل تحقيق الردع والتوثيق عبر الكاميرات (Khan et al., 2023).
 2. الاحتيال من الداخل: تصرفات الموظفين الاحتيالية تعتبر خطراً حقيقياً، وتُستخدم الكاميرات لمراقبة نشاطهم والتقاط أي سلوك مخالف (Khan et al., 2023).
 3. التخريب وسوء استخدام أجهزة الصراف الآلي: تتعرض بعض أجهزة ATM للتخريب أو التلاعب، والكاميرات توفر أدلة مباشرة وتساعد في منع هذه الأعمال (Khan et al., 2023).
 4. التهديدات السيبرانية المتزامنة: رغم أن الكاميرات تركز على الأمان المادي، إلا أن الاعتماد على الشبكات يجعلها عرضة للاختراق؛ لذا تتكامل مع أنظمة الأمن السيبراني لتحقيق حماية شاملة (Khan et al., 2023).
- تُشكل أنظمة كاميرات المراقبة خط الدفاع الأول في المؤسسات المصرفية، حيث تردع الجرائم، توفر الأدلة، وتمكّن من الاستجابة السريعة، بالإضافة إلى حماية الموظفين والعملاء داخلياً وخارجياً. وهي ضرورية لمواجهة التحديات الأمنية المتواصلة، بما في ذلك الجرائم المادية والاحتيال الداخلي وعمليات التخريب. ومع تطورها التقني، أصبحت جزءاً أساسياً من منظومة الأمان المتكاملة في القطاع المصرفي.

2.3 التقنيات الحديثة في أنظمة المراقبة:

تشهد أنظمة المراقبة تطورات متسارعة بفضل التقنيات الحديثة، وعلى رأسها الذكاء الاصطناعي والتعلم العميق. هذه التقنيات تساهم في تحسين كفاءة ودقة أنظمة المراقبة، وتمكينها من التعامل مع التحديات الأمنية المعقدة في المؤسسات المصرفية وغيرها من المؤسسات الحيوية (Saudi Vision 2030 Office, 2024).

2.3.1 الذكاء الاصطناعي والتعلم العميق في أنظمة المراقبة:

1. تحليل الفيديو الذكي: يمكن للذكاء الاصطناعي تحليل الفيديو في الوقت الفعلي، والتعرف على الأنماط غير الاعتيادية، وتحديد التهديدات المحتملة على سبيل المثال، يمكن للأنظمة الذكية التمييز بين الوجوه المشبوهة أو اكتشاف السلوكيات غير الاعتيادية، مما يعزز مستوى الأمان ويقلل من مخاطر التهديدات المحتملة (Alhazmi & Al-Sarawi, 2023). تستخدم البنوك الذكاء الاصطناعي لتحسين خدمة العملاء، وكشف الاحتيال، وإدارة الأموال والاستثمارات (Almuqrin et al., 2023).
2. التعرف على الوجوه: تعتبر تقنية التعرف على الوجوه من أبرز الابتكارات في أنظمة المراقبة، حيث تعتمد على تحليل الصور والبيانات البيومترية للأفراد لتحديد الهوية بدقة، يمكن استخدام هذه التقنية لتمييز الأشخاص المصرح لهم بالدخول إلى المناطق الحساسة من غير المصرح لهم، وتعزيز الأمن في الأماكن العامة والمحطات الحيوية مثل المطارات (Alhazmi & Al-Sarawi, 2023).
3. تحسين كفاءة العمليات: تساهم تقنيات الذكاء الاصطناعي في أتمتة العديد من العمليات في أنظمة المراقبة، مما يقلل الحاجة إلى التدخل البشري، ويوفر الوقت والجهد والموارد (Zahrawi & Shaalan, 2023). يمكن للذكاء الاصطناعي أتمتة المهام الروتينية مثل معالجة القروض وإدارة الحسابات والتحقق من الامتثال (Elnaim et al., 2024).
4. تعزيز الأمن السيبراني: يساهم الذكاء الاصطناعي في تعزيز الأمن السيبراني واكتشاف الاحتيال، حيث يمكنه تحليل كميات كبيرة من البيانات لتحديد الأنشطة المشبوهة والتنبيه بالتهديدات المحتملة (Almuqrin et al., 2023). يجب على المؤسسات المصرفية إنشاء أطر عمل قوية لإدارة المخاطر النموذجية والتحقق من صحتها والمراقبة المستمرة لضمان نزاهة عملية صنع القرار القائمة على الذكاء الاصطناعي (Abu-Taieh et al., 2024).

2.3.2 تحليل السلوكيات المشبوهة واكتشاف الأنماط:

1. اكتشاف الأنشطة غير الاعتيادية: يمكن لأنظمة المراقبة المدعومة بالذكاء الاصطناعي اكتشاف الأنشطة غير الاعتيادية في المؤسسات المصرفية، مثل التحويلات الكبيرة غير المتوقعة أو تسجيل الدخول من مواقع غير معتادة (Zahrawi & Shaalan, 2023). يتم رفع هذه الأمور لمزيد من التحقيق لضمان سلامة العمليات المالية.

2. تحليل الأنماط السلوكية: تستخدم برامج تحليل السلوك المتطورة المدعومة بالذكاء الاصطناعي للبحث عن الاتجاهات والأنماط في البيانات، مثل تسجيل الدخول من نفس الموقع أو إجراء معاملات صغيرة ومتكررة (Zahrawi & Shaalan, 2023). يساعد هذا التحليل في تحديد السلوكيات المشبوهة واتخاذ الإجراءات اللازمة.
3. الكشف عن التهديدات المحتملة: يمكن للذكاء الاصطناعي تحليل البيانات الضخمة ومراقبة الأنشطة المشبوهة على المنصات الرقمية للكشف عن التهديدات المحتملة، بما في ذلك التطرف والإرهاب (Alhazmi & Al-Sarawi, 2023). يمكن لأنظمة المراقبة الذكية اكتشاف الحالات الشاذة التي عادة ما تمر دون أن تلاحظها العين البشرية (Maprix, 2024).
4. تحسين الاستجابة للحوادث: يمكن للذكاء الاصطناعي تحسين الاستجابة للحوادث الأمنية من خلال أتمتة المهام الأمنية القائمة على السلوك واكتشاف التهديدات ومراقبتها في الوقت الفعلي (Almuqrin et al., 2023).

2.4 فعالية أنظمة كاميرات المراقبة:

تعد أنظمة كاميرات المراقبة أداة حيوية لتعزيز الأمن في المؤسسات المصرفية، ولكن تقييم فعاليتها يتطلب دراسة متأنية لتأثيرها في جوانب مختلفة (Cuevas et al., 2016). تشمل هذه الجوانب دراسات سابقة حول فعالية الأنظمة وتأثيرها على تقليل الجرائم المصرفية (Al-Zahrani, 2023).

2.4.1 دراسات سابقة عن فعالية الأنظمة:

- أظهرت الدراسات أن كاميرات المراقبة تساهم في الكشف المبكر عن الأنشطة المشبوهة، وتعزيز فرص منع الجرائم قبل وقوعها، والحد من السرقات والاعتداءات (Vennam et al., 2021).
- تشير بعض الدراسات إلى أن مجرد وجود كاميرات المراقبة يشكل رادعاً قوياً للمجرمين، حيث يتجنبون الأماكن التي تحتوي على كاميرات مراقبة لعلمهم أن ذلك يزيد من فرص اكتشافهم ومعاقبتهم (Cuevas et al., 2016).
- أكدت دراسات أخرى أهمية كاميرات المراقبة في توفير أدلة مرئية في التحقيقات الجنائية، مما يساعد في الكشف عن الجرائم وتحديد الجناة (Saudi Ministry of Education, 2023).

- في دراسة نشرت عام 2018، أشار أولياء الأمور والمختصون إلى أن كاميرات المراقبة عززت الانضباط السلوكي في مدارس البنين (Alotaibi et al., 2022).
- 2.4.2 تأثير أنظمة المراقبة على تقليل الجرائم المصرفية:
- تساهم كاميرات المراقبة في تقليل الجرائم المصرفية من خلال توثيق العمليات المصرفية، وتوفير لقطات فيديو يمكن استخدامها لتحديد المجرمين وحماية حسابات العملاء (Al-Zahrani, 2023).
- تساعد أنظمة المراقبة في اكتشاف الأنشطة غير الاعتيادية في المؤسسات المصرفية، مثل التحويلات الكبيرة غير المتوقعة أو تسجيل الدخول من مواقع غير معتادة (Zahrawi & Shaalan, 2023).
- يمكن لأنظمة المراقبة المدعومة بالذكاء الاصطناعي تحليل الأنماط السلوكية للعملاء والموظفين، مما يساعد في تحديد السلوكيات المشبوهة واتخاذ الإجراءات اللازمة (Zahrawi & Shaalan, 2023).
- تساهم كاميرات المراقبة في الحد من جرائم سرقة السيارات والتخريب في المواقف والمرائب، وتوفر أدلة حاسمة في التحقيقات الجنائية (Cuevas et al., 2016).
- تلعب أنظمة المراقبة دوراً هاماً في مكافحة غسل الأموال من خلال مراقبة المعاملات المالية، والكشف عن الأنشطة المشبوهة التي قد تشير إلى غسل الأموال أو الاحتيال أو الجرائم المالية الأخرى (Alghamdi et al., 2023).

2.5 التكامل بين أنظمة المراقبة والأمن السيبراني:

في العصر الرقمي الحالي، أصبح التكامل بين أنظمة المراقبة والأمن السيبراني ضرورة حتمية للمؤسسات المصرفية لحماية أصولها المادية والرقمية. يهدف هذا التكامل إلى توفير رؤية شاملة للتهديدات الأمنية والاستجابة لها بشكل فعال (Saudi National Cybersecurity Authority, 2024).

2.5.1 أهمية الربط بين أنظمة المراقبة وأنظمة الأمن السيبراني:

1. تعزيز الحماية الشاملة: يوفر الربط بين أنظمة المراقبة المرئية وأنظمة الأمن السيبراني طبقة حماية إضافية تتجاوز الحماية التقليدية، حيث يمكن لأنظمة المراقبة اكتشاف التهديدات المادية مثل التسلل أو السرقة، بينما

تحمي أنظمة الأمن السيبراني من الهجمات الإلكترونية (Saudi National Cybersecurity Authority, 2024);
(Alohali et al., 2022).

2. تحسين الاستجابة للحوادث: يساعد التكامل في تحسين الاستجابة للحوادث الأمنية من خلال توفير معلومات دقيقة وفورية حول طبيعة الحادث وموقعه، مما يتيح لفرق الأمن اتخاذ الإجراءات المناسبة بسرعة وفعالية (Alghamdi, Alshahrani, & Al-Masabi, 2023). على سبيل المثال، عند حدوث تسلسل إلى مبنى المؤسسة، يتم إطلاق إنذار، وغلق الأبواب، وتوجيه الكاميرات إلى مكان الحادث، وإخطار الجهات الأمنية في وقت قليل جداً (Saudi National Cybersecurity Authority, 2024).
3. تقليل الإنذارات الكاذبة: يمكن لأنظمة الذكاء الاصطناعي تحليل بيانات الفيديو من كاميرات المراقبة لتحديد التهديدات الحقيقية وتصفية الإنذارات الكاذبة، مما يوفر الوقت والجهد على فرق الأمن (Alghamdi, Alshahrani, & Al-Masabi, 2023).
4. الامتثال التنظيمي: يساعد التكامل المؤسسات المصرفية على الامتثال للوائح والمعايير الأمنية المحلية والدولية، والتي تتطلب حماية شاملة للأصول المادية والرقمية (GOV.SA, 2025).

2.6 استراتيجيات الأمن المتكاملة:

1. توحيد أنظمة الأمن: يجب على المؤسسات المصرفية توحيد أنظمة الأمن المختلفة في نظام مركزي واحد، مما يتيح إدارة ومراقبة جميع جوانب الأمن من مكان واحد (Alghamdi, Alshahrani, & Al-Masabi, 2023 Saudi National Cybersecurity Authority, 2022).
2. تحليل البيانات المشترك: يجب أن تتشارك أنظمة المراقبة والأمن السيبراني في تحليل البيانات للكشف عن الأنماط المشبوهة والتهديدات المحتملة (Alghamdi et al., 2023). على سبيل المثال، يمكن ربط بيانات تسجيل الدخول غير المعتادة على الشبكة مع لقطات الفيديو لتحديد ما إذا كان هناك نشاط مشبوه يحدث في الموقع الفعلي (Saudi National Cybersecurity Authority, 2024).
3. أتمتة الاستجابة للحوادث: يمكن أتمتة بعض الإجراءات الأمنية استجابةً للحوادث، مثل إغلاق الأنظمة المخترقة أو تنبيه فرق الأمن (Saudi National Cybersecurity Authority, 2024).

4. التدريب والتوعية: يجب تدريب الموظفين على أهمية الأمن المتكامل وكيفية التعرف على التهديدات والإبلاغ عنها (Saudi National Cybersecurity Authority, 20).

2.6 التحديات المرتبطة بأنظمة كاميرات المراقبة:

على الرغم من الفوائد العديدة التي توفرها أنظمة كاميرات المراقبة، إلا أنها تواجه عدداً من التحديات التي يجب معالجتها لضمان فعاليتها وحماية الحقوق الفردية (Fernández-Caramés et al., 2023). تشمل هذه التحديات المخاطر الأمنية المرتبطة بالأنظمة ومسائل الخصوصية وحماية البيانات (Alkhalil et al., 2023).

2.7.1 المخاطر الأمنية المرتبطة بالأنظمة:

1. الاختراق والوصول غير المصرح به: يمكن للمتسللين اختراق أنظمة كاميرات المراقبة والوصول إلى لقطات الفيديو الحية أو المسجلة، مما يعرض أمن المؤسسة والأفراد للخطر (Fernández-Caramés et al., 2023). يجب على الشركات اتخاذ خطوات لحماية كاميرات المراقبة الخاصة بها من المتسللين، بما في ذلك تغيير كلمات المرور الافتراضية وتحديث البرامج بانتظام (Fernández-Caramés et al., 2023).
2. هجمات حجب الخدمة (DoS): يمكن للمهاجمين شن هجمات حجب الخدمة على أنظمة كاميرات المراقبة، مما يعطل عملها ويمنعها من تسجيل الأحداث المهمة (Fernández-Caramés et al., 2023).
3. البرامج الضارة: يمكن أن تصاب أنظمة كاميرات المراقبة بالبرامج الضارة، مما قد يؤدي إلى تلف البيانات أو تعطيل النظام بأكمله (Alkhalil et al., 2023).
4. التصيد الاحتيالي: يمكن للمهاجمين استخدام رسائل البريد الإلكتروني أو الرسائل النصية للتصيد الاحتيالي لخداع المستخدمين للكشف عن معلومات تسجيل الدخول الخاصة بهم، مما يتيح لهم الوصول إلى أنظمة كاميرات المراقبة (Fernández-Caramés et al., 2023).

2.7.2 مسائل الخصوصية وحماية البيانات:

1. انتهاك الخصوصية: يمكن أن تنتهك كاميرات المراقبة خصوصية الأفراد إذا تم استخدامها لتسجيل الأنشطة في الأماكن الخاصة أو لتتبع تحركات الأفراد دون علمهم أو موافقتهم (Fernández-Caramés et al., 2023).

2. تخزين البيانات: يجب على المؤسسات المصرفية تخزين لقطات الفيديو بشكل آمن ومنع الوصول غير المصرح به إليها. يجب أيضًا وضع سياسات واضحة بشأن مدة الاحتفاظ بالبيانات وكيفية التخلص منها بشكل آمن (Alkhalil et al., 2023).
3. الاستخدام غير المصرح به للبيانات: يجب على المؤسسات المصرفية التأكد من أن لقطات الفيديو لا تستخدم لأغراض أخرى غير الأغراض الأمنية المصرح بها، مثل التسويق أو المراقبة غير القانونية للموظفين (Alkhalil et al., 2023).
4. الشفافية والمساءلة: يجب على المؤسسات المصرفية أن تكون شفافة بشأن استخدامها لأنظمة كاميرات المراقبة وإعلام الأفراد بوجود الكاميرات وأغراضها. يجب أيضًا وضع آليات للمساءلة لضمان عدم إساءة استخدام الأنظمة (Fernández-Caramés et al., 2023).
5. حماية البيانات الحساسة: يجب على الشركات تشفير بيانات كاميرات المراقبة لحمايتها من الوصول غير المصرح به. يجب أيضًا التأكد من أن لديها سياسات وإجراءات معمول بها لحماية البيانات الحساسة، مثل معلومات العملاء (Fernández-Caramés et al., 2023).

2.8 السياق المحلي: البنك العربي الوطني:

في هذا الجزء، سيتم التركيز على دراسة تطبيقية حول كيفية استخدام البنك العربي الوطني لأنظمة كاميرات المراقبة، وتقييم فعالية هذه الأنظمة في السياق المحلي للمملكة العربية السعودية (SAMA Research Department, 2024).

2.8.1 استراتيجيات البنك العربي الوطني في استخدام أنظمة المراقبة:

1. تغطية شاملة للفروع وأجهزة الصراف الآلي: يقوم البنك العربي الوطني بتغطية جميع فروعه وأجهزة الصراف الآلي بأنظمة كاميرات مراقبة متطورة لضمان أمن العملاء والموظفين والممتلكات (SAMA Research Department, 2024).
2. استخدام تقنيات متقدمة: يعتمد البنك على أحدث التقنيات في أنظمة المراقبة، مثل كاميرات IP عالية الدقة، وأنظمة التسجيل الرقمي، وبرامج تحليل الفيديو الذكية (Sijan et al., 2022).

3. المراقبة المركزية: يتم ربط جميع كاميرات المراقبة في نظام مركزي واحد يسمح لموظفي الأمن بمراقبة جميع الفروع وأجهزة الصراف الآلي من موقع واحد (Sijan et al., 2022).
4. التكامل مع أنظمة الإنذار: يتم دمج أنظمة كاميرات المراقبة مع أنظمة الإنذار الأخرى، مثل أنظمة إنذار السرقة وأنظمة التحكم في الوصول، لتوفير نظام أمني متكامل (Sijan et al., 2022).
5. التدريب والتأهيل: يحرص البنك على تدريب وتأهيل موظفي الأمن على استخدام أنظمة كاميرات المراقبة وتحليل لقطات الفيديو والتعامل مع الحوادث الأمنية (SAMA Research Department, 2024).

2.8.2 تقييم فعالية الأنظمة في السياق المحلي:

1. تقليل الجرائم: تساهم أنظمة كاميرات المراقبة في تقليل الجرائم المصرفية، مثل السرقات والاحتيال والتخريب، من خلال توفير رادع قوي للمجرمين وتوثيق الأدلة في حالة وقوع جريمة (Sijan et al., 2022).
 2. تحسين الاستجابة للحوادث: تساعد أنظمة المراقبة في تحسين الاستجابة للحوادث الأمنية من خلال توفير معلومات دقيقة وفورية حول طبيعة الحادث وموقعه، مما يتيح لفرق الأمن اتخاذ الإجراءات المناسبة بسرعة وفعالية (Sijan et al., 2022).
 3. تعزيز ثقة العملاء: تساهم أنظمة كاميرات المراقبة في تعزيز ثقة العملاء في البنك من خلال توفير بيئة آمنة ومأمونة لإجراء المعاملات المصرفية (SAMA Research Department, 2024).
 4. الامتثال للوائح: تساعد أنظمة كاميرات المراقبة البنك على الامتثال للوائح والمعايير الأمنية المحلية والدولية (SAMA Research Department, 2024).
 5. دراسة تطبيقية: يمكن إجراء دراسة تطبيقية لتقييم فعالية أنظمة كاميرات المراقبة في البنك العربي الوطني من خلال تحليل بيانات الجرائم والحوادث الأمنية قبل وبعد تركيب الأنظمة، وإجراء استطلاعات للرأي لقياس رضا العملاء والموظفين عن مستوى الأمان (SAMA Research Department, 2024).
- تُعد أنظمة كاميرات المراقبة أداة أساسية لتعزيز الأمن في المؤسسات المصرفية، حيث تُساهم في حماية الأصول وضمان سلامة العملاء والموظفين. مع التطورات التكنولوجية، انتقلت هذه الأنظمة من التناظرية إلى الرقمية، مُعززةً بتقنيات الذكاء الاصطناعي، مما زاد من فعاليتها في ردع الجرائم وتوفير الأدلة.

على الرغم من فوائدها، تواجه أنظمة المراقبة تحديات تتعلق بالخصوصية وحماية البيانات، مما يتطلب التزام المؤسسات بالقوانين والتشريعات. يُظهر البنك العربي الوطني نموذجًا ناجحًا في استخدام هذه الأنظمة لتعزيز الأمان والثقة بين العملاء.

2.9 الدراسات السابقة:

من خلال هذا القسم سوف نتناول فيه الدراسات السابقة وما يميز هذه الدراسة عن الدراسات السابقة.

2.9.1 الدراسات العربية:

1. دراسة (العامري، 2025) بعنوان: "دراسة شاملة حول تقنيات الكشف عن الأجسام الثقيلة والمراقبة: تفصيلية مختصرة".

هدفت هذه الدراسة إلى تقديم مراجعة منهجية لأحدث تقنيات الكشف عن الأجسام (Object Detection) المستخدمة في أنظمة المراقبة الأمنية، وخاصة في البيئات التي تتطلب تحليلًا فوريًا لحركة الأجسام المشبوهة، مثل البنوك والمنشآت الحيوية. ركز الباحث فيصل العامري على تتبع تطور خوارزميات الرؤية الحاسوبية من الطرق التقليدية مثل HOG و Viola-Jones إلى الأساليب المعتمدة على التعلم العميق مثل YOLO و SSD و Fast R-CNN، مشيرًا إلى أن نماذج YOLO تحديدًا تتميز بالكفاءة العالية والدقة، مما يجعلها مناسبة للتطبيق في البيئات المصرفية ذات الكثافة الحركية المرتفعة.

اعتمدت الدراسة على المنهج الوصفي التحليلي من خلال مراجعة أكثر من 80 دراسة وتجربة مقارنة أداء النماذج في بيئات واقعية تتضمن ضعف الإضاءة، الزحام، والزوايا غير المباشرة. كما ناقشت الدراسة إمكانيات دمج الذكاء الاصطناعي التوليدي (Generative AI) والخوارزميات الميتاهوريستية (مثل PSO و GA) في تحسين أداء أنظمة المراقبة.

أبرزت النتائج أن الدمج بين خوارزميات التعلم العميق وخوارزميات التحسين التكرارية يُنتج أنظمة أكثر استجابة ومرونة، خصوصًا في اكتشاف الحالات غير الطبيعية والتصرفات العدائية.

وأوصت الدراسة بضرورة تبني هذه النماذج في البيئات المصرفية لدعم كفاءة الأمن الوقائي والتقليل من الإنذارات الكاذبة، كما نادت بإنشاء إطار معياري لتقييم أداء هذه الأنظمة في مختلف البيئات.

2. دراسة (وزارة الداخلية السعودية، 2022) بعنوان: "نظام كاميرات المراقبة الأمنية للبنوك والمؤسسات المالية في المملكة العربية السعودية".

هدفت هذه الدراسة الرسمية إلى تحليل أثر تطبيق نظام كاميرات المراقبة على أمن وسلامة المؤسسات المصرفية والمالية، عبر عرض المتطلبات التقنية والتشغيلية والنتائج الأمنية المتحققة.

اعتمدت الدراسة على المنهج الوصفي التحليلي، مستندة على نظام معتمد من وزارة الداخلية صدر في ديسمبر 2022، يلزم البنوك والمؤسسات المالية بطرق تشغيل دقيقة لكاميرات المراقبة، تشمل تغطية شاملة لمحيط البنك والفرع بما فيها الصرافات والمداخل الرئيسية، استخدام كاميرات عالية الدقة وتسجيل مباشر بمعدل ≤ 25 إطاراً/ثانية، تشغيل الإنذار المفعّل بالحركة، مع عرض الوقت والتاريخ المتناسق محلياً، الاحتفاظ بالتسجيلات لفترات محددة: 180 يوماً داخل الفرع، 90 يوماً حول أجهزة الصراف، 30 يوماً في المحيط الخارجي، ربط الكاميرات بغرف المراقبة الأمنية أو محطات الإنذار الحكومية المرخصة، مع فرض غرامات مالية كبيرة للمخالفين.

أظهرت الدراسة أن التطبيق الفاعل لهذا النظام أدى إلى رفع دقة مراقبة النشاط المحيط بالبنوك وتعزيز القدرة على كشف التسلل أو الاعتداء، دعم التحقيقات الأمنية من خلال توفر تسجيلات دقيقة وموثقة، تعزيز الردع الأمني عبر نشر الكاميرات في المواقع الحساسة مع ضمان آلية تشغيل منظّمة، رفع مستوى ثقة العملاء والموظفين بوجود نظام رقابي فعال يلبي معايير الأمان الرسمية.

وأوصت الدراسة برفع جودة البنية التحتية الأمنية في البنوك لتعزيز التغطية وتلافي الثغرات، تحديث الكاميرات ونظم التسجيل لتقنيات عالية الدقة والذكاء الاصطناعي، ضبط إجراءات التشغيل والتعليمات الفنية بوضوح لضمان موثوقية واستغلالات أمنية فعلية للنظام.

3. دراسة (الزهرراوي والشعلان، ٢٠٢٣) بعنوان: "تحسين أنظمة المراقبة بالفيديو في البنوك باستخدام تقنيات التعلم العميق".

هدفت هذه الدراسة إلى تعزيز فعالية أنظمة كاميرات المراقبة داخل البنوك من خلال استخدام تقنيات تعلم عميق للكشف التلقائي عن الأسلحة، مما يُمكن الحراس أو نظم الأمان من الاستجابة الفورية لمنع عمليات السلب المسلح.

اعتمد الباحثان على المنهج الوصفي التحليلي، مطورين إطاراً للكشف المبكر عن الأسلحة باستخدام نماذج رائدة في الوقت الفعلي مثل YOLO وSSD. ركّزوا بشكل خاص على تقليل الإنذارات الكاذبة لضمان ملائمة النظام للتطبيقات الحقيقية داخل البنوك ومواقع مماثلة.

تم اختبار النموذج على فيديوهات مراقبة فعلية لكاميرات داخلية في بيئات مصرفية، كما قابله اختبارات أولية على كاميرات خارجية. أظهر النظام دقة عالية في التعرف المبكر على الأسلحة ضمن المشاهد الحية، مع معدلات إنذار زائفة منخفضة، مما يعزز القدرة الوقائية لأمن المنشآت المصرفية.

وأبرزت الدراسة أهمية الدمج بين التعلم العميق وتقنيات كشف الأشياء في تعزيز قدرات المراقبة الأمنية داخل القطاع البنكي، وخاصة فيما يتعلق بالكشف السريع عن الأسلحة قبل وقوع الجريمة. كما أكدت على ضرورة إجراء اختبارات حية موسعة وتحديث النماذج لتحسين الأداء المستمر.

وأوصى الباحثان بتطبيق هذا الإطار ضمن الأنظمة الأمنية للبنوك، وتطويره ليشمل أسلحة أخرى والشخصيات المشتبه بها، بالاستفادة من تقنيات التعلم العميق الأكثر تقدماً لضمان حماية فعالة وشاملة.

4. دراسة (ربيع، 2024) بعنوان: "أثر تبني البنوك لحلول التكنولوجيا الرقابية على فعالية هيكل الرقابة والمراجعة الداخلية: دراسة تجريبية".

هدفت هذه الدراسة إلى تحليل فعالية أنظمة التكنولوجيا الرقابية، بما فيها كاميرات المراقبة، في تعزيز الرقابة الداخلية وأداء المراجعة داخل البنوك المصرية. ركزت على تقييم دور هذه الحلول التكنولوجية في تحسين فعالية الهيكل الأمني المؤسسي، وتقليل الاعتماد على الرقابة اليدوية.

اعتمدت الدراسة المنهج التجريبي التحليلي، من خلال دراسة حالتين افتراضيتين في بنكين مصريين، باستخدام الاستبانات وتحليل البيانات بواسطة برنامج SPSS الإصدار 29. واستهدفت الدراسة الكوادر المختصة من أقسام تكنولوجيا المعلومات والرقابة الداخلية والمراجعة.

أظهرت النتائج وجود أثر إيجابي وذو دلالة إحصائية لتبني التكنولوجيا الرقابية مثل أنظمة الكاميرات الرقمية، وأنظمة التنبيه الذكي، وأنظمة التحكم في الوصول على تعزيز فعالية الرقابة الداخلية والمراجعة داخل المؤسسات البنكية. وقد استخلص أن هذه الحلول تسهم في رفع دقة الرصد، وتسريع الاستجابة للحوادث، وتقليل الأخطاء البشرية والانحرافات المحتملة .

وأوصت الدراسة بضرورة دمج التكنولوجيا الرقابية داخل خطط الرقابة الداخلية الرسمية للبنوك، وتبني برامج تدريبية للعاملين على استخدامها بكفاءة، فضلاً عن تعزيز التعاون بين أقسام تقنية المعلومات والرقابة الداخلية لضمان تكامل فعال وسلس. كما دعت الباحثة لإجراء أبحاث مقارنة تمتد إلى مؤسسات مالية أخرى لتعميم النتائج.

5. دراسة (شريك، 2024) بعنوان: "تعزيز الأمن السيبراني في القطاع المصرفي المغربي: التكامل الاستراتيجي للذكاء الاصطناعي والبلوك تشين وذكاء الأعمال".

هدف الدراسة الى تحليل دور التقنيات الرقمية المتقدمة—بما في ذلك تقنيات الذكاء الاصطناعي المطبقة على تحليل الفيديوهاات الأمنية وتكوين إنذارات ذكية—في تعزيز الأمن السيبراني والوقاية في البنوك المغربية.

اتبعت الدراسة المنهج الوصفي التحليلي المستند إلى مراجعة الأدبيات والتقارير الخاصة بالأمن البنكي المغربي، مع تحليل تقني للأطر الاستراتيجية التي تجمع بين الذكاء الاصطناعي، البلوك تشين، وتحليلات الأعمال في منظومة أمنية متكاملة.

أظهرت الدراسة أن دمج الذكاء الاصطناعي مع تحليل الأنشطة السيبرانية وسجلات الفيديو يعزز قدرة الكشف المبكر عن التهديدات، ساعد إدخال تقنية البلوك تشين في تأمين سلامة وتسلسل التسجيلات، ما يجعلها غير قابلة للتعديل ويعزز من الأطراف الرقابية، مكنت تقنيات ذكاء الأعمال من معالجة البيانات الأمنية الضخمة عبر بنية التحليلات الذكية لاتخاذ قرارات أمنية مبنية على البيانات.

أوصت الدراسة على اعتماد أنظمة كشف تحليلات الفيديو الذكية ضمن الكاميرات الأمنية المصرفية، لدعم الاستجابة الفورية، دمج آليات التوثيق اللامركزي عبر البلوك تشين في سجل تسجيلات الفيديو لمنع التلاعب وضمان الأمان القانوني، إطلاق منصات تحليل أمنية متقدمة (SIEM و BI) لدعم فرق الأمن السيبراني في التصدي للتهديدات المتقدمة.

6. دراسة (البنك المركزي السعودي، 2023) بعنوان: "اشتراط كاميرات متلفزة لمراقبة البنوك"

تهدف هذه الدراسة إلى وضع إطار تنظيمي موحد لتركيب وتشغيل أنظمة المراقبة التلفزيونية (CCTV) في المؤسسات المالية بالمملكة العربية السعودية، بهدف تعزيز مستويات الأمان والرقابة الوقائية.

اعتمدت الدراسة على المنهج الوصفي التحليلي، من خلال مراجعة وتقييم الإجراءات التنظيمية والتقنية، وتشمل تحديد مواقع تركيب الكاميرات (مداخل/مخارج، موقف السيارات، أجهزة الصراف الآلي)، وضع مواصفات للأجهزة (جودة التسجيل، سرعة الإطارات، تشغيل الإنذار الحراري بتاريخ ووقت)، تحديد فترة الاحتفاظ بالتسجيلات حسب المكان (داخل الفرع - 180 يوماً)، (حول جهاز الصراف الآلي - 90 يوماً)، (خارجياً - 30 يوماً).

أظهرت النتائج أن تنفيذ هذه المواصفات يساهم في تعزيز التغطية الأمنية عبر كاميرات عالية الجودة وتركيب شامل، دعم التحقيقات الجنائية بتوفر تسجيلات دقيقة، رفع مستوى الردع الأمني وضمان التزام البنوك بتنظيم المراقبة بالفيديو، تحسين مستوى الثقة والاطمئنان لدى العملاء تجاه أمن التعاملات البنكية.

أوصت الدراسة على تطبيق فوري لتغطية الكاميرات حسب المواصفات في جميع البنوك، توحيد ضبط الوقت والتاريخ في نظم البث والتسجيل، تركيب أنظمة إنذار مرتبطة بالكاميرات، ضمان وصول التسجيلات لغرف أمنية مركزية أو مرخصة للاطلاع فور الحاجة.

2.9.2 الدراسات الأجنبية:

1. دراسة (Quinn Dennis P. Cuevas et al., 2016) بعنوان "التصميم والتكوين والاستخدام الفعال لكاميرات

المراقبة الرقمية". "Effective design, configuration, and use of digital CCTV"

هدفت هذه الدراسة إلى تحديد فعالية كاميرات المراقبة التلفزيونية المغلقة في مدينة باتانجاس ودورها في منع الجريمة، مع التركيز على مخالفات المرور والجرائم ضد الممتلكات والأشخاص. تكون مجتمع الدراسة من 150 مشاركاً تم اختيارهم عشوائياً، شمل الموظفين الإداريين ومشغلي كاميرات المراقبة وضباط الشرطة.

اعتمدت الدراسة على منهج البحث الوصفي، حيث تم جمع البيانات من خلال استبيان ذاتي الصنع. أظهرت النتائج أن كاميرات المراقبة كانت فعالة للغاية في منع الجرائم، خاصة الجرائم ضد الأشخاص والممتلكات، من خلال تسجيل المشاهد التي تساهم في حل حوادث السرقة أو السطو.

كما أكدت الدراسة على أهمية التعرف على الشخصيات المشبوهة ومراقبة الأفراد الذين يدخلون ويخرجون من المؤسسات.

أوصت الدراسة بضرورة تعزيز استخدام كاميرات المراقبة في مختلف القطاعات، وتطوير خطط عمل تعتمد على نتائج البحث لتحسين فعالية أنظمة المراقبة في منع الجريمة.

2. دراسة (Tan, Abbas, and Shafie, 2021) بعنوان: "مراجعة منهجية للأدبيات حول منع الجريمة من خلال

مبادئ التصميم البيئي، مقارنةً بفعالية الأمن المادي لأجهزة الصراف الآلي للبنوك"

"A systematic literature review of crime prevention through environmental design principles against banks ATM physical security effectiveness"

هدفت الدراسة إلى تحليل فعالية الأمن المادي لأجهزة الصراف الآلي للبنوك، من خلال مراجعة الأدبيات العلمية التي تناولت مبادئ التصميم البيئي كأداة لمنع الجريمة في القطاع المصرفي. اعتمد الباحثون المنهج الكيفي القائم على المراجعة المنهجية للأدبيات (SLR) لتحليل الدراسات المنشورة في المكتبة الرقمية عبر الإنترنت، وذلك بهدف تقييم مدى فعالية الضوابط الأمنية المادية في بيئة مصرفية تتطور باستمرار بفعل الابتكار التكنولوجي.

اشتملت عملية المراجعة على تحليل عدة عناصر تؤثر في الوضع الأمني، مثل أنظمة التحكم، وبيئة الموقع، وسلوك الأفراد، وعوامل المحيط، وذلك في ضوء التحول نحو النظام البيئي المالي الرقمي. وقد أكدت الدراسة على أن تزايد اعتماد العملاء على الخدمات المصرفية الإلكترونية والأجهزة الآلية، يفرض تحديات أمنية جديدة تتطلب إعادة تقييم مستمرة لسياسات الأمان والتصميم البيئي.

أظهرت النتائج أن هناك علاقة وثيقة بين جودة مبادئ التصميم البيئي وبين كفاءة الأنظمة الأمنية في حماية أجهزة الصراف الآلي من السلوكيات الإجرامية. كما خلصت الدراسة إلى ضرورة إجراء مراجعات دورية للمبادئ والإطار المعياري للمراقبة الأمنية، وذلك لضمان فعالية الإجراءات الوقائية في مواجهة التهديدات المستجدة.

وأوصت الدراسة بتبني منهج تكاملي يجمع بين التصميم البيئي والتكنولوجيا المتقدمة لتعزيز أمن المنشآت المصرفية، مع التأكيد على أهمية مواكبة التحولات الرقمية وتطور سلوكيات المستخدمين في البيئة المصرفية.

3. دراسة (Bisati, Astia, and Chauhan, 2024) بعنوان: "مراجعة متعمقة لكشف الجرائم باستخدام الذكاء

الاصطناعي في مقاطع فيديو كاميرات المراقبة". "A Profound Review of AI-Driven Crime Detection In

"CCTV Videos

هدفت هذه الدراسة إلى تحليل فعالية استخدام تقنيات الذكاء الاصطناعي في أنظمة كاميرات المراقبة لكشف الجرائم المختلفة، من خلال مراجعة شاملة للدراسات والمنهجيات الحديثة خلال السنوات الخمس الماضية. استعرضت الدراسة مدى كفاءة خوارزميات الذكاء الاصطناعي، خاصة خوارزميات التعلم العميق، في التعرف على الأنماط الإجرامية وتحليل مقاطع الفيديو الخاصة بأنظمة المراقبة في المواقع العامة مثل البنوك، الأسواق، المستشفيات، الشوارع، وغيرها.

اعتمدت الدراسة على المنهج الوصفي التحليلي عبر المراجعة المنهجية للأدبيات المنشورة في قواعد بيانات رقمية، حيث تم تحليل بيانات ومخرجات دراسات مقارنة تناولت فعالية خوارزميات الذكاء الاصطناعي في اكتشاف أنواع متعددة من الجرائم مثل السرقة، السطو، العنف، وجرائم الشوارع. كما أولت الدراسة اهتماماً خاصاً بتحديات كشف الشذوذات في مقاطع الفيديو مثل تعقيد النشاط البشري، ضعف الإضاءة، تنوع البيئات، وغياب مجموعات البيانات القياسية.

أظهرت نتائج الدراسة تفوق خوارزميات التعلم العميق على باقي الأساليب التقليدية في اكتشاف الجرائم وتحليل السلوك الإجرامي من خلال الفيديوها. كما أكدت على أهمية وجود مجموعات بيانات عالية الجودة ومتنوعة لتدريب النماذج، وتطوير حلول ذكاء اصطناعي يمكن الاعتماد عليها في أنظمة المراقبة الأمنية.

وأوصت الدراسة بضرورة استمرار البحث والتطوير في هذا المجال، وتحديث أنظمة المراقبة الأمنية في المنشآت الحساسة مثل المؤسسات المصرفية، بحيث تدمج خوارزميات الذكاء الاصطناعي مع التصميمات الأمنية التقليدية، مما يساهم في رفع كفاءة اكتشاف التهديدات وتقليل زمن الاستجابة الأمنية.

4. دراسة (John, Kim, Kim, and Kim, 2024) بعنوان: "PASS-CCTV: نظام مراقبة استباقي لاكتشاف الشذوذ في لقطات كاميرات المراقبة ضمن ظروف بيئية قاسية"

"PASS-CCTV: Proactive Anomaly surveillance system for CCTV footage analysis in adverse environmental conditions"

هدفت هذه الدراسة إلى تطوير نظام مراقبة ذكي قائم على الذكاء الاصطناعي لتحليل فيديوها كاميرات المراقبة في ظل الظروف البيئية المتغيرة والمعقدة، مثل ضعف الإضاءة، الأمطار، وتعدد زوايا التصوير، وهي عوامل غالباً ما تعيق دقة أنظمة التتبع التقليدية. ركز الباحثون على تصميم نظام استباقي قادر على اكتشاف الشذوذات السلوكية المختلفة مثل التسلسل، التجول غير المبرر، التخلي عن الأغراض، والحرق العمد.

اعتمدت الدراسة على المنهج الوصفي التحليلي، من خلال تطوير وحدة لتتبع الأجسام البشرية باستخدام تقنيات التعلم العميق، مدعومة بخوارزميات ترشيح مبتكرة لتقليل معدلات الإنذارات الخاطئة، وتحسين دقة التتبع. كما تم تضمين آلية تنبيه ذكية قائمة على "الأوامر الموجهة" (Prompt-based) تُتيح مشاركة المستخدمين في تحديد السيناريوهات غير الطبيعية بشكل مباشر.

تم اختبار النظام باستخدام بيانات حقيقية من كاميرات المراقبة ضمن قواعد بيانات مثل قاعدة KISA (الوكالة الكورية للإنترنت والأمن)، بالإضافة إلى قواعد ABODA و FireNet، حيث أظهرت النتائج دقة عالية وأداءً متقدماً حتى دون الحاجة لتدريب إضافي، وهو ما يعكس قدرة النظام على التكيف مع مختلف البيئات التشغيلية.

وأبرزت الدراسة أهمية تعزيز أنظمة المراقبة الأمنية بقدرات استباقية تعتمد على الذكاء الاصطناعي لتقليل التكاليف التشغيلية، وزيادة مرونة النظام في رصد التهديدات الفورية في الوقت الفعلي، خصوصاً في البيئات المعرضة للتغيرات الجوية أو ذات البنى التحتية غير المستقرة.

وأوصى الباحثون بضرورة اعتماد مثل هذه الأنظمة في المؤسسات العامة والحيوية مثل البنوك، ومحطات النقل، والمراكز الحكومية، لما لها من أثر مباشر في تحسين الاستجابة الأمنية وتقليل الاعتماد على التدخل البشري.

5. دراسة (Vinnam, Pramod, Thepaswamy, & Kim, 2021) بعنوان: "هجمات وإجراءات الحماية على أنظمة المراقبة بالفيديو: مراجعة تحليلية" "Attacks and Preventive Measures on Video Surveillance Systems: A Review"

هدفت هذه الدراسة إلى تقديم مراجعة تحليلية شاملة لأنواع الهجمات الإلكترونية التي تستهدف أنظمة المراقبة بالفيديو (VSS)، مع استعراض الإجراءات الوقائية الممكنة لحماية هذه الأنظمة، خصوصاً في ظل التوسع الكبير في استخدامها في المنشآت العامة والخاصة، مثل البنوك والمطارات والشوارع ومراكز المدن. اعتمدت الدراسة على المنهج الوصفي التحليلي، حيث قام الباحثون بتحليل أبرز أنواع الهجمات الأمنية التي يمكن أن تتعرض لها أنظمة المراقبة، ومنها:

هجمات طبقة الصور (Visual Layer) مثل التلاعب في البث الحي عن طريق تكرار الإطارات (Frame Duplication)، الهجمات عبر القنوات السرية (Covert Channels) التي تستخدم تقنيات مثل الاستيجانوجرافي والتحكم بالأشعة تحت الحمراء، هجمات الحرمان من الخدمة (DoS & Jamming) والتي تؤدي إلى تعطيل كاميرات المراقبة مؤقتاً أثناء الأحداث الأمنية الحرجة، الهجمات عبر امتيازات الوصول (Privilege Escalation) والتي تستهدف تجاوز الصلاحيات الأمنية للولوج إلى معلومات حساسة، بالإضافة إلى هجمات البرمجيات الخبيثة (Malware) مثل فيروس Mirai الذي استهدف الكاميرات المتصلة بالإنترنت.

كما تناولت الدراسة التهديدات المرتبطة بالخصوصية، خاصة في كاميرات الـ IP المرتبطة بالإنترنت، والتي قد تكون عرضة للاختراق عبر تطبيقات أو خدمات غير آمنة. أوضحت الدراسة أن استخدام كلمات مرور افتراضية، وعدم تحديث البرمجيات، وضعف إعدادات الأمان، تعتبر من أبرز أسباب اختراق الأنظمة.

استعرض الباحثون أيضاً تطور السوق العالمي لكاميرات المراقبة، مشيرين إلى أن تقنيات إنترنت الأشياء (IoT) ساهمت بشكل كبير في تحويل أنظمة المراقبة التقليدية إلى أنظمة ذكية قادرة على اكتشاف الأحداث وتحليلها آلياً دون تدخل بشري مباشر، لكنها في الوقت نفسه أصبحت أكثر عرضة للهجمات المعقدة.

وأوصت الدراسة بضرورة اعتماد سياسات أمنية صارمة في مراحل تصميم ونشر أنظمة المراقبة، وتطبيق أنظمة كشف التسلسل، والتشفير، والتحقق الثنائي، وتحديث البرمجيات بشكل دوري، إلى جانب التوعية بأمن الخصوصية للمستخدمين.

6. دراسة (Sijan, Shahoriar, Salimullah, Islam, & Khan, 2022) بعنوان: "مراجعة حول أمن الخدمات

المصرفية الإلكترونية في بنغلاديش: دراسة تجريبية". "A Review on E-Banking Security in Bangladesh: "

"An Empirical Study

هدفت هذه الدراسة إلى تحليل الوضع الراهن لأمن الخدمات المصرفية الإلكترونية (E-Banking) في بنغلاديش في ظل التوسع الرقمي السريع الذي تشهده المؤسسات المالية. ركز الباحثون على تقييم التهديدات الأمنية التي تواجه القطاع المصرفي الإلكتروني البنغلاديشي، ومدى فعالية الحلول الوقائية المعتمدة، وذلك في سياق النمو الاقتصادي والتقني الذي يشهده البلد.

اعتمدت الدراسة على المنهج الوصفي التحليلي التجريبي، حيث تم استعراض وتحليل مجموعة من الحوادث الأمنية التي تعرضت لها المؤسسات المصرفية البنغلاديشية، مثل هجمات الاختراق، والاحتيال الإلكتروني، واستغلال الثغرات الأمنية، سواء على مستوى المستخدمين أو الخوادم البنكية. كما تناولت الدراسة مدى تأثير هذه التهديدات ببنية البنية التحتية الرقمية الضعيفة، واستخدام البرمجيات غير المحدثة، ونقص الوعي الأمني لدى المستخدمين.

استعرض الباحثون أبرز المخاطر، مثل: التصيد الاحتيالي، الوصول غير المصرح به، اختراق تطبيقات الهواتف الذكية، هجمات البرامج الخبيثة، انعدام تشفير البيانات في بعض العمليات، ضعف أدوات التوثيق والتحقق.

كما قدمت الدراسة إطاراً مقترحاً لتعزيز أمن الخدمات المصرفية الإلكترونية، يتضمن تحديث السياسات الأمنية، وتبني معايير الحماية الإلكترونية الحديثة، مثل التحقق الثنائي (FA2)، وتوعية المستخدمين، وتكامل الأنظمة

البنكية مع تقنيات الأمن السيبراني الذكية، إضافةً إلى مراجعة القوانين المحلية لضمان تكامل الحلول التقنية مع البيئة القانونية.

أوصى الباحثون بضرورة تبني منهجية وطنية شاملة لأمن المعلومات في القطاع المصرفي، تشمل تحديث البنية التحتية الرقمية، وإنشاء فرق استجابة سريعة للحوادث السيبرانية، وتعزيز التعاون بين البنوك والمؤسسات الحكومية لمواجهة التهديدات المتزايدة في هذا المجال الحيوي.

2.9.3 التعقيب على الدراسات السابقة:

تتناول الدراسات السابقة فعالية أنظمة كاميرات المراقبة في تعزيز أمن المؤسسات المصرفية، مما يبرز أهميتها في مواجهة التهديدات الأمنية المتزايدة. وتشير الدراسات العربية، مثل دراسة العامري (2025) التي تبرز دور تقنيات الكشف الحديثة ودمج الذكاء الاصطناعي، إلى توجه متزايد نحو استخدام هذه الأنظمة بشكل أكثر فعالية. كما توضح دراسة (Saudi Legal Portal, 2022). أهمية الأنظمة التنظيمية في تأمين المؤسسات المالية، وهو ما يتماشى مع الحاجة لتقييم فعالية الأنظمة في السياق المحلي، كما يركز عليه البحث الحالي. من جهة أخرى، تركز الدراسات الأجنبية، مثل دراسة (Quinn et al. 2016) التي تسلط الضوء على دور كاميرات المراقبة في منع الجرائم، على أهمية هذه الأنظمة في المؤسسات المصرفية، بينما تفحص دراسة (Bisati et al. 2024) أثر الذكاء الاصطناعي في كشف الجرائم، مما يعزز من قيمة استخدامها. ومع ذلك، تقدم دراسة (Vinnam et al. 2021) تحليلاً شاملاً للتهديدات الإلكترونية، مما يثير النقاش حول التحديات الأمنية التي تواجه البنك العربي الوطني. بشكل عام، تبرز هذه الدراسات الحاجة الملحة لتقييم فعالية أنظمة المراقبة في السياق المحلي، وهو ما يسعى البحث الحالي لتحقيقه، مما يساهم في تطوير استراتيجيات أمنية متكاملة تعزز من أمان المؤسسات المصرفية.

الخلاصة:

يعد الفصل الثاني من البحث بمثابة الإطار النظري الذي يسلط الضوء على أهمية أنظمة كاميرات المراقبة في تعزيز أمن المؤسسات المصرفية. من خلال تحليل التعريفات والتطورات التاريخية لهذه الأنظمة، تمكنا من فهم كيفية تحولها إلى أدوات حيوية في مواجهة التهديدات الأمنية المتزايدة. تظهر النتائج أن أنظمة كاميرات المراقبة تُساهم بشكل كبير في تعزيز الأمان من خلال ردع الجرائم، وتوثيق الأحداث، وتوفير الأدلة اللازمة للتحقيقات. كما أن إدخال تقنيات

الذكاء الاصطناعي في هذه الأنظمة قد أضاف بعداً جديداً من الفعالية، مما يمكّن المؤسسات من معالجة البيانات بشكل أسرع وأكثر دقة. ومع ذلك، يظل هناك تحديات تتعلق بالخصوصية وحماية البيانات، مما يتطلب من المؤسسات المصرفية الالتزام بالقوانين والتشريعات ذات الصلة، بالإضافة إلى تطوير استراتيجيات شاملة تعزز من الأمان. تتناول الدراسات السابقة التي تم استعراضها في هذا الفصل أهمية هذه الأنظمة، مما يُبرز الحاجة المستمرة لتقييم فعاليتها في السياقات المختلفة. يُظهر البحث الحالي كيف يمكن أن تسهم أنظمة كاميرات المراقبة في تحسين بيئة الأمان داخل المؤسسات المصرفية، وبالتالي تعزيز ثقة العملاء ورفع مستوى الخدمة المقدمة. من خلال هذا الفصل، تم تأسيس قاعدة معرفية قوية تساعد في فهم الدور الحيوي لأنظمة كاميرات المراقبة في تعزيز الأمان، مما يمهد الطريق لمزيد من البحث والدراسة في الفصول التالية.

الفصل الثالث: منهجية وإجراءات الدراسة

تمهيد

يعد الفصل الثالث من هذا البحث محوراً أساسياً لفهم منهجية الدراسة المتبعة في تحليل فعالية أنظمة كاميرات المراقبة في تعزيز أمن البنك العربي الوطني. يتناول هذا الفصل الأساليب البحثية المستخدمة لجمع البيانات وتحليلها، مما يساهم في تحقيق أهداف الدراسة والإجابة عن تساؤلاتها.

تم تصميم هذا الفصل بعناية لوصف الآليات التي سيتم من خلالها جمع المعلومات من عينة متنوعة من موظفي البنك، بما في ذلك موظفي الأمن والإدارة. يعتمد البحث على منهج وصفي تحليلي، وهو منهج معتمد في الدراسات الأكاديمية، يتيح للباحثين استكشاف العلاقات بين المتغيرات وفهم تأثيرها بشكل دقيق.

سيتناول الفصل أيضاً خصائص العينة المستهدفة، وأداة الدراسة المستخدمة في جمع البيانات، بالإضافة إلى الأساليب الإحصائية التي سيتم استخدامها لتحليل النتائج. يهدف هذا التمهيد إلى تقديم إطار عمل متكامل يوضح كيفية معالجة البيانات وتفسير النتائج، مما يساهم في تعزيز المصداقية والموثوقية في النتائج النهائية للدراسة.

من خلال هذا الفصل، يسعى البحث إلى تقديم رؤية شاملة حول كيفية تأثير أنظمة كاميرات المراقبة على الأمن المصرفي، مما يمكن المؤسسات المالية من اتخاذ قرارات مبنية على الأدلة لتحسين استراتيجيات الأمان.

3.1 منهج الدراسة:

تعتمد هذه الدراسة على المنهج الوصفي التحليلي، الذي يعتبر من المناهج البحثية الأساسية المستخدمة في مجال العلوم الاجتماعية، حيث يتيح للباحثين جمع وتحليل البيانات الكمية والنوعية بشكل شامل. يهدف هذا المنهج إلى توضيح فعالية أنظمة كاميرات المراقبة في تعزيز الأمن داخل البنك العربي الوطني، من خلال فهم كيفية تأثير هذه الأنظمة على مستوى الأمان وتفاعلها مع مختلف العوامل الداخلية والخارجية. سيتضمن منهج الدراسة عدة خطوات رئيسية، تبدأ بتصميم أداة جمع البيانات، وهي استبيان مُعد خصيصاً لهذا الغرض. ستتضمن هذه الأداة أسئلة مقسمة إلى قسمين رئيسيين: الأسئلة المغلقة التي ستسمح بجمع بيانات كمية قابلة للتحليل الإحصائي، والأسئلة

المفتوحة التي ستتيح للموظفين التعبير عن آرائهم وتجاربهم بشكل أكثر تفصيلاً. سيتم استخدام الاستبيانات لجمع المعلومات من موظفي الأمن والإدارة، مما يضمن الحصول على رؤية شاملة حول فعالية الأنظمة.

3.2 مجتمع وعينة الدراسة:

تستهدف الدراسة مجتمع الموظفين في البنك العربي الوطني، والذي يتضمن مجموعة متنوعة من الأدوار والمستويات الوظيفية. يشمل هذا المجتمع موظفي الأمن الذين يتعاملون بشكل مباشر مع أنظمة كاميرات المراقبة، بالإضافة إلى موظفي الإدارة الذين يمكنهم تقييم تأثير هذه الأنظمة على الأعمال اليومية. سيتم اختيار عينة عشوائية من 100 موظف، مما يضمن تمثيلاً جيداً لمختلف الأقسام داخل البنك، مثل الأمن، الإدارة، والتقنية.

تضمن العينة تمثيلاً متوازناً بين الجنسين والأعمار، مما يساهم في تعزيز موثوقية النتائج. ستساعد هذه الطريقة في تقليل التحيز وضمان أن تكون البيانات التي يتم جمعها تعكس بشكل دقيق الآراء والتجارب المختلفة للموظفين.

3.3 خصائص العينة:

تتكون العينة من موظفين تتراوح أعمارهم بين 25 و50 عاماً، مما يعكس تنوعاً في الخبرات العملية. تشمل الخلفيات التعليمية للعينة الدرجات الجامعية والدراسات العليا، حيث يُتوقع أن يكون لدى المشاركين مستوى عالٍ من الوعي بالتقنيات الحديثة في مجال الأمن والمراقبة. بالإضافة إلى ذلك، تتضمن العينة موظفين ذوي خبرات عملية تتراوح بين 2 إلى 15 عاماً في المجال المصرفي، مما يمنحهم القدرة على تقييم فعالية أنظمة كاميرات المراقبة من منظور عملي وتجريبي.

ستساعد هذه الخصائص في ضمان أن تكون البيانات المستخلصة غنية بالمعلومات، مما يساهم في تحقيق أهداف الدراسة بشكل أكثر فعالية.

3.4 أداة الدراسة:

سيتم استخدام استبيان معد خصيصاً لجمع البيانات، يتضمن مجموعة من الأسئلة المغلقة التي تستخدم لتقييم جوانب محددة من فعالية أنظمة كاميرات المراقبة وتأثيرها على الأمن. بالإضافة إلى ذلك، ستحتوي الأداة على أسئلة مفتوحة تسمح للمشاركين بالتعبير عن آرائهم وتجاربهم بشكل أعمق. ستشمل الأسئلة جوانب مثل:

- مدى فعالية الكاميرات في ردع الجرائم.

- تقييم جودة الصور والفيديو الملتقط.

- مدى سهولة الوصول إلى البيانات المسجلة.

- التحديات التي يواجهها البنك في تطبيق هذه الأنظمة.

سيتم التأكد من صلاحية الاستبيان من خلال إجراء اختبار تجريبي مع عينة صغيرة، مما يتيح تعديل الأسئلة وفقاً للملاحظات المستخلصة.

3.5 الأساليب الإحصائية:

ستحلل البيانات باستخدام برنامج SPSS، حيث سيتم تطبيق مجموعة من الأساليب الإحصائية المتنوعة للحصول على نتائج دقيقة وموثوقة. تتضمن هذه الأساليب:

- التحليل الوصفي: والذي يُستخدم لوصف خصائص العينة، مثل التوزيع العمري والخلفيات التعليمية. سيوفر هذا التحليل معلومات أساسية حول المشاركين، مما يُساعد في فهم السياق الذي يتم فيه تقييم فعالية الأنظمة.

- اختبار t: هذا الاختبار يُستخدم لمقارنة المتوسطات بين مجموعتين أو أكثر، مما يساعد في تحديد ما إذا كانت هناك فروقات ذات دلالة إحصائية في الآراء حول فعالية أنظمة كاميرات المراقبة بين موظفي الأمن والإدارة.

- التحليل الانحداري: سيتمكن هذا التحليل من تحديد العلاقة بين استخدام كاميرات المراقبة ومستويات الأمان، حيث سيتم فحص كيف تؤثر المتغيرات المختلفة على فعالية هذه الأنظمة.

- التحليل العاملي: يُستخدم لاستكشاف العوامل المؤثرة في فعالية الأنظمة، مما يساعد في تحديد العوامل التي تسهم بشكل أكبر في تعزيز الأمن داخل البنك. سيمكن هذا التحليل الباحثين من فهم كيفية تفاعل العوامل المختلفة مع أنظمة كاميرات المراقبة، مما يعزز من قدرة البنك على تطوير استراتيجيات أمنية أكثر فعالية.

ستساعد هذه الأساليب في تقديم نتائج موثوقة ودقيقة تعكس فعالية أنظمة كاميرات المراقبة في تعزيز الأمن في البنك العربي الوطني. من خلال تحليل البيانات بشكل دقيق، يمكن استنتاج استنتاجات تعزز من فهم كيفية تحسين أنظمة المراقبة الحالية والتعامل مع التحديات المرتبطة بها.

3.6 الأخلاقيات:

تمت مراعاة المعايير الأخلاقية في جميع مراحل البحث، حيث تم الحصول على موافقة المشاركين قبل تعبئة الاستبيانات. تم توضيح هدف الدراسة لهم، بالإضافة إلى التأكيد على سرية المعلومات وعدم استخدامها لأغراض أخرى غير البحث الأكاديمي. تم ضمان أن تكون جميع البيانات المجمعة مُعالجة بشكل يضمن خصوصية الأفراد.

3.7 حدود الدراسة:

1. الحدود الزمنية:

تقتصر الدراسة على فترة زمنية محددة، حيث يتم جمع البيانات خلال العام 2025. قد تؤثر هذه الفترة الزمنية المحددة على النتائج، حيث أن الظروف الأمنية والتكنولوجية قد تتغير بمرور الوقت، مما قد يجعل النتائج غير قابلة للتعميم على المدى البعيد.

2. الحدود المكانية:

تم إجراء الدراسة في البنك العربي الوطني فقط، مما قد يحد من إمكانية تعميم النتائج على مؤسسات مصرفية أخرى في المملكة العربية السعودية أو في دول أخرى. قد تختلف ظروف الأمان والتكنولوجيا من بنك لآخر، مما يؤدي إلى نتائج مختلفة في سياقات أخرى.

3. الحدود الموضوعية:

تركز الدراسة على تقييم فعالية أنظمة كاميرات المراقبة في تعزيز الأمن، مما يعني أن بعض الجوانب الأخرى المتعلقة بالأمن المصرفي، مثل استراتيجيات الأمان السيبراني أو الإجراءات الداخلية، قد لا تُغطى بشكل كافٍ. هذا التركيز قد يحد من فهم شامل لعوامل الأمان في المؤسسات المصرفية.

4. الحدود البشرية:

تستند الدراسة إلى عينة من 100 موظف فقط، مما قد لا يعكس تنوع آراء جميع موظفي البنك. قد تؤثر العوامل الشخصية مثل الخبرة، والوظيفة، والتوجهات الثقافية على آراء المشاركين، مما قد يؤدي إلى تحيز في النتائج. كما أن الاعتماد على استبيانات قد يحد من عمق المعلومات المستخلصة من التجارب الشخصية للموظفين.

الخلاصة:

ختاماً يمثل الفصل الثالث جزءاً أساسياً من الدراسة، حيث يوضح المنهجية التي تم اتباعها لجمع وتحليل البيانات. من خلال استخدام الاستبيان كأداة لجمع البيانات، تهدف هذه الدراسة إلى تحقيق فهم شامل لفعالية أنظمة كاميرات المراقبة في البنك العربي الوطني. ستساهم النتائج المستخلصة من هذه الدراسة في تعزيز استراتيجيات الأمان وتحسين مستوى الحماية في المؤسسات المصرفية، مما يعكس أهمية البحث في هذا المجال الحيوي.

المراجع والمصادر:

• المراجع باللغة العربية:

البنك العربي الوطني. (2023). التقرير السنوي 2023: التحول الرقمي والأمن. تم الاسترجاع في 15 يونيو 2024 من <https://www.alinma.com/wps/wcm/connect/alinma/alinma/general+content+site/Investor+relations/reports/annual+reports>

البنك المركزي السعودي (. (2023). (SAMA) الإطار الأمني السيبراني للمؤسسات المالية. تم الاسترجاع في 18 مايو 2024 من <https://www.sama.gov.sa/ar-sa/mediacenter/pressreleases/Pages/cyber2023.aspx>

العامري، ف. (2025). دراسة شاملة حول كشف الأجسام لأغراض الأمن والمراقبة: مراجعة موجزة. أدوات وتطبيقات الوسائط المتعددة. <https://doi.org/10.1007/s11042-025-20801-6>

الزهرابي، م.؛ شعلان، ك. (2023). تحسين أنظمة المراقبة بالفيديو في البنوك باستخدام تقنيات التعلم العميق. التقارير العلمية، 13(1)، 7911. <https://doi.org/10.1038/s41598-023-35190-9>

ربيع، م. إ. (2024). أثر تبني البنوك لحلول التكنولوجيا الرقابية على فعالية هيكل الرقابة والمراجعة الداخلية- دراسة تجريبية. المجلة العلمية للبحوث التجارية - جامعة المنوفية، 54(3)، الجزء الثاني)، 657-728. https://sjsc.journals.ekb.eg/article_366553.html

شُريك، ش. (2024). تعزيز الأمن السيبراني في القطاع المصرفي المغربي: التكامل الاستراتيجي للذكاء الاصطناعي والبلوك تشين وذكاء الأعمال. أرشيف المجلة الدولية للعلوم والبحوث، 13(2)، 1723-1734. <https://doi.org/10.30574/ijrsra.2024.13.2.2312>

الهيئة السعودية للبيانات والذكاء الاصطناعي (. (2024). (SDAIA) تقرير سوق أنظمة المراقبة في المملكة. تم الاسترجاع في 10 أبريل 2024 من <https://sdaia.gov.sa/ar/strategy/Pages/default.aspx>

الهيئة الوطنية للأمن السيبراني. (2023). الورقة البيضاء: أنظمة إدارة الفيديو المتكاملة. تم الاسترجاع في 22 مارس 2024 من <https://nca.gov.sa/ar/awareness/Documents/VMSSaudi.pdf>

المملكة العربية السعودية. (2025). أنظمة وتشريعات البيانات والأمن السيبراني. تم الاسترجاع في 5 يناير 2025 من <https://my.gov.sa/ar/content/legal-regulatory-framework>

● المراجع باللغة الإنجليزية:

- Abu-Taieh, Evon; Elhadi, Moamin; Al Khaled, Zaher (2024). AI transformation in Arab banking security. *Journal of Financial Services Research*, 65(2), 189–213. <https://doi.org/10.1007/s10693-023-00407-3>
- Al-Almarshad, Ahmed; Al-Salem, Rashed; Al-Harbi, Fahad (2024). Legal aspects of AI surveillance in GCC countries. *Computer Law & Security Review*, 51, 105812. <https://doi.org/10.1016/j.clsr.2023.105812>
- Alghamdi, Rashed; Alshahrani, Mohammed; Al-Masabi, Sultan (2023). An Integrated framework for AI-driven banking security systems. *Journal of Financial Services Research*, 65(3), 301–325. <https://doi.org/10.1007/s10693-023-00412-6>
- Alghamdi, Rashed; Al-Otaibi, Abdullah; Al-Subaie, Mohammed (2023). Real-time transaction fraud detection using federated learning. *Expert Systems with Applications*, 225, 120105. <https://doi.org/10.1016/j.eswa.2023.120105>
- Al-Ghamdi, Ahmed; Al-Mutairi, Naif; Al-Harbi, Saud (2024). Deep learning applications in intelligent bank surveillance. *Journal of Arabian Security*, 15(2), 45–60. <https://doi.org/10.1016/j.jas.2024.03.005>
- Al-Ghamdi, Rashed; Al-Mutairi, Majed; Al-Harbi, Sultan (2024). Cybersecurity vulnerabilities In biometric authentication systems. *Computers & Security*, 136, 103502. <https://doi.org/10.1016/j.cose.2024.103502>
- Alhazmi, Omar; Al-Sarawi, Said (2023). AI-driven security systems In critical Infrastructure: A taxonomy. *Computers & Security*, 128, 103156. <https://doi.org/10.1016/j.cose.2023.103156>
- Alkhalil, Zaid; Al-Mansour, Ahmed; Al-Jabreen, Saleh (2023). Digital security threats In MENA banking sector. *Computers & Security*, 124, 102976. <https://doi.org/10.1016/j.cose.2022.102976>
- Almuqrin, Abdullah; Al-Harhi, Saud; Al-Otaibi, Mohammed (2023). AI-driven transaction monitoring In Saudi banks. *Arabian Journal for Science and Engineering*, 48(5), 6789–6805. <https://doi.org/10.1007/s13369-023-07908-4>

- Alohali, Mana; Al-Nasser, Rami; Al-Shammari, Ahmed (2022). Cyber-physical security integration In banking systems. *Journal of Information Security and Applications*, 68, 103289. <https://doi.org/10.1016/j.jisa.2022.103289>
- Alom, Mohammad Z.; Taha, Tarek M.; Yakopcic, Corey; Westberg, Samuel; Asari, Vijayan K. (2019). Real-time intrusion detection In banking surveillance using deep learning. *IEEE Transactions on Industrial Informatics*, 15(12), 6314–6323. <https://doi.org/10.1109/TII.2019.2946055>
- Alotaibi, Naif; Al-Rashidi, Khalid; Al-Fahad, Laila (2022). Behavioral Impact of surveillance In educational institutions. *Educational Technology Research and Development*, 70(4), 1567–1589. <https://doi.org/10.1007/s11423-022-10130-y>
- Alshammari, Turki; Alwan, Ahmed (2023). Measuring smart CCTV effectiveness in Saudi banking security. *International Journal of Security Technology*, 8(4), 112–130. <https://doi.org/10.1109/IJST.2023.10245678>
- Al-Zahrani, Fahad (2023). Electronic monitoring strategies in Saudi banks. *Journal of Financial Crime*, 30(4), 891–907. <https://doi.org/10.1108/JFC-01-2023-0005>
- Bisati, Rohit; Astia, Riya; Chauhan, Prashant (2024). An In-depth review of crime detection using artificial intelligence in CCTV videos. *Proceedings of the 6th International Conference on Computational Intelligence and Communication Technologies*. Sonipat, India: IEEE. <https://ieeexplore.ieee.org/abstract/document/10596586>
- Boukerche, Azzedine (2023). Video analytics for financial crime detection. *ACM Computing Surveys*, 55(8), 1–38. <https://doi.org/10.1145/3568765>
- Boukerche, Azzedine; Wang, Jingyu; Zhang, Li; Liu, Chang (2023). AI-integrated surveillance for financial institutions. *IEEE Transactions on Systems, Man, and Cybernetics*, 53(7), 2301–2315. <https://doi.org/10.1109/TSMC.2023.3267890>
- Central Bank of Saudi Arabia (2024). Regulatory Framework for AI Implementation in Banking Security. Retrieved from https://www.sama.gov.sa/documents/AI_Regulatory_Framework_2024.pdf

- Cuevas, Queenie D. P.; Corachea, Joseph C. P.; Escabel, Emma B.; Bautista, Maria L. A. (2016). Effectiveness of CCTV cameras installation in crime prevention. *College of Criminology Research Journal*, 7, 35–48. <https://discovery.ucl.ac.uk/id/eprint/15793/>
- Elnaim, Basem; Al-Juhani, Ahmed; Al-Salem, Hamed (2024). Fintech Innovations in banking security. *Journal of Financial Technology*, 8(1), 78–95. <https://doi.org/10.3390/fintech8010005>
- Fernández-Caramés, Tiago; Blanco-Novoa, Óscar; Fraga-Lamas, Paula (2023). Security protocols for IoT-based surveillance devices. *IEEE Internet of Things Journal*, 10(1), 876–890. <https://doi.org/10.1109/JIOT.2022.3218765>
- Interpol (2024). Global banking security trends 2024. Interpol Innovation Centre. Retrieved from <https://www.interpol.int/en/Publications/Financial-Crime>
- Jeon, Hyunwoo; Kim, Hyunsu; Kim, Donghyun; Kim, Junmo (2024). PASS-CCTV: Proactive anomaly surveillance system for CCTV footage analysis in adverse environmental conditions. *Expert Systems with Applications*, 254, 124391. <https://doi.org/10.1016/j.eswa.2024.124391>
- Khan, Shujaat; Ahmed, Ali; Rahman, Tariq (2023). Adaptive video analytics for financial infrastructure protection. *Expert Systems with Applications*, 225, 120105. <https://doi.org/10.1016/j.eswa.2023.120105>
- Ministry of Communications and Information Technology, KSA (2023). Cybersecurity Standards for Financial Institutions. Retrieved from https://www.mcit.gov.sa/documents/Financial_Cybersecurity_Standards_2023.pdf
- Monetary Authority of Saudi Arabia (2023). Technical Regulations for Banking Surveillance Systems. Retrieved from https://www.sama.gov.sa/documents/Surveillance_Regulations_2023.pdf
- SAMA Research Department (2024). Innovation in Saudi Banking Security. Retrieved from https://www.sama.gov.sa/documents/Banking_Innovation_Report_2024.pdf
- Saudi Authority for Data and Artificial Intelligence (2024). National AI Strategy in Security Systems. Retrieved from https://sdaia.gov.sa/documents/AI_Security_Strategy_2024.pdf
- Saudi Ministry of Education (2023). Social Impact of Security Technologies. Retrieved from https://moe.gov.sa/documents/Security_Tech_Social_Impact_2023.pdf

Saudi Ministry of Interior (2022, October 3). Royal Decree No. M/34 and the Law on the Use of Surveillance Cameras. Bureau of Experts at the Council of Ministers. Retrieved from <https://laws.boe.gov.sa/BoeLaws/Laws/Viewer/abc2a15a-ad44-4215-be7d-af340139151d?lawId=f3a44a6f-9217-478b-b7ca-af3401391514>

Saudi National Cybersecurity Authority (2023). Cybersecurity Guidelines for Banking Surveillance Systems. Retrieved from https://nca.gov.sa/documents/Banking_Surveillance_Guidelines_2023.pdf

Saudi National Cybersecurity Authority (2024). Integrated Security Framework for Financial Institutions. Retrieved from https://nca.gov.sa/documents/Financial_Security_Framework_2024.pdf

Saudi Vision 2030 Office (2024). AI Applications in National Security Projects. Retrieved from https://vision2030.gov.sa/documents/AI_Security_Applications_2024.pdf

Sijan, Md. Abu Hena; Shahoriar, Ahmed; Salimullah, Md.; Islam, A. K. M. Shahariar; Khan, Rashed Hossain (2022). A Review on E-Banking Security in Bangladesh: An Empirical Study. *Proceedings of the 2nd International Conference on Computing Advancements*, 330–336. <https://doi.org/10.1145/3542954.3543002>

Tan, Hwee San; Abas, Hafizah; Shafie, Nurul (2021). A systematic literature review of crime prevention through environmental design principles against banks ATM physical security effectiveness. *Open International Journal of Informatics*, 9(1), 30–44. <https://doi.org/10.11113/oiji2021.9n1.19>

Vennam, Prasanna; Pramod, Thippeswamy C.; Thippeswamy, B. M.; Kim, Young Gab (2021). Attacks and Preventive Measures on Video Surveillance Systems: A Review. *Applied Sciences*, 11(12), 5571. <https://doi.org/10.3390/app11125571>

Wu, Kui (2023). Automated threat detection in surveillance systems. *Information Sciences*, 642, 119087. <https://doi.org/10.1016/j.ins.2023.119087>

Zahrawi, Hana; Shaalan, Khaled (2023). Improving video surveillance systems In banks using deep learning techniques. *Scientific Reports*. <https://doi.org/10.1038/s41598-023-35190-9>