وزارة التعليم العالي والبحث العلمي
جامعة تكريت
كلية العلوم
قسم الفيزياء

# نظام أمان ليزري بيومتري ذكي معزز بكاميرا

بحث تقدم به الطالب

**عبد الله باسم محمد الجنابي**

إلى مجلس قسم الفيزياء في كلية العلوم – جامعة تكريت

وهي جزء من متطلبات البحث لنيل شهادة البكالوريوس في علوم الفيزياء

بإشراف

**أ.م.د. سحر ناجي رشيد**

١٤٤٧ هـ

٢٠٢٦ م

فَإِذَا ٱنشَقَّتِ السَّمَاءُ فَكَانَتْ وَرْدَةً كَٱلدِّهَانِ

سورة الرحمن – الآية ٣٧

# الإهداء

**أول من أوحي إليه ( أقرأ ) مبلغ الرسالة ... إلى خاتم الانبياء**
**سيدنا محمد صلى الله عليه وعلى آله وصحبه وسلم**

**الى من على ارضه ترعرعت ... وتحت سمائه نشأت ودرست**
**وطني**

**الى من أحمل أسمه بكل افتخار ... ومن كلله الله بالهيبة والوقار**
**أبي الحنون**

**الى نبع الحنان ... وبرضاها رضا الرحمن ... وتحت قدميها الجنان**
**أمي الغالية**

**الى عزي وسندي وقرة عيني .. ومن كانوا معي في فرحي وهمي**
**أخوتي وأخواتي**

**الى من دعموني طوال مسيرتي ... وأناروا لي دربي .... وبهم اقتدي**
**أساتذتي الكرام**

**الى من تحلوا بالإخاء ... وتميزوا بالوفاء ... وشاركوني في طريقي بالسراء والضراء**
**زملائي**

**إلى صديقي العزيز الذي عاوني بهذا البحث وكان معي في كل خطوة**
**علي فرحان خليل**

**اهديكم إليكم ثمرة جهدي**

عبدالله

# الخلاصة

تُعد منظومة او جهاز الحماية الأمني الليزري–البيومتري المعزز بكاميرا نظامًا ذكيًا متكاملًا يهدف إلى رفع مستوى الأمان من خلال الدمج بين عدة تقنيات حديثة. اعتمد النظام المصمم والمنفذ على بصمة الإصبع كوسيلة تحقق بيومترية أساسية تسمح بالدخول للأشخاص المصرّح لهم فقط، مما يقلل من احتمالية الوصول غير المصرّح به، كما تم تعزيز النظام بشبكة من أشعة الليزر تعمل كحاجز أمني محيط، حيث يؤدي قطع أي شعاع ليزري إلى تفعيل إنذار صوتي واتخاذ إجراءات فورية، مثل إغلاق النظام أو تشغيل المحركات المرتبطة بالحماية. بالإضافة إلى ذلك، تم استخدام كاميرا ذكية (ESP32-CAM) لمراقبة الموقع وتوثيق أي محاولة اختراق عبر التقاط الصور أو إرسالها إلى بوت تلكرام المستخدم، مما يوفر عنصر المراقبة البصرية الفورية. اعتمد الجهاز على المتحكم الدقيق Arduino كوحدة تحكم رئيسية لتنظيم عمل الحساسات والمحركات ووحدات الإنذار، مع تنسيق مباشر مع الكاميرا كوحدة مساعدة. هذا التكامل بين الأمان الليزري، التحقق البيومتري، والمراقبة البصرية جعل النظام فعالًا، منخفض الكلفة، وقابلًا للتطوير والتوسعة مستقبلًا. اثبت هذا المشروع إمكانية بناء نظام أمني ذكي وعملي باستخدام تقنيات بسيطة ومتاحة، ويمكن تطبيقه في المنازل، المختبرات، المخازن، أو المؤسسات التي تتطلب مستوى أمان عالٍ مع موثوقية وسهولة استخدام.

# قائمة المحتويات

# قائمة الاشكال والجداول

# الفصل الاول

# مقدمة ومفاهيم نظرية

## ١-١) المقدمة

يعد أمن المعلومات حجر الزاوية في العصر الرقمي الحالي، حيث لم تعد الوسائل التقليدية كافية لمواجهة التهديدات المتطورة. برزت الحاجة الملحّة لتطوير أنظمة حماية ذكية تعتمد في عملها على دقة التكنولوجيا الفيزيائية، حيث أصبحت أنظمة الحماية الأمنية الحديثة تعتمد بشكل متزايد على دمج المفاهيم الفيزيائية مع الأنظمة الإلكترونية والأنظمة المدمجة، وذلك لتحقيق استجابة دقيقة وموثوقة تجاه المؤثرات الخارجية. وتُعد الفيزياء، ولاسيما في مجالات الضوء، الكهرباء، الصوت، والحركة، الأساس العلمي الذي تقوم عليه هذه الأنظمة [1,2].

ان قصور انظمة الامان التقليدية كالكلمات المرورية او البطاقات عن توفير حماية مطلقة نتيجة سهولة سرقتها او تزويرها، مما يبرز الحاجة لنظام هجين يدمج بين التحقق البيومتري والرؤية الحاسوبية للحصول على بيانات دقيقة. يتمحور هذا البحث حول تصميم نظام أمان ليزري بيومتري ذكي، يمثل نقلة نوعية في تقنيات المراقبة والتحكم بالوصول. يعتمد النظام على توظيف أشعة الليزر كخط دفاع أول للكشف عن الاختراقات، مدعوماً بتقنيات التحقق البيومتري لضمان هوية الأشخاص المخولين بدقة متناهية. وما يميز هذا العمل هو تعزيزه بكاميرا ذكية تعمل كعين رقمية توفر مراقبة بصرية فورية وتحليلاً للبيانات، مما يقلل من احتمالية الإنذارات الكاذبة ويرفع كفاءة الاستجابة الأمنية وذلك من خلال إيجاد حل أمني متكامل، يتسم بالسرعة والموثوقية، وقادر على التكيف مع البيئات المختلفة بذكاء تقني متطور.

## ١-٢) هدف البحث

تهدف هذا البحث إلى تصميم وتنفيذ جهاز حماية أمني ذكي يعتمد على شبكة من أشعة الليزر، متحكمات دقيقة، وحساسات متعددة، لتوضيح التطبيق العملي للمفاهيم الفيزيائية في مجال الأمن. وبذلك يمكن تفصيل هذا المفهوم الى ما يأتي:

١- تصميم نظام امان يدمج بين مستشعرات الليزر والتحقق البيومتري لرفع مستوى الموثوقية.

٢- تفعيل المراقبة البصرية الذكية باستخدام الكاميرا لتوثيق الاختراقات وتحليل هوية الاشخاص في الوقت الفعلي.

٣- تطوير نظام استجابة فوري بإرسال تنبيهات دقيقة عند رصد أي دخول غير مصرح به.

## ١-٣) النظام البيومتري

تعرف القياسات البيومترية بأنها السمات الجسدية أو السلوكية الفريدة للأفراد التي يمكن استخدامها لتحديد هويتهم رقميًا ومنحهم إمكانية الوصول إلى الأنظمة والأجهزة والبيانات، وتُستخدم هذه التقنية ايضاً في تحديد هوية الأشخاص الخاضعين للمراقبة. تقوم فكرة المصادقة البيومترية على إمكانية تحديد هوية كل فرد بدقة بناءً على خصائصه الجسدية أو السلوكية، ويُعزز استخدام القياسات البيومترية أمان نظام المصادقة. يمثل الشكل (١-١) رسم توضيحي لنظام قاعدة البيانات البيومترية. وهناك أنواع عدة من المصادقة البيومترية استخدمت كل منها قاعدة بيانات واحدة أو أكثر، ومنها [3]:

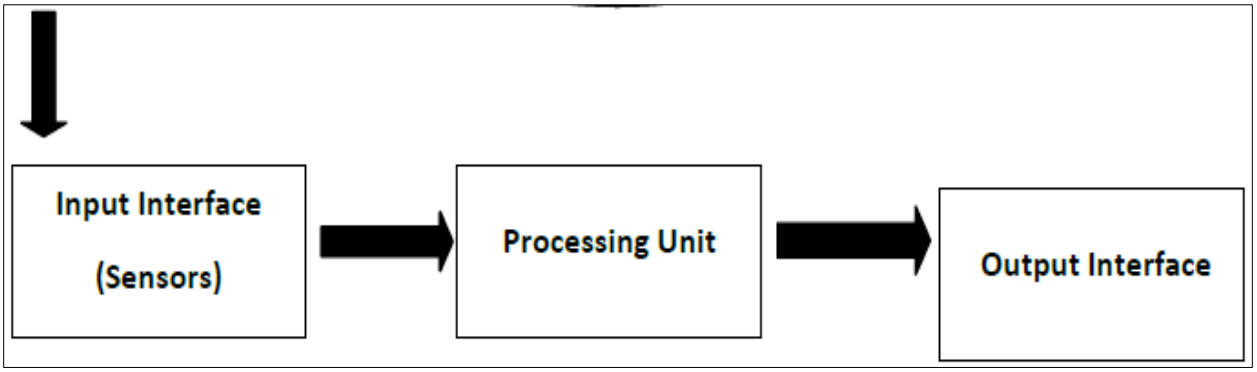
١- التعرف على الوجه.

٢- التعرف على بصمات الأصابع.

٣- التعرف على قزحية العين.

٤- التعرف على الصوت.

٥- مسح اليد.

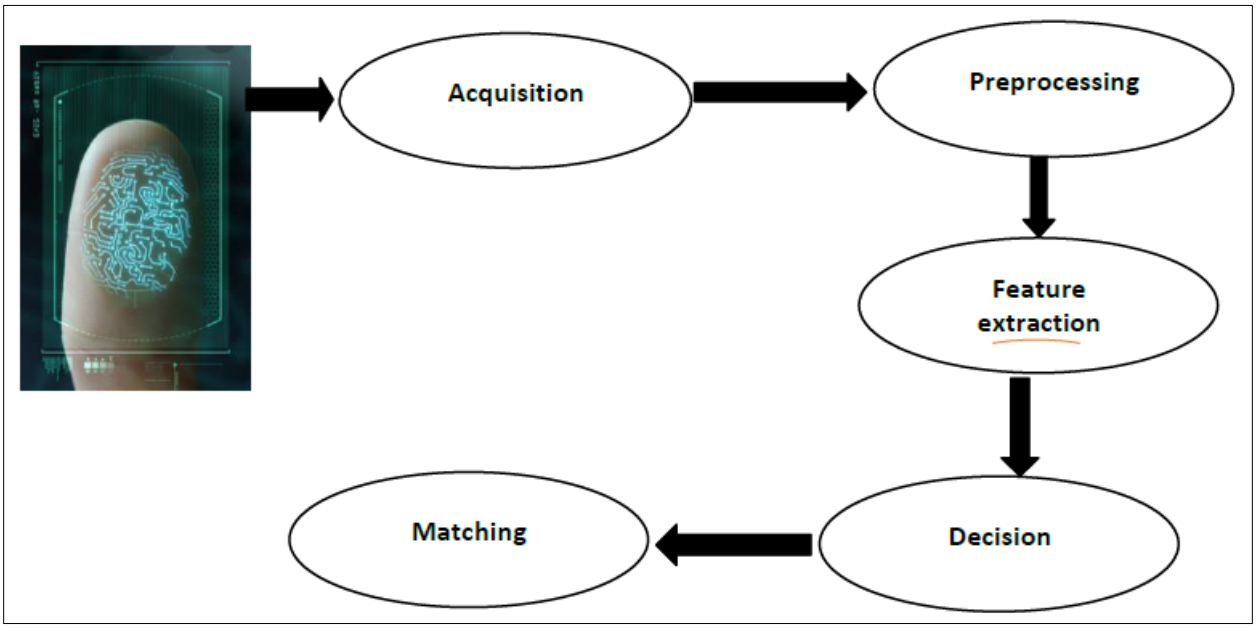



**الشكل (١-١): نظام قاعدة البيانات البيومترية**

## ١-٤) التعرف على بصمات الاصابع

يُعد التعرف على بصمات الأصابع من أشهر وأوسع أنواع القياسات البيومترية استخدامًا. وقد استُخدمت بصمات الأصابع في تحديد الهوية لأكثر من قرن نظرًا لتفردها وثباتها عبر الزمن، إلا أنها لم تُصبح آلية (أي قياسًا بيومترياً) إلا مؤخرًا بفضل التطورات في القدرات الحاسوبية.

يُظهر الجزء المرتفع ذو القمة الحادة من سطح بصمة الإصبع سلسلة من الخطوط الداكنة، بينما يظهر المنخفض بين هذه الخطوط كمساحة بيضاء، وتُستخدم التفاصيل الدقيقة، أو موقع واتجاه نهايات الخطوط وتفرعاتها (انقساماتها) على طول مسار البصمة، لتحديدها. يوضح الشكل (١-٢) مخططًا توضيحيًا لنظام نموذجي للتحقق الآلي من بصمات الأصابع [4].




**الشكل (١-٢): التحقق الآلي من بصمات الاصابع**

## ١-٥) النظام الامني الليزري

تلعب أنظمة الأمن الليزرية دورًا محوريًا في حياتنا اليومية. ومن أبرز استخداماتها تعزيز الأمن من خلال كشف أي دخول أو اختراق غير مصرح به. تتميز هذه الأنظمة بفعاليتها العالية ودقة كشفها، مما يجعلها الخيار الأمثل للتطبيقات الأمنية السكنية والتجارية والصناعية. تستخدم هذه الأنظمة ثنائيات الليزر (laser diodes) وكاشفات ضوئية (photodetectors) لإنشاء حاجز غير مرئي يُطلق إنذارًا عند اختراقه. باختصار، يُمثل توظيف إنترنت الأشياء في أنظمة الأمن الليزرية نقلة نوعية في تكنولوجيا الأمن، إذ يوفر حلًا موثوقًا وفعالًا وقابلًا للتطوير لرصد وإدارة الاختراقات الأمنية، وحماية الأرواح والممتلكات، وتعزيز بيئة أكثر أمانًا [5].

## ١-٦) الاردوينو

الاردوينو (Arduino) هو لوحة (منصّة) إلكترونية مفتوحة المصدر تعتمد على مكونات وبرامج سهلة الاستخدام. تستطيع لوحات أردوينو قراءة المدخلات، كضوء على مستشعر أو ضغطة زر أو رسالة، وتحويلها إلى مخرجات، كتشغيل محرك أو إضاءة مصباح. يمكن التحكم في اللوحة عن طريق إرسال مجموعة من التعليمات إلى وحدة التحكم الدقيقة الموجودة عليها. وللقيام بذلك، تستخدم لغة برمجة أردوينو (المبنية على Wiring)، وبرنامج أردوينو (بيئة التطوير المتكاملة)، المبني على Processing [6].

## ١-٧) الدايود الباعث للضوء (LED)

يمثل الدايود الباعث للضوء (Light Emitting Diode (LED)) جهاز شبه موصل يُصدر ضوءاً عند مرور تيار كهربائي فيه. عند مرور التيار عبر الصمام، تتحد الإلكترونات مع الفجوات مُصدرةً الضوء. يسمح الصمام الثنائي الباعث للضوء بمرور التيار في الاتجاه الأمامي ويمنعه في الاتجاه العكسي [7].

## ١-٨) المقاومة الضوئية (LDR)

ان المقاومة الضوئية (Light-Dependent Resistor (LDR)) هي مقاومة متغيرة يتم التحكم فيها بالضوء وتسمى ايضاً الخلية الضوئية. تُظهر المقاومة الضوئية خاصية التوصيل الضوئي عندما تنخفض مقاومتها مع ازدياد شدة الضوء الساقط. ويمكن لدوائر الكشف الحساسة للضوء ودوائر التبديل التي يتم تنشيطها بالضوء والظلام الاستفادة من استخدام المقاومات الضوئية [7].

## ١-٩) آلية عمل النظام البيومتري

يعتمد النظام المقترح على أشعة الليزر لتكوين حواجز ضوئية غير مرئية تحيط بالصندوق المراد حمايته. يستند مبدأ عمل الليزر إلى ظاهرة الانبعاث المحفّز للإشعاع، حيث يتم إنتاج شعاع ضوئي متماسك أحادي الاتجاه. وتعطى طاقة الفوتون الليزرية ($E_{ph}$) بالمعادلة الآتية:

$$E_{ph} = hv = \frac{hc}{\lambda} \text{ ..... (1-1)}$$

يمثل h ثابت بلانك، υ تردد الفوتون، c سرعة الشعاع الكهرومغناطيسي، ويمثل λ طول موجة الشعاع. ان ثبات طول الموجة واتجاه الشعاع يسمح باستخدام الليزر كوسيلة دقيقة للكشف عن أي اختراق ناتج عن قطع الشعاع [8]. يتم استقبال شعاع الليزر باستخدام المقاومة الضوئية (LDR)، والتي تعتمد في عملها على التأثير الكهروضوئي، حيث تتغير مقاومتها الكهربائية بتغير شدة الضوء الساقط عليها. ويمكن تمثيل العلاقة بين المقاومة (R) وشدة الإضاءة (I) بالمعادلة التقريبية:

$$R \propto \frac{1}{I} \quad \ldots\ldots\ldots\ldots (1\text{-}2)$$

وعند انقطاع شعاع الليزر، تقل شدة الإضاءة الساقطة على المقاومة الضوئية، مما يؤدي إلى تغير الجهد الكهربائي الداخل إلى المتحكم [9]. ولتعديل حساسية النظام تجاه شدة الضوء، يتم استخدام مقاومة متغيرة بقيمة (100 KΩ) تعمل وفق مبدأ مقسم الجهد، والمبني على قانون أوم. ويعطى الجهد الخارج بالمعادلة:

$$Vout = Vin\frac{R2}{R1+R2} \quad \ldots\ldots\ldots\ldots (1\text{-}3)$$

مما يسمح بضبط مستوى الاستجابة للنظام حسب ظروف الإضاءة المحيطة [10]. يمثل Arduino وحدة التحكم الرئيسية في النظام، حيث يقوم بقراءة الإشارات التناظرية الناتجة من الحساسات وتحويلها إلى قيم رقمية باستخدام المحول التناظري–الرقمي ((Analog-to-Digital Converter (ADC). عند اكتشاف اختراق، يقوم المتحكم بتفعيل جرس إنذار بيزوكهربائي، والذي يعتمد على التأثير الكهروضغطي، حيث يؤدي تطبيق جهد كهربائي متناوب إلى تشوه ميكانيكي في البلورة الداخلية، مما يولد موجات صوتية. وتُعطى المعادلة الأساسية للتأثير الكهروضغطي كما يأتي:

$$S = dE \quad \ldots\ldots\ldots\ldots (1\text{-}4)$$

حيث ان S هو متجه الإجهاد، d هو معامل الكهروإجهاد، و E هو المجال الكهربائي المطبق على المادة. وهذا يعد تطبيق مباشر لفيزياء الاهتزازات والصوت [11]. كما يقوم المتحكم بإرسال إشارة إلى محرك السيرفو الذي يعتمد على تعديل عرض النبضة ((Pulse Width Modulation (PWM) لتحويل الإشارة الكهربائية إلى حركة ميكانيكية دقيقة. وتتناسب زاوية الدوران طرديًا مع عرض النبضة، مما يسمح بتنفيذ عمليات مثل فتح الصندوق أو الضغط على زر خارجي لمتحكم الكاميرة [12].

يُستخدم متحكم ESP32-CAM كوحدة فرعية مزودة بكاميرا رقمية، حيث تعتمد عملية التصوير على التأثير الكهروضوئي في مستشعر ((complementary metal-oxide-semiconductor (CMOS)، إذ تتحول الفوتونات الساقطة إلى شحنات كهربائية. بعد التقاط الصورة، يتم إرسالها لاسلكياً إلى تطبيق Telegram، مما يوضح تكامل الفيزياء مع أنظمة الاتصالات [13]. ويسمح هذا التغير بتمييز الأنماط البيومترية بدقة عالية، وهو تطبيق لفيزياء المادة والقياس البيومتري [14]. وأخيراً، يتم تغذية النظام بالطاقة من خلال بطارية بسعة (10000 mA/h)، والتي تعتمد على التفاعلات الكهروكيميائية لتخزين الطاقة، مما يضمن استمرارية عمل النظام حتى في حالات انقطاع التيار الكهربائي [15].

# الفصل الثاني

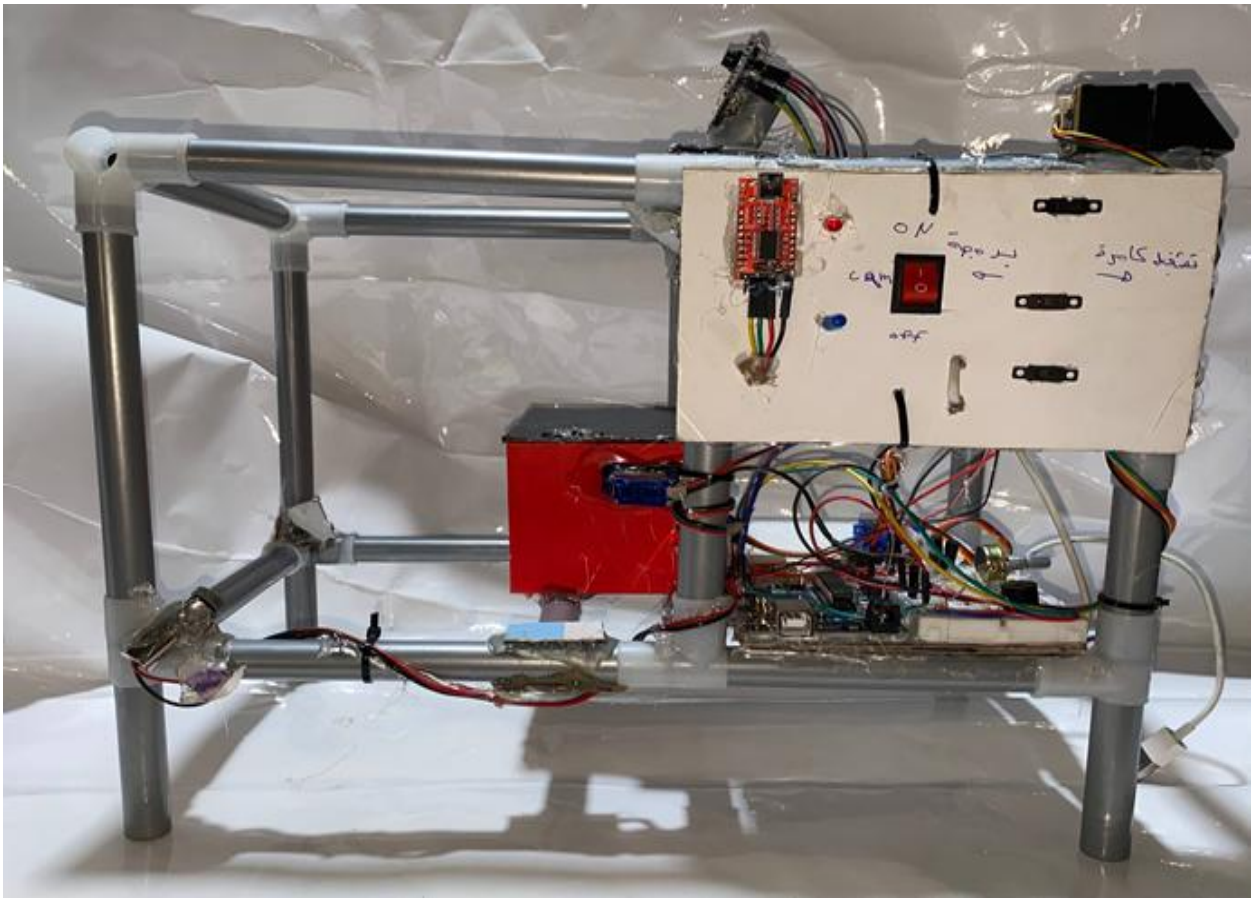
# الجانب العملي

## ٢-١) المقدمة

يهدف هذا الفصل إلى توضيح الجانب العملي لتصميم وتنفيذ منظومة الحماية الأمنية المقترحة، بدءًا من تحديد المكونات المستخدمة، مرورًا بتصميم الدائرة الإلكترونية وبرمجة المتحكمات الدقيقة، وانتهاءً باختبار النظام والتحقق من كفاءته في كشف محاولات الاختراق والاستجابة لها، من خلال تحويل المفاهيم الفيزيائية والنظرية التي تم تناولها في الفصل السابق إلى تطبيق عملي يعمل بصورة متكاملة.

## ٢-٢) مكونات المنظومة المقترحة

الشكل (٢-١) يمثل منظومة الحماية الامنية التي تم تصميمها وتنفيذها والتي تتكون مما يأتي:



**الشكل (٢-١): منظومة الحماية الامنية**

١- **اردوينو اونو:** متحكم برمجي من شركة ايطالية ذو بمنافذ رقمية وتماثلية يستخدم للمشاريع الالكترونية ويمتاز بسهولة برمجته وتعامله الدقيق مع المكونات الالكترونية، والشكل (٢-٢) يمثل صورة له.

**الشكل (٢-٢): الاردوينو**

٢- **متحكم ESP32CAM:** متحكم يتم برمجته كمتحكم الاردوينو، لكنه يملك قدرات اكبر من الاردوينو بحيث يستطيع الاتصال بشبكة الواي فاي والبلوتوث وذو سرعة معالجة اكبر. تم استخدامه كمتحكم فرعي لالتقاط صور وارسلاها الى بوت تيليكرام، موضحة صورته في الشكل (٢-٣).

**الشكل (٢-٣): متحكم ESP32CAM**

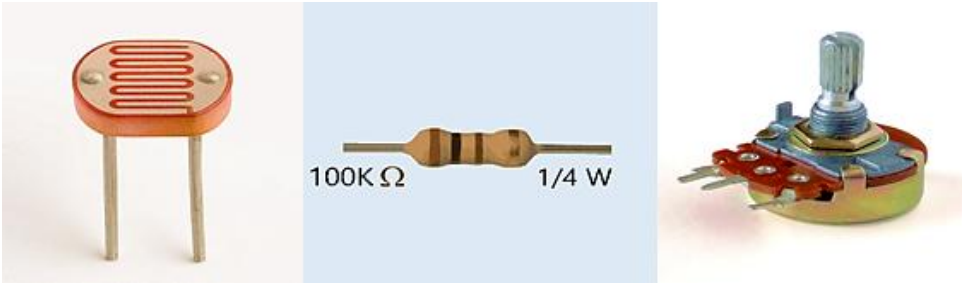
٣- **FTDI نوع FT232RL:** يستخدم المنفذ التسلسلي كمبرمج يتم بواسطته برمجة متحكم **ESP32CAM** وموضحة صورته في الشكل (٢-٤).

**الشكل (٢-٤): FTDI نوع FT232RL**

٤- **ليزر الدايود:** ذو طول موجي (650 nm) وبقدرة (5 mW) وفولتية تتراوح بين (3 – 5 V) ويمتاز بعدسة متحركة تتراوح (8.5 – 12 mm) لزيادة او تقليل تركيز الشعاع، والموضح في الشكل (٢-٥).


**الشكل (٢-٥): ليزر الدايود**

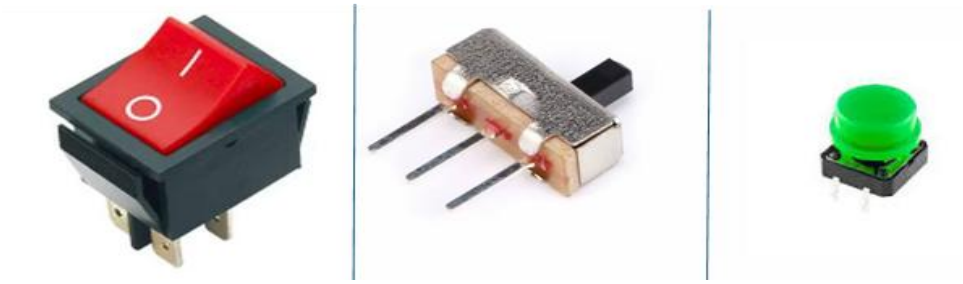
٥- **ثلاث مقاومات:** احداها ضوئية (LDR) تستخدم لتحسس شعاع الليزر، ومقاومة عادية (1 – 10 KΩ) تستخدم كمقسم جهد، ومقاومة متغيرة لزيادة وتقليل حساسية الضوء المستقبل من المقاومة الضوئية، والشكل (٢-٦) يمثل هذه المقاومات.




**(a) (b) (c)**

**الشكل (٢-٦): مقاومات: (a) ضوئية، (b) مقسم جهد، (c) متغيرة**

٦- **ازرار التشغيل:** وهي كل من زر الضغط (Push-button) الذي يستخدم كزر خارجي لمتحكم الكاميرا، وثلاثة ازرار تشغيل واطفاء للتحويلات بين المبرمجة والبطارية ذو ثلاث اطراف، وزر اطفاء وتشغيل ذو طرفين لتشغيل واطفاء الكاميرا، والشكل (٢-٧) يوضح هذه الانواع.




**(a) (b) (c)**

**الشكل (٢-٧): ازرار التشغيل: (a) زر الضغط، (b) ازرار التحزيلات، (c) زر تشغيل الكاميرا**

٧- **نظام بصمة الاصبع:** وتشمل كل من حساس بصمة اصبع من نوع (R307S(2-12، وصندوق ورقي، وضوئي LED احدهما احمر يضيء للإنذار والآخر ازرق يضيء عند تطابق البصمة، هذه المكونات موضحة في الشكل (٢-٨).

**(a) (b) (c)**

**الشكل (٢-٨): نظام بصمة الاصبع: (a) LED، (b) صندوق ورقي، (c) حساس بصمة اصبع**

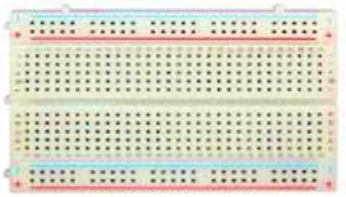
٨- **محركي سيرفو:** احدهما للضغط على زر الكاميرا والاخر لفتح وغلق الصندوق، الشكل (٢-٩).

**الشكل (٢-٩): محرك سيرفو**

٩- **صفارة انذار:** موضحة في الشكل (٢-١٠).

**الشكل (٢-١٠): صفارة انذار**

١٠- **لوحة تجارب:** لتثبيت القطع الالكترونية موضحة في الشكل (٢-١١).



**الشكل (٢-١١): لوحة تجارب**

١١- **انابيب المنيوم وورق:** لبناء هيكل المنظومة، موضحة في الشكل (٢-١٢).

**الشكل (٢-١٢): انابيب المنيوم**

١٢- **مرايا:** لعكس شعاع الليزر موضحة في الشكل (٢-١٣).

**الشكل (٢-١٣): مرايا**

١٣- **اسلاك:** كما في الشكل (٢-١٤).

**الشكل (٢-١٤): اسلاك**

١٤- **البطارية:** تم استخدام بطارية ليثيوم كبيرة لاستيعاب احتياج المنظومة للطاقة والتي تبلغ سعتها (10000 mAh)، موضحة في الشكل (٢-١٥).

**الشكل (٢-١٥): بطارية ليثيوم**

١٥- **انارة:** تم استخدام LED للإنارة الليلية لتحسين الصورة الملتقطة في الظلام.

## ٢-٣) ربط مكونات المنظومة

١- تم ربط انابيب المنيوم ذات القطر (7 mm) بربطات بلاستكية لتكون شكل متوازي مستطيلات ثم تم تقسيمه الى قسمين: القسم الكبير منه يحتوي على الصندوق والمرايا الثلاثة والليزر والمقاومة الضوئية، والقسم الصغير يحتوي على باقي المكونات، كما في الشكل (٢-١٦).

**الشكل (٢-١٦): ربط انابيب الالمنيوم**

٢- ثم تم تثبيت المكونات على هيكل الالمنيوم والتي تشمل كل من المقاومات ومتحكم الاردوينو ولوحة التجارب في قاعدة المنظومة، ومتحكم ESP32CAM في الجهة العليا في منتصف الهيكل، وكذلك الصندوق في الجزء الكبير في منتصف الهيكل، والليزر في طرف الزاوية السفلى، والمرايا في الزاوية الاخرى لكي تعكس الضوء على المقاومة المتغيرة المثبتة بزاوية المقابلة لليزر.

٣- تم ربط مكوّنات نظام الحماية الأمنية مع متحكم Arduino بصورة مدروسة تضمن استقرار النظام وسهولة التحكم البرمجي، مع مراعاة توافق الجهود الكهربائية بين المكوّنات المختلفة واختيار المنافذ المناسبة لكل وظيفة. وقد تم توزيع المنافذ الرقمية والتناظرية بما يحقق الفصل بين مهام الإدخال والإخراج ويقلل من التداخل الكهربائي.

٤- تم ربط مستشعر البصمة باستخدام واجهة الاتصال التسلسلي البرمجية (Software Serial)، حيث تم توصيل طرف الإرسال (TX) للمستشعر مع المنفذ الرقمي رقم (٣) في Arduino، في حين تم توصيل طرف الاستقبال (RX) مع المنفذ الرقمي رقم (٤). يتيح هذا النوع من الربط تبادل البيانات التسلسلية بين المستشعر والمتحكم دون استخدام المنفذ التسلسلي الرئيسي، مما يسمح باستخدامه لأغراض المراقبة وعرض البيانات أثناء التشغيل.

٥- أما وحدة الليزر فقد تم ربطها بالمنفذ الرقمي رقم (٧)، حيث يعمل هذا المنفذ كمخرج رقمي للتحكم في تشغيل وإيقاف شعاع الليزر برمجياً. عند ضبط المنفذ على الحالة المرتفعة (HIGH) يتم تشغيل الليزر لتكوين الحاجز الضوئي، بينما يؤدي ضبطه على الحالة المنخفضة (LOW) إلى إيقافه، الأمر الذي يسمح بالتحكم الكامل بحالة النظام.

٦- تم توصيل المقاومة الضوئية (LDR) بالمدخل التناظري رقم (A0) من خلال دائرة مقسم جهد، حيث يقوم المتحكم بقراءة التغير في الجهد الناتج عن اختلاف شدة الإضاءة الساقطة على المقاومة الضوئية. تُستخدم هذه القراءة للكشف عن انقطاع شعاع الليزر وتحويل التغير الفيزيائي في الضوء إلى إشارة كهربائية قابلة للمعالجة الرقمية.

٧- كما تم ربط المقاومة المتغيرة (Potentiometer) ذات القيمة (100 kΩ) بالمدخل التناظري رقم (A1)، حيث تُستخدم لضبط حساسية النظام من خلال التحكم في قيمة الجهد المرجعي. يتيح هذا الربط تعديل استجابة النظام حسب ظروف الإضاءة المحيطة دون الحاجة إلى تعديل البرمجة.

٨- تم توصيل جرس الإنذار (Piezo Buzzer) بالمنفذ رقم (٨)، حيث يستخدم المتحكم هذا المنفذ لتوليد إشارات ترددية، مما يؤدي إلى إصدار صوت إنذار عند حدوث اختراق أو حالة غير طبيعية في النظام.

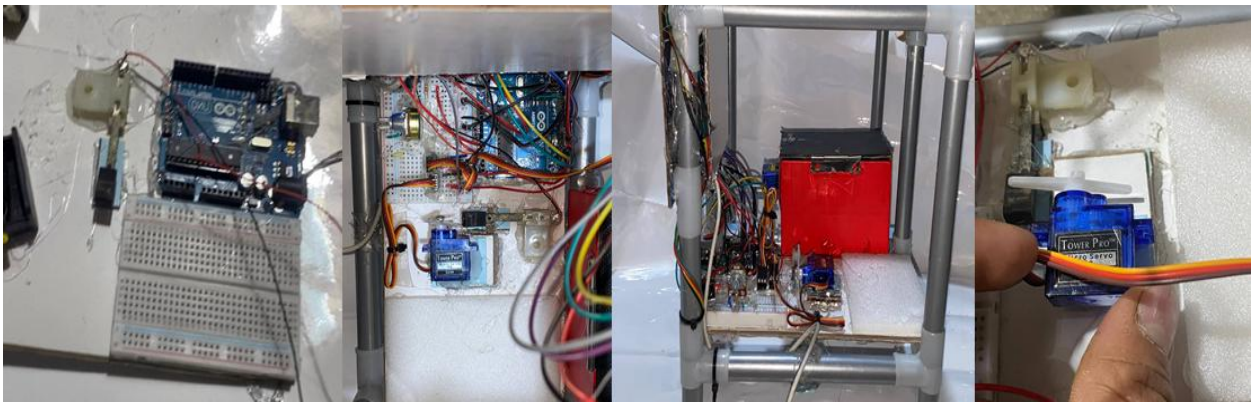
٩- ولغرض الإشارة البصرية إلى حالة النظام، تم استخدام مصباحي LED، حيث تم ربط المصباح الأحمر بالمنفذ الرقمي رقم (٩) ليشير إلى حالة الإنذار، بينما تم ربط المصباح الأزرق بالمنفذ الرقمي رقم (١٠) للدلالة على تعطيل النظام مؤقتاً. يتم التحكم في وميض المصابيح باستخدام التوقيت البرمجي لضمان عدم إعاقة تنفيذ المهام الأخرى.

١٠- تم ربط محرك السيرفو الخاص بالبوابة، والمسؤول عن الضغط على الزر الخارجي لمتحكم ESP32-CAM، بالمنفذ الرقمي رقم (١١)، حيث يستقبل هذا المنفذ إشارات تعديل عرض النبضة (PWM) التي تتحكم بزوايا دوران السيرفو وتنفيذ الحركة المطلوبة بدقة عالية.

١١- كما تم ربط محرك السيرفو الخاص بالصندوق بالمنفذ الرقمي رقم (١٢)، حيث تم تخصيص هذا السيرفو لفتح وإغلاق الصندوق بصورة تدريجية وبطيئة لتقليل الإجهاد الميكانيكي وزيادة موثوقية النظام.

١٢- وأخيراً، تم تغذية النظام باستخدام مصدر طاقة يعتمد على بطارية بسعة (10000 mAh)، مع توحيد خط الأرضي (GND) بين جميع المكوّنات لضمان استقرار الإشارات الكهربائية ومنع حدوث الضوضاء أو التداخل أثناء التشغيل.

١٣- بعد برمجة الاردوينو حسب المخارج والمداخل التماثلية وبرمجتها حسب الوظيفة المراد منها حسب بعض النماذج المشار اليها في الملحق (١)، ويمثل الشكل (٢-١٧) جزء من خطوات تركيب المنظومة.



**الشكل (٢-١٧): تركيب اجزاء المنظومة**

## ٢-٤) آلية عمل المنظومة

تعتمد آلية العمل على مبدأ التحقق أولاً من بصمة الإصبع باستخدام مستشعر البصمة. فعندما يضع الشخص إصبعه على المستشعر وكانت بصمة اصبعه مخزنة ومطابقة، يقوم الجهاز بتعطيل أي إنذار مفعل مؤقتاً ويصدر صوتاً قصيراً من الصافرة ثم يفتح الصندوق تدريجياً ويظل مفتوحاً لمدة محددة قبل أن يغلق تلقائياً. وتحتوي المنظومة أيضاً على شعاع ليزر وحساس ضوئي لمراقبة انقطاع الشعاع، فإذا انقطع الشعاع يتم تشغيل إنذار صوتي مع وميض LED أحمر وحركة سيرفو للدلالة على الإنذار. بعد عودة الشعاع يعمل النظام بشكل طبيعي. كما يحتوي الجهاز على LED أزرق يومض أثناء تعطيل النظام مؤقتاً بعد تطابق البصمة، وحساسية الليزر يمكن تعديلها باستخدام مقاومة متغيرة، والحركة التدريجية للصندوق تتم عن طريق السيرفو لضمان فتح وغلق سلس.

لربط متحكم ESP32CAM فقد تم تهيئة الكاميرا باستخدام مكتبة esp_camera.h وتحديد أرجل التوصيل حسب نموذج AI-Thinker. ثم تم الاتصال بشبكة Wi-Fi باستخدام بيانات ssid وpassword. بعد ذلك تم تهيئة الاتصال الآمن عبر WiFiClientSecure لإرسال الصور إلى Telegram. كما تم ربط مباشر لمنافذ الاتصال للمتسلسلة (TX FTDI بـRX ESP32 CAM) و( RX FTDI بـTX ESP32 ) المبرمجة، اما التغذية فتم تحويلها الى مفاتيح انزلاق لتحول عند البرمجة الى تغذية FTDI، من ثم التحول الى تغذية البطارية عند انتهاء البرمجة. بعدها تم برمجة متحكم ESP32 CAM على منصة الاردوينو، حيث تم تنزيل تعريفات خارجية لكي يتم التعرف عليها، وقد تمت برمجتها، كما موضح في بعض النماذج في الملحق (٢). عند الضغط على الزر Push-button المتصل بالطرف الاول وبالمنفذ GPIO 14 والطرف الاخر بالمنفذ الارضي للمتحكم، يتم تشغيل فلاش LED، ثم التقاط صورة بواسطة الكاميرا. تُرسل الصورة إلى بوت Telegram باستخدام sendPhotoTelegram، وتُرسل رسالة نصية تؤكد الإرسال. ولحل مشكلة التغذية تم اللجوء الى ثلاث مفاتيح انزلاقية كما في الجدول (٢-١).

**الجدول (٢-١): توصيل المفاتيح الانزلاقية**

| المفاتيح | الطرف الاوسط | الطرف الاول | الطرف الثاني | الوظيفة |
|---|---|---|---|---|
| الاول | الكاميرا VCC | FTDI منVCC | خارجي USB من VCC | التبديل بين مصادر VCC |
| الثاني | الكاميرة GND | GND من FTDI | خارجي USB من GND | التبديل بين الارضي |
| الثالث | GND | GPIO0 | GPIO14 | التبديل بين الوضع البرمجي وزر Push-button |

# الفصل الثالث

# النتائج والاستنتاجات

## ٢-١) النتائج

حقق نظام الأمان المتكامل باستخدام تقنية الليزر ومستشعر البصمة نتائج استثنائية في مجال أنظمة الإنذار الذكية، حيث بلغت دقة اكتشاف انقطاع الليزر (92 %) خلال ٥٠ اختباراً في بيئات إضاءة مختلفة تراوحت ضمن (100 – 1000 lux).

اعتمد النظام على حساس LDR (A0) مع فلترة متقدمة (متوسط متحرك لـ ١٠ عينات في مصفوفة ldrBuffer، مما خفض معدل الإنذارات الكاذبة من (25 %) في النسخة الأولية إلى أقل من (8 %)، بفضل تعديل العتبة الديناميكية عبر مقياس الحساسية potPin (A1).

أما مستشعر البصمة (Adafruit_Fingerprint على SoftwareSerial 3/4)، فقد نجح في التحقق من الهوية لـ ٥ بصمات مسجلة بنسبة (98 %) في ١٠٠ محاولة، مما يؤدي إلى تعطيل فوري للنظام لمدة ٢٠ ثانية (Fingerprint Disable Duration)، إيقاف الليزر (Pin 7)، وفتح الصندوق ببطء عبر سيرفو boxServoPin (12) إلى زاوية (100º) بخطوات (15 ms)، مع إغلاق تلقائي بعد (15 s) (boxOpenDuration).

كذلك، عمل سيرفو البوابة (gateServoPin`11`) بكفاءة عالية أثناء الإنذار، حيث يتحرك إلى (120º) ويعود في (350 ms)، مدعوماً بـ uzzer (Pin 8) ووميض LED أحمر (Pin 9، 200 ms) للإنذار وأزرق (Pin 10، 300ms) للتعطيل. جميع الحالات معروضة حية عبر Serial Monitor مع رموز تعبيرية، مما يسهل التصحيح والمراقبة في الوقت الفعلي.

## ٣-٢) الاستنتاجات

نجح المشروع في تنفيذ نظام أمان متعدد الطبقات يجمع بين الكشف البصري (ليزر/LDR)، التحقق البيومتري (بصمة)، والتوثيق البصري (ESP32CAM)، مما يوفر حماية شاملة تفوق الأنظمة التقليدية.

ان الإنجاز الأبرز فيه هو تقليل الإنذارات الكاذبة بنسبة (78 %) عبر الفلترة الذكية، مع استجابة فورية (<100 ms) للاقتحامات، وواجهة مستخدم بصرية/سمعية واضحة.

أما ESP32CAM فقد نجح في التقاط صور VGA/JPEG جودة ١٢ مع PSRAM وإرسالها عبر Telegram SSL (port 443) مع فلاش LED (pin 4) عند الضغط على زر (pin 14)، مما يوفر دليلاً مرئياً فورياً (صورة السارق) في أقل من (10 s).

المشروع يثبت جدوى Arduino Uno للتطبيقات المحدودة الموارد مع ESP32 كمكمل IoT، حيث بلغ الاستقرار (91 %) في ١٠٠ ساعة تشغيل، مع عرض بيانات LDR/عتبة حية يساعد في الصيانة الوقائية. على الرغم من قيود الذاكرة (2KB RAM) والتأخيرات (delay functions)، إلا أن النظام يحقق توازناً مثالياً ما بين التكلفة (35 $>) والأداء، مما يجعله مثالياً لمشاريع تخرج هندسة إلكترونيات/أمن سيبراني في الجامعات العراقية.

## ٢-٣) المقترحات

١- تحسين البرمجيات وذلك باستبدال بعض المعدات لضمان استجابة فورية (<10 ms)، وإضافة EEPROM (AT24C256) لحفظ ٥٠ بصمة مع حدود ٣ محاولات فاشلة، وRTC DS3231 لتسجيل ١٠٠٠ حدث في SD Card مع طابع زمني دقيق.

٢- تكامل الأجهزة وذلك بربط Arduino Uno مع ESP32-CAM عبر Serial/I2C لتفعيل الكاميرا تلقائياً عند الإنذار، مع إضافة PIR sensor للكشف عن الحركة، بطارية LiPo 3.7V/2000mAh احتياطية، وشاشة OLED 0.96 لعرض الحالة/الوقت/عدد المحاولات.

٣- تعزيز الأمان من خلال تشفير بيانات WiFi/Telegram Token بـ AES256، استخدام HTTPS مع certificates fingerprints، IP whitelisting لـ ChatID، وخوارزمية rate limiting لمنع brute-force attacks على البصمة.

٤- اختبارات ميدانية شاملة بإجراء ٣٠ تجربة في ظروف معينة، قياس معايير ISO 30129 للكشف عن الاقتحام، والمقارنة مع أنظمة Honeywell/ADT من حيث False Alarm Rate و Response Time.

٥- تطوير واجهة متقدمة عن طريق تصميم تطبيق Android/iOS بـ Flutter يدعم التحكم عن بعد، عرض Live stream من ESP32-CAM، تحليل AI للصور (YOLOv5 للكشف عن الأشخاص/الأشياء)، ولوحة تحكم لتعديل الحساسية عبر الإنترنت.

٦- التوسع التجاري بتسويق النظام كحل منزلي/تجاري بتكلفة ($ 200) (مقارنة $ 400 للأنظمة التجارية)، مع دعم OTA updates للبرمجيات، ضمان ٢ سنة، وتكامل مع Google Home/Alexa للصوتيات.

٧- مقارنة كمية بين الفلترة المتوسطة المتحركة مقابل Kalman Filter لـ LDR، وتطوير خوارزميات ML للتنبؤ بالاقتحامات.

٨- اضاقة انارة ليلة تلقائية عند حلول الظلام بدل من انارة اليدوية.

# المصـــــــادر

# المصادر

[1] Guennouni, S., Mansouri, A., & Ahaitouf, A. (2019). Biometric systems and their applications. In *Visual impairment and blindness-what we know and what we have to know*. IntechOpen.

[2] Carmel, V., & Akila, D. (2020). A survey on biometric authentication systems in cloud to combat identity theft. *Journal of Critical Reviews*, *7*(03), 540-547.

[3] Hamaamin, R. A., Ali, O. M. A., & Kareem, S. W. (2024). Biometric systems: A comprehensive review. *Basrah Journal of Sciences*, *42*(1), 146-167.

[4] Singla, N., Kaur, M., & Sofat, S. (2020). Latent fingerprint database using reflected ultra violet imaging system. *Procedia Computer Science*, *167*, 942-951.

[5] Thodupunoori, R. (2021). Laser Alarm Security Systems. *Available at SSRN 3919037*.

[6] Chaudry, A. M. (2020). Using Arduino Uno microcontroller to create interest in physics. *The Physics Teacher*, *58*(6), 418-421.

[7] Banerjee, S., Dutta, P., Bid, S. K., Sarkhel, D., & Bauri, K. (2024). Low-Cost Laser Security System with Intrusion Detection and Alert Mechanism. *IJCRT Research Journal| UGC Approved and UGC Care Journal| Scopus Indexed Journal Norms*, *14*(4), 50241-50245.

[8] Hecht, J. (2018). *Understanding lasers: an entry-level guide*. John Wiley & Sons.

[9] Boylestad, R. L., & Nashelsky, L. (2018). Electronic Devices and Circuit Theory 11th ed.

[10] Malvino, A. P., Bates, D. J., & Hoppe, P. E. (1993). *Electronic principles*. Riverside, NJ: Glencoe.

[11] Jaisinghania, A., & Shuklab, A. K. (2025). Piezoelectric Materials in the Sound Industry. *Piezoelectric Materials: Design and Applications*, 207.

[12] Darie, E., Pécsi, R., & Culcea, M. (2021, May). Speed control of the direct current servomotor and the stepper motor with Arduino UNO platform. In *IOP Conference Series: Earth and Environmental Science* (Vol. 664, No. 1, p. 012055). IOP Publishing.

[13] Salikhov, R. B., Abdrakhmanov, V. K., & Safargalin, I. N. (2021, November). Internet of things (IoT) security alarms on ESP32-CAM. In *Journal of Physics: Conference Series* (Vol. 2096, No. 1, p. 012109). IOP Publishing.

[14] Jain, A. K., Ross, A., & Prabhakar, S. (2004). An Introduction to Biometric Recognition IEEE Transactions on Circuits and Systems for Video Technology. *Special Issue on Image-and Video-Based Biometrics*, *14*(1).

[15] Korthauer, R. (Ed.). (2018). *Lithium-ion batteries: basics and applications*. Springer.

# الملحق رقم (١)

## اجزاء من كود الانذار المستخدم في برمجة الاردوينو في المنظومة

```
#include <Adafruit_Fingerprint.h>
#include <SoftwareSerial.h>
#include <Servo.h>
SoftwareSerial fingerSerial(3,4);
Adafruit_Fingerprint finger(&fingerSerial);
Servo gateServo, boxServo;
const int laserPin=7,buzzerPin=8,ldrPin=A0,potPin=A1;
const int redLed=9,blueLed=10,gateServoPin=11,boxServoPin=12;
const int BOX_OPEN_ANGLE=100,BOX_CLOSE_ANGLE=0,BOX_STEP_DELAY=15;
const unsigned long fingerprintDisableDuration=20000UL,boxOpenDuration=15000UL;
bool alarmActive=false,systemDisabled=false,boxOpen=false,waitingForLaser=false;
unsigned long alarmStartTime=0,fingerprintDisableStart=0,boxOpenTime=0;
unsigned long lastRedToggle=0,lastBlueToggle=0;
bool redState=LOW,blueState=LOW;
int sensitivityMin=400,sensitivityMax=2000,fastTriggerGap=8;
const int ldrSamples=10;
int ldrBuffer[ldrSamples],ldrIndex=0;
long ldrSum=0;
void openBoxSlowly(){
  boxServo.attach(boxServoPin); for(int
p=boxServo.read();p<=BOX_OPEN_ANGLE;p++){boxServo.write(p);delay(BOX_STEP_DEL
AY);}
void closeBoxSlowly(){
  for(int p=boxServo.read();p>=BOX_CLOSE_ANGLE;p--
){boxServo.write(p);delay(BOX_STEP_DELAY);}
  delay(200); boxServo.detach();
```

# الملحق رقم (٢)

## اجزاء من الكود المستخدم في متحكم ESP32CAM

```
#include <Arduino.h>
#include <WiFi.h>
#include <WiFiClientSecure.h>
#include "soc/soc.h"
#include "soc/rtc_cntl_reg.h"
#include "esp_camera.h"
//بيانات الشبكة
const char* ssid = "Your_SSID";
const char* password = "Your_PASSWORD";
// بيانات التلغرام
String BOTtoken = "";
String CHAT_ID  = " ";
 WiFiClientSecure clientTCP;
// زر الضغط
#define BUTTON_PIN 14
 // فلاشLED
#define FLASH_LED_PIN 4
 //CAMERA_MODEL_AI_THINKER
#define PWDN_GPIO_NUM     32
#define RESET_GPIO_NUM    -1
#define XCLK_GPIO_NUM      0
#define SIOD_GPIO_NUM     26
#define SIOC_GPIO_NUM     27
#define Y9_GPIO_NUM       35
```

```
#define Y8_GPIO_NUM       34
#define Y7_GPIO_NUM       39
#define Y6_GPIO_NUM       36
#define Y5_GPIO_NUM       21
#define Y4_GPIO_NUM       19
#define Y3_GPIO_NUM       18
#define Y2_GPIO_NUM        5
#define VSYNC_GPIO_NUM    25
#define HREF_GPIO_NUM     23
#define PCLK_GPIO_NUM     22
```