مذكرة تخرج مقدمة في

جامعة محمد بوضياف - المسيلة

كلية الرياضيات والإعلام الآلي

قسم الإعلام الآلي

من أجل الاستيفاء الجزئي لمتطلبات شهادة

ليسانس في الإعلام الآلي

إعداد

فاتح زروتي

عبد النور نش

عنوان المذكرة

اعداد برنامج تشفير الملفات

تحت إشراف الأستاذ

طاهري زهير

تحت إشراف الأستاذ مساعد

وفاء بوراس

أعضاء لجنة المناقشة

الاسم اللقب	**جامعة المسيلة**	**رئيسا**
الاسم اللقب	**جامعة المسيلة**	**مقررا**
الاسم اللقب	**جامعة المسيلة**	**ممتحنا**

جوان، 2025

الملخص

تُعالج هذه المذكرة موضوع حماية البيانات الرقمية من خلال تصميم وتطوير برنامج مكتبي يعتمد على تقنيات التشفير والإخفاء. يهدف المشروع إلى تمكين المستخدم من تشفير الملفات النصية والصوتية والصورية باستخدام خوارزميات RSA وAES، مع دمج تقنيات Steganography لإخفاء البيانات داخل وسائط متعددة. تم تطوير الأداة المقترحة بلغة Python، بالاعتماد على مكتبات متخصصة في التشفير، معالجة الصور والصوت، وإنشاء واجهات رسومية يشمل العمل دراسة نظرية لمفاهيم التشفير والأمان، وتحليل أدوات قائمة، ثم تصميم وتنفيذ تطبيق عملي باسم SecureShield. أظهرت النتائج أن الأداة توفر حماية فعالة وسهلة الاستخدام، مما يجعلها مناسبة لتعزيز أمن المعلومات في الاستخدامات اليومية.

الكلمات المفتاحية:تشفير، Steganography، RSA، AES، Python، أمن المعلومات.

Abstract

This thesis addresses the topic of digital data protection through the design and development of a desktop application that relies on encryption and steganography techniques. The project aims to enable users to encrypt text, audio, and image files using RSA and AES algorithms, while integrating steganography methods to hide data within various media. The proposed tool was developed using the Python programming language, relying on specialized libraries for cryptography, image and audio processing, and graphical user interface deve -lopment. The work includes a theoretical study of encryption and security concepts, an analysis of existing tools, followed by the design and implementation of a practical application called SecureShield. The results showed that the

tool provides effective and user-friendly protection, making it suitable for enhancing information security in everyday use.
Keywords: Encryption, Steganography, RSA, AES, Python, Information Security

الشكر والتقدير

نتقدم بجزيل الشكر والامتنان إلى مشرفنا على هذه المذكرة [**االاستاذ طاهري زهير والاستاذة وفاء بوراس**]، الذي كان دعمهم المستمر ومصدر إلهامنا الدائم سبباً في نجاح هذا العمل. نشكره بشكل خاص على توجيهاتهم المتواصلة وتشجيعه لنا طيلة فترة هذا البحث.

كما نخص بالشكر أصدقاءنا وأفراد عائلاتنا الذين تحمّلوا معنا اللحظات الصعبة، وقدموا لنا الدعم والمساندة طيلة فترة الدراسة.

ولا يفوتنا أن نشكر مؤسستنا التي منحتنا فرصة العمل الجماعي، مما ساهم في تعزيز روح التعاون والمهارات التواصلية بيننا. كما نُعبّر عن خالص تقديرنا لجميع أعضاء الفريق على التزامهم وتضامنهم.

المحتويات

الشكر والتقدير **3**

المقدمة **8**

1 الفصل الأول:مقدمة في عل التشفير **10**

1.1 المقدمة 10

2.1 بعض التعريفات 10

1.2.1 علم التشفير. 10

2.2.1 التشفير 10

3.2.1 تحليل التشفير 11

3.1 جوانب الأمان 11

1.3.1 النزاهة 11

2.3.1 التوافر. 11

3.3.1 السرية 11

4.3.1 عدم التنصل 11

5.3.1 التوثيق 12

6.3.1 المساءلة 12

7.3.1 إخفاء الهوية 12

8.3.1 القدرة على التحمل 12

4.1 أنواع التشفير. 12

1.4.1 التشفير المتماثل. 12

5.1 التشفير غير المتماثل 13

6.1 التشفير على الوسائط المتعددة 14

7.1 أدوات التشفير للنصوص والصور وملفات الصوت 17

8.1 مقارنة بين أدوات التشفير 21
9.1 الخاتمة 21

2 الفصل الثاني: لغات البرمجة والمكتبات المستخدمة 22
1.2 المقدمة 22
2.2 لغات البرمجة 22
3.2 المكتبات والوحدات المستخدمة 22
4.2 إدارة قاعدة البيانات 25

3 الفصل الثالث : تصميم النظام وتطبيقه 27

الخلاصة العام 33

المراجع 34

قائمة الجداول

1.1 مقارنة بين أدوات التشفير المختلفة 21

قائمة الأشكال

1.1 مثال على عملية AES [4] 13
2.1 االتجارب بين أنواع التشفير المختلفة على الصورة 15
3.1 آلية مدمجة للتشفير والتخبئة في التواصل الآمن [8] 16
4.1 واجهة OpenPuff [9] 17
5.1 واجهة StegHide [10] 18
6.1 واجهة SilentEye [11] 19
7.1 واجهة VeraCrypt [12] 20

1.2 جدول يوضع هيكلة الداتا 26
2.2 واجهة SQLCipher [22] 26

1.3 واجهة الدخول 28
2.3 واجهة تشفير النصوص باستخدام AES 29
3.3 واجهة تشفير الصور باستخدام AES 29
4.3 واجهة تشفير باستخدام RSA 30
5.3 واجهة تشفير باستخدام RSA 31
6.3 واجهة إخفاء النصوص في الملفات الصوتية 32

المقدمة

في عصرٍ تتسارع فيه وتيرة التطور التكنولوجي وتزداد فيه الاعتماد على الأنظمة الرقمية في معالجة البيانات وتخزينها، يشكل مجال علوم الحاسوب ركيزةً أساسيةً لهذه التحولات، حيث يساهم في تطوير تقنيات ذكية تُحسّن من جودة الحياة وتُسهم في تطوير الصناعات والقطاعات المختلفة. ومع التوسع الكبير في استخدام هذه التقنيات، نشأت تحديات جديدة تتعلق بأمن المعلومات، لا سيما في ظل انتشار جرائم سرقة البيانات والاختراقات الأمنية التي تستهدف معلومات حساسة تشمل الصور، والفيديوهات، والصوتيات.

تُبرز هذه الظاهرة خطورة الاعتماد المطلق على الأنظمة التقليدية في حماية البيانات، حيث أن كل ثغرة أمنية قد تؤدي إلى تسرب المعلومات واستخدامها في أغراض غير مشروعة، مما يعرّض الأفراد والمؤسسات لمخاطر جسيمة مثل فقدان الثقة وتكبد خسائر مالية ومعنوية. وفي هذا السياق، تعتبر تقنيات التشفير والإخفاء من الأدوات الحيوية التي تسهم في رفع مستوى الأمان، إذ تعمل على حماية البيانات من الوصول غير المصرح به والتلاعب بها.

من هنا، يهدف هذا المشروع إلى برمجة تطبيق سطح مكتب يستخدم تقنيات التشفير الحديثة، جنبًا إلى جنب مع تقنيات الإخفاء (Steganography) لتوفير حلٍ متكامل وفعّال يحمي البيانات الحساسة من عمليات السرقة والاختراق. يقوم التطبيق بتحويل الملفات الرقمية مثل الصور والفيديوهات والصوتيات إلى بيانات مشفرة يُستحيل قراءتها دون الحصول على المفتاح الصحيح، مما يعزز من مستوى الأمان والحماية. كما يتيح التطبيق إمكانية إخفاء المعلومات داخل وسائط رقمية أخرى، مما يضيف طبقة إضافية من الحماية ويجعل من عملية استخراج البيانات دون المعرفة الدقيقة بأسلوب التشفير شبه مستحيلة.

بهذه الطريقة، يسعى المشروع إلى تقديم مساهمة عملية في مجال أمن المعلومات داخل علوم الحاسوب، من خلال اعتماد منهجيات وتقنيات متقدمة تهدف إلى مواجهة التحديات المعاصرة في عالم الأمن السيبراني وحماية البيانات وذلك من خلال الفصول التالية:

- الفصل الأول: سيتم فيه تقديم دراسة تمهيدية عن التشفير ومبادئه الأساسية التي تضمن فعاليته، وأنواعه، ومناقشة أدوات التشفير للنصوص والصور وملفات الصوت.

- الفصل الثاني: يتناول شرح لغات البرمجة والمكتبات المستخدمة، بالإضافة إلى إدارة قواعد البيانات.
- الفصل الثالث: سيتم فيه توضيح التشفير باستخدام خوارزمية "المعيار المتقدم للتشفير" (AES) وخوارزمية "ريفيست-شامير-أدلمان" (RSA) لتشفير النصوص والصور والفيديوهات، مع شرح خوارزمية التخبئة ودمجها مع التشفير.

الفصل الأول:مقدمة في عل التشفير

1.1 المقدمة

يُعد التشفير تقنية أساسية لحماية البيانات الرقمية من خلال تحويلها إلى صيغة غير قابلة للقراءة، مما يضمن أن الأطراف المخوّلة فقط هي التي تستطيع الوصول إليها. ومع تزايد التهديدات السيبرانية، أصبح التشفير يلعب دورًا جوهريًا في تأمين المعلومات الحساسة، سواء في الاتصالات أو التخزين أو المعاملات. يقدّم هذا الفصل نظرة عامة على التشفير، ومبادئه، والأدوات التي تسهّل التعامل الآمن مع البيانات.

2.1 بعض التعريفات

1.2.1 علم التشفير

علم التشفير هو علم تشفير وتأمين المعلومات لحمايتها من الوصول غير المصرح به. ويتضمن إنشاء خوارزميات تضمن سرية البيانات، نزاهتها، التوثيق، وعدم التنصل منها.[1]

2.2.1 التشفير

التشفير هو تقنية تشفير تتحول من خلالها البيانات القابلة للقراءة (النص العادي) إلى صيغة غير قابلة للقراءة (النص المشفر) باستخدام خوارزمية تشفير ومفتاح. ويُعيد فك التشفير هذه العملية لاستعادة البيانات الأصلية.[2]

3.2.1 تحليل التشفير

تحليل التشفير هو دراسة كسر آليات الأمان في علم التشفير لاكتشاف الثغرات. ويتضمن تقنيات لفك تشفير البيانات المشفرة دون الوصول إلى مفتاح فك التشفير، مما يساعد في تحسين خوارزميات التشفير.[3]

3.1 جوانب الأمان

عدة مبادئ أساسية تضمن فعالية التشفير في تأمين البيانات الرقمية:[4]

1.3.1 النزاهة

تضمن النزاهة أن تظل البيانات غير معدّلة أثناء التخزين أو النقل. تُستخدم دوال التجزئة (مثل SHA-256) والتوقيعات الرقمية للتحقق من نزاهة البيانات.

2.3.1 التوافر

يضمن التوافر أن البيانات تكون متاحة للمستخدمين المصرح لهم عند الحاجة. تشمل آليات الأمان، بما في ذلك التكرار، استراتيجيات النسخ الاحتياطي، وحمايات من هجمات حجب الخدمة، لضمان التوافر.

3.3.1 السرية

تضمن السرية أن المعلومات متاحة فقط للأشخاص المصرح لهم. تحمي طرق التشفير مثل AES و RSA البيانات من الوصول غير المصرح به.

4.3.1 عدم التنصل

تضمن عدم التنصل أن المرسل لا يستطيع إنكار إرسال الرسالة، وأن المستقبل لا يستطيع إنكار استلامها. تُستخدم التوقيعات الرقمية وتكنولوجيا البلوكشين عادة لضمان عدم التنصل.

5.3.1 التوثيق

يضمن التوثيق التحقق من هوية المستخدمين أو الأنظمة قبل السماح بالوصول إلى البيانات المشفرة. يمنع هذا المستخدمين غير المصرح لهم من الوصول إلى المعلومات الحساسة. يتم استخدام تقنيات مثل كلمات المرور، التوثيق متعدد العوامل ،(MFA) والشهادات الرقمية للتوثيق.

6.3.1 المساءلة

تضمن المساءلة أن الإجراءات المتعلقة بالتشفير وفك التشفير يمكن تتبعها إلى كيان معين. تساعد آليات التسجيل والمراجعة في تتبع من وصل إلى البيانات المشفرة أو عدّل عليها، مما يعزز الامتثال الأمني.

7.3.1 إخفاء الهوية

يضمن إخفاء الهوية أنه حتى إذا تم اعتراض البيانات المشفرة، فلا يمكن تتبعها إلى مستخدمين محددين. وهذا أمر بالغ الأهمية في تقنيات الحفاظ على الخصوصية مثل شبكات ،VPN شبكات ،Tor وإثباتات المعرفة الصفرية.

8.3.1 القدرة على التحمل

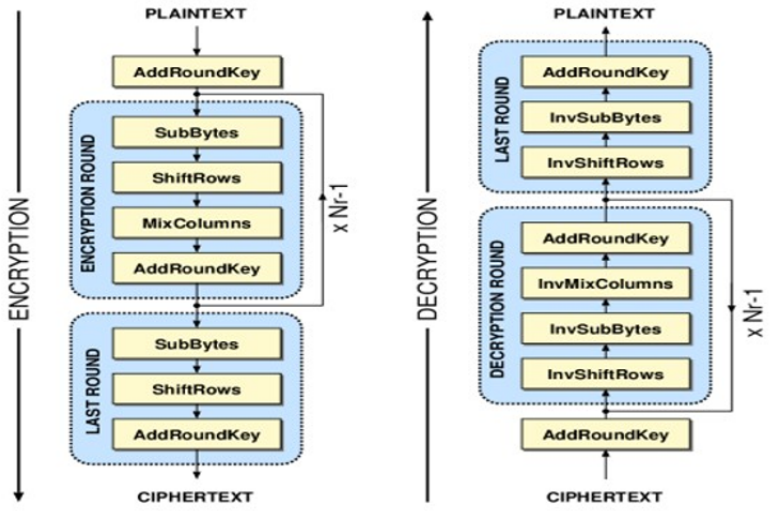
تشير القدرة على التحمل إلى قدرة نظام التشفير على الصمود في وجه الهجمات، بما في ذلك الهجمات التشفيرية والتلاعب الفيزيائي. ويتضمن ذلك استخدام خوارزميات تشفير قوية، وإدارة مفاتيح آمنة، ومقاومة للهجمات الجانبية.

4.1 أنواع التشفير

1.4.1 التشفير المتماثل

يستخدم التشفير المتماثل نفس المفتاح لكل من التشفير وفك التشفير. إنه فعال ولكنه يتطلب طريقة آمنة لمشاركة المفتاح. تشمل الأمثلة:

- **معيار التشفير المتقدم :(AES)** معيار تشفير معتمد على نطاق واسع ويعرف بقوته وكفاءته.



شكل 1.1: مثال على عملية AES [4]

- **معيار التشفير البياني :(DES)** خوارزمية تشفير قديمة تم استبدالها بـ AES بسبب القيود الأمنية.

5.1 التشفير غير المتماثل

يستخدم التشفير غير المتماثل مفتاحين: مفتاحًا عامًا للتشفير وآخر خاصًا لفك التشفير. يساهم هذا النوع من التشفير في تعزيز الأمان، ولكنه يتطلب موارد حسابية كبيرة. ومن أبرز الأمثلة على التشفير غير المتماثل:

- **تشفير ريفست-شامير-أدلمان :(RSA)** نظام تشفير شائع يستخدم لتأمين الاتصالات الرقمية والتوقيعات الإلكترونية.
- **تشفير المنحنى الإهليلجي :(ECC)** نهج حديث يوفر أمانًا قويًا باستخدام مفاتيح أصغر حجمًا، مما يجعله أكثر كفاءة من RSA [5].

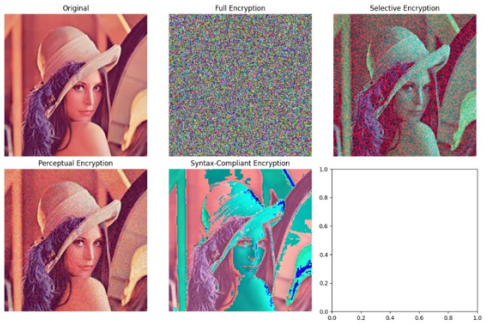
6.1 التشفير على الوسائط المتعددة

يختلف تشفير الوسائط المتعددة عن التشفير التقليدي نظرًا لتعقيد البيانات الرقمية التي يتعامل معها [6]. وعلى عكس تقنيات التشفير الكلاسيكية التي تركز على النصوص أو البيانات المهيكلة، فإن تشفير الوسائط المتعددة يجب أن يأخذ بعين الاعتبار تحديات إضافية مثل:

- **البساطة المنخفضة:** يجب أن يكون فعالًا من حيث الأداء لتمكين المعالجة في الوقت الحقيقي، خصوصًا على الأجهزة ذات الموارد المحدودة مثل الهواتف الذكية، أجهزة إنترنت الأشياء (IoT)، والأنظمة المدمجة [6].
- **التحكم في تسريب المحتوى:** يجب منع الوصول غير المصرح به مع السماح بمستويات وصول انتقائية حسب أذونات المستخدم [6].
- **كفاءة الضغط:** ينبغي أن تتكامل تقنيات التشفير مع خوارزميات الضغط دون التأثير الكبير على الأداء أو التخزين [6].
- **المرونة في مواجهة الأخطاء:** يجب أن يكون النظام قادرًا على الصمود في وجه فقدان الحزم أو أخطاء الشبكة، خاصة في بيئات البث اللاسلكي [6].
- **القدرة على التكيف والتوسع:** من الضروري دعم تنسيقات وسائط متعددة مختلفة وتوفير تحكم مرن في الوصول [6].
- **الامتثال للقواعد النحوية:** ينبغي أن تظل الملفات المشفرة قابلة للتشغيل باستخدام برامج فك التشفير القياسية [6].

تشمل تقنيات تنفيذ تشفير الوسائط المتعددة:

- **التشفير الكامل:** يتم فيه تشفير الملف بالكامل، ويوفر مستوى أمان عالٍ لكنه يتطلب موارد حسابية كبيرة. يُستخدم في التطبيقات ذات الحساسية الأمنية العالية مثل الاتصالات العسكرية [7].
- **التشفير الانتقائي:** يركّز على تشفير الأجزاء الأهم من المحتوى مثل إطارات I في الفيديو أو متجهات الحركة، مما يحقق توازنًا بين الأمان والكفاءة [7].



شكل 2.1: االتجارب بين أنواع التشفير المختلفة على الصورة

- **التشفير الإدراكي:** يسمح بعرض المحتوى بطريقة مشوشة للمستخدمين غير المصرح لهم، ما يفيد في خدمات الاشتراك ذات الوصول المتدرج [7].
- **التشفير المتكامل مع الضغط:** يدمج التشفير في عملية الضغط لتعزيز الكفاءة، وهو مفيد في بيئات محدودة النطاق أو التخزين [6].
- **التشفير المتوافق مع القواعد النحوية:** يحافظ على توافق الملفات المشفرة مع برامج الترميز القياسية، مما يسهل توزيعها وتشغيلها [7].

التخبئة :(Steganography) نظرة عامة

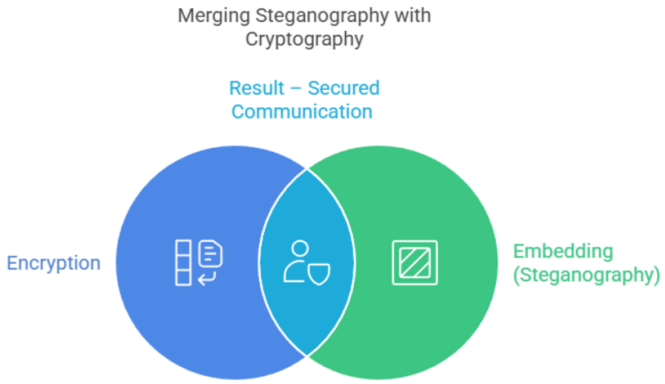
تُعرف التخبئة بأنها علم وفن إخفاء المعلومات داخل وسائط رقمية بطريقة تخفي وجود الرسالة ذاتها، بخلاف التشفير الذي يهدف إلى إخفاء محتوى الرسالة فقط. وتُعد التخبئة وسيلة فعالة لتحقيق إخفاء تام للاتصال الرقمي [8].

دمج التشفير مع التخبئة

يُتيح الجمع بين التشفير والتخبئة تحقيق طبقة أمان مزدوجة:

1. **المرحلة الأولى: التشفير** — يُشفَّر المحتوى الأصلي باستخدام خوارزمية مثل AES أو RSA.
2. **المرحلة الثانية: التخبئة** — يُدمج النص المشفر داخل وسيط (مثل صورة أو ملف صوتي) باستخدام تقنيات مثل LSB.

3. **النتيجة** — حتى إذا تم اكتشاف الوسيط المعدل، فإن محتواه المشفر يبقى غير قابل للفهم دون مفتاح فك التشفير.



شكل 3.1: آلية مدمجة للتشفير والتخبئة في التواصل الآمن [8]

أنواع تقنيات التخبئة

فيما يلي نظرة عامة على أبرز أنواع التخبئة الرقمية [8]:

- **تخبئة الصور:** تشمل تقنيات مثل LSB وتضمين البيانات في مجالات التردد (DCT/DWT).
- **تخبئة الصوت:** تستخدم تقنيات مثل إخفاء الصدى وترميز الطور إلى جانب LSB.
- **تخبئة الفيديو:** يتم تضمين البيانات عبر الإطارات مع الاستفادة من الخصائص الزمنية والمكانية للفيديو.
- **تخبئة النصوص:** تعتمد على تغييرات تنسيقية أو لغوية غير مرئية.
- **تخبئة الشبكات:** تُدمج البيانات داخل رؤوس البروتوكولات مثل TCP/IP.
- **تخبئة المستندات:** تستغل البيانات الوصفية وخصائص التنسيق غير الظاهرة.

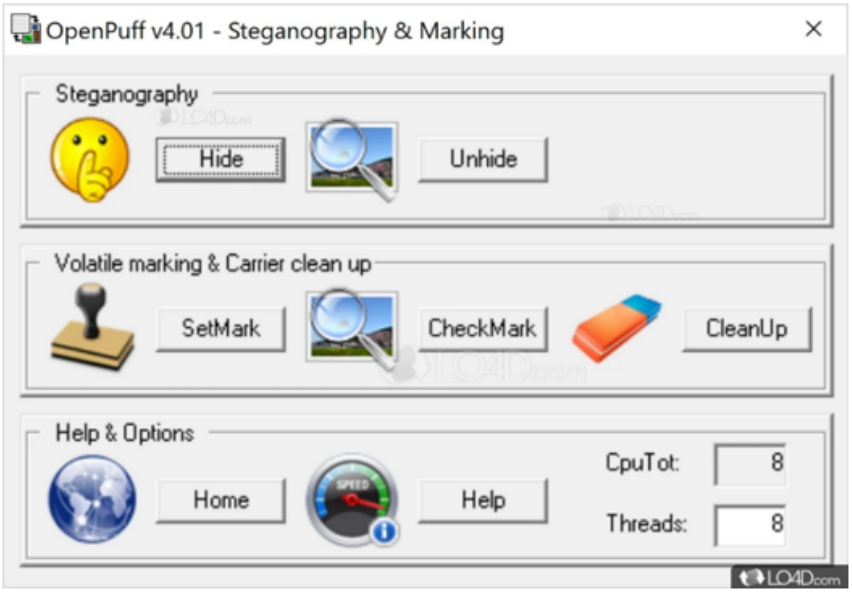
7.1 أدوات التشفير للنصوص والصور وملفات الصوت

توفر العديد من أدوات التشفير الأمان لمختلف أنواع الملفات، مما يضمن الحفاظ على السرية وسلامة البيانات. فيما يلي بعض التطبيقات البارزة:

5.1 OpenPuff

أداة قوية للتخفي الرقمي (ستيجانوجرافي) تدعم التشفير وإخفاء البيانات داخل الصور، الفيديوهات، وملفات الصوت. **المميزات:**

- تشفير متعدد الطبقات من أجل أمان قوي.
- يدعم تنسيقات وسائط متعددة لإخفاء البيانات.
- مثالي للتواصل السري ومشاركة الملفات بشكل آمن.



شكل 4.1: واجهة OpenPuff [9]

5.2 StegHide

أداة للتخفي الرقمي تخفي البيانات المشفرة داخل ملفات الصور والصوت دون التسبب في تدهور ملحوظ في الجودة.

شكل 5.1: واجهة StegHide [10]

المميزات:

- خفيف ويعمل من خلال سطر الأوامر.
- يدعم تنسيقات الملفات JPEG وWAV.
- يستخدم التشفير القائم على عبارة مرور (Passphrase) لتحقيق الأمان.

5.3 SilentEye

أداة تشفير متعددة المنصات تتيح للمستخدمين إخفاء الرسائل النصية داخل الصور وملفات الصوت.

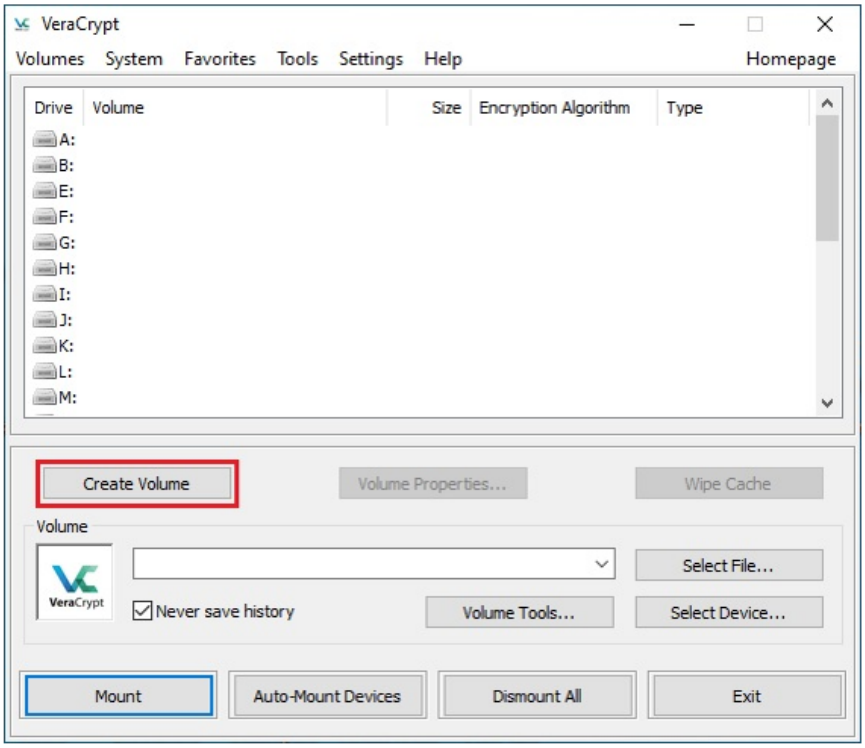
شكل 6.1: واجهة SilentEye [11]

المميزات:

- واجهة رسومية سهلة الاستخدام.
- دعم لتقنيات الإخفاء في الصور والصوت.
- تشفير أساسي لدمج البيانات بأمان.

5.4 VeraCrypt

برنامج تشفير شائع يُستخدم لتأمين الملفات وأجزاء التخزين بالكامل.



شكل 7.1: واجهة VeraCrypt [12]

المميزات:

- خوارزميات تشفير، AES، Serpent وTwofish.
- ميزة ``الوحدة المخفية" لتعزيز الأمان.
- دعم متعدد المنصات، (Windows، Linux وmacOS).

8.1 مقارنة بين أدوات التشفير

جدول 1.1: مقارنة بين أدوات التشفير المختلفة

الميزة	OpenPuff	StegHide	SilentEye	VeraCrypt
تشفير AES/RSA	✗	✗	✗	✓
إخفاء في الصور	✓	✓	✓	✗
إخفاء في الصوت	✗	✓	✓	✗
واجهة سهلة الاستخدام	✗	✗	✓	✓
دعم تنسيقات الملفات	الصور والفيديو	JPEG وWAV	الصوت والصور	الصوت والقرص بالكامل

توفر أدوات التشفير هذه مستويات مختلفة من الأمان وسهولة الاستخدام، لتلبية احتياجات متنوعة مثل الإخفاء داخل الوسائط ،(Steganography) وتشفير الملفات، وحماية وحدات التخزين.

9.1 الخاتمة

يُعدّ التشفير عنصرًا أساسيًا في أمن المعلومات السيبراني، حيث يحمي البيانات الرقمية من الوصول غير المصرح به والتهديدات السيبرانية. إن فهم المبادئ التشفيرية واستخدام أدوات موثوقة يعزز من حماية البيانات.

ومع تطور التهديدات الأمنية، ستكون التحسينات المستمرة في تقنيات التشفير ضرورية للحفاظ على الخصوصية الرقمية وسلامة المعلومات. في هذا السياق، قدم هذا التقرير أداة **SecureShield**، وهي أداة مقترحة تهدف إلى تقديم ميزات أمان محسّنة للنصوص والصور وملفات الصوت. وتسعى **SecureShield** إلى دمج خوارزميات تشفير قوية مع واجهة استخدام بسيطة، لضمان الوصول السهل إلى البيانات دون المساس بمستوى الحماية.

الفصل الثاني: لغات البرمجة والمكتبات المستخدمة

1.2 المقدمة

في هذا الفصل، نناقش لغات البرمجة والمكتبات التي تم استخدامها في تنفيذ المشروع. تتضمن هذه المكتبات عدة وحدات ضرورية لوظائف التشفير، وواجهات المستخدم الرسومية، وإدارة قواعد البيانات، وعمليات النظام.

2.2 لغات البرمجة

تم تطوير المشروع أساسًا باستخدام لغة بايثون ،(Python) وهي لغة قوية ومتعددة الاستخدامات تُستخدم على نطاق واسع في تطبيقات الأمان نظرًا لمكتباتها الغنية، وسهولة تنفيذها، والدعم القوي الذي توفره للعمليات التشفيرية [13].

3.2 المكتبات والوحدات المستخدمة

Subprocess

تُستخدم هذه الوحدة لتنفيذ أوامر على مستوى النظام من داخل سكربت بايثون، مما يتيح التفاعل مع نظام التشغيل وتشغيل تطبيقات خارجية [14].

PyQt5

PyQt5 هي ربط بايثون مع إطار عمل ،Qt وتوفر أدوات لإنشاء تطبيقات رسومية تعمل على مختلف المنصات. وتتكون من الوحدات الأساسية التالية [15]:

- **PyQt5.QtWidgets**: تتضمن عناصر واجهة المستخدم الأساسية لبناء تطبيقات تفاعلية، مثل:
  - QMessageBox QPushButton, QLineEdit, QLabel, QWidget, QApplication,
  - QFileDialog, QTextEdit, QHBoxLayout, QVBoxLayout, QShortcut, QDesktopWidget
- **PyQt5.QtCore**: توفر وظائف أساسية مثل معالجة الأحداث ودعم بيانات MIME.
- **PyQt5.QtGui**: تدعم الخطوط، الصور، واختصارات لوحة المفاتيح.

Sys

تُستخدم هذه الوحدة للتفاعل مع النظام، مثل التعامل مع وسيطات سطر الأوامر، وتنفيذ السكربت، والوظائف الخاصة بالنظام [14].

sqlite3

توفر هذه المكتبة واجهة للتعامل مع قواعد بيانات SQLite، مما يسمح للمشروع بتخزين وإدارة بيانات اعتماد المستخدمين بأمان [14].

Re (التعابير النمطية)

تُستخدم وحدة *re* لمطابقة الأنماط والتحقق من صحة المُدخلات، وذلك لضمان توافق بيانات اعتماد المستخدمين مع التنسيقات الصحيحة [14].

Crypto.Cipher

تتضمن هذه الوحدة خوارزميات التشفير وفك التشفير التالية [16]:

- معيار التشفير المتقدم (AES)
- PKCS1_OAEP للحشو الأمثل لتشفير RSA

Crypto.Util.Padding

توفر هذه الوحدة وظائف لضمان أن البيانات محشوة بشكل صحيح قبل التشفير [16]:

- *pad*: يُضيف الحشو إلى النص قبل التشفير.
- *unpad*: يُزيل الحشو بعد فك التشفير.

base64

يُستخدم ترميز Base64 لتحويل البيانات الثنائية إلى أحرف ASCII، مما يجعلها مناسبة للتخزين والنقل [14].

(cv2) OpenCV

مكتبة رؤية حاسوبية توفر وظائف لمعالجة الصور. وتُستخدم في هذا المشروع لتشفير وفك تشفير الصور بشكل آمن [17].

(np) numpy

مكتبة للحوسبة العددية تُستخدم في عمليات المصفوفات والتعامل مع المصفوفات، وتلعب دورًا أساسيًا في تشفير الصور [18].

os

توفر هذه الوحدة وظائف للتفاعل مع نظام التشغيل، مثل التعامل مع نظام الملفات والمتغيرات البيئية [14].

Pydub

تُستخدم مكتبة Pydub لمعالجة الصوت، خاصة عند التعامل مع ملفات الصوت [19]:

- *AudioSegment*: توفر أدوات لتحويل وتعديل صيغ الصوت.

shutil

تُستخدم وحدة *shutil* لإجراء عمليات عالية المستوى على الملفات [14]:

- *which*: تُساعد في تحديد مكان التبعيات الخارجية.

rsa

تُنفذ هذه الوحدة خوارزمية تشفير RSA لتأمين نقل البيانات والمصادقة [16].

Crypto.PublicKey

تحتوي هذه الوحدة على أدوات لإدارة مفاتيح التشفير [16]:

- *RSA*: تُستخدم لإنشاء وإدارة مفاتيح RSA للتشفير وفك التشفير.

4.2 إدارة قاعدة البيانات

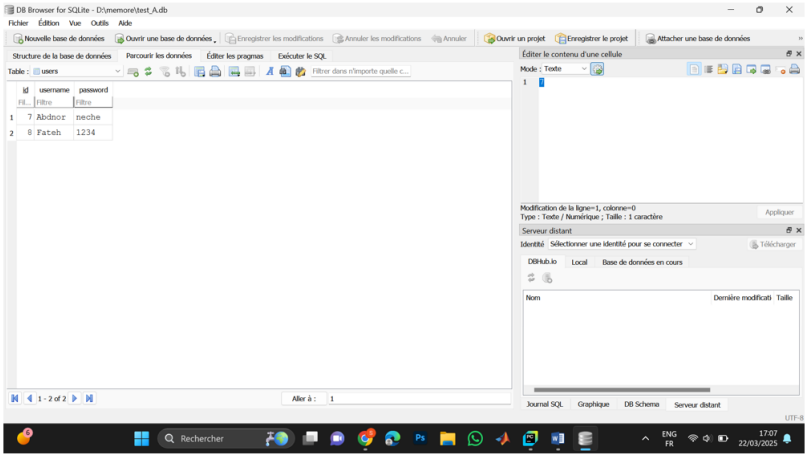
نستخدم قاعدة بيانات SQLite مع تشفير SQLCipher لتخزين أسماء المستخدمين وكلمات المرور بأمان. SQLCipher هو امتداد مفتوح المصدر لـ SQLite ويوفر تشفيرًا شفافًا باستخدام AES-256 [20].

أدوات إدارة قاعدة البيانات المستخدمة

- **SQLite for Browser DB**: أداة بواجهة رسومية تتيح للمستخدمين التفاعل مع قاعدة البيانات، وتنفيذ الاستعلامات، وإدارة البيانات المخزنة [21].
- **SQLCipher**: يضمن أن تظل بيانات اعتماد المستخدمين مشفّرة ومحميّة من الوصول غير المصرح به [22].

Field Name	Data Type	Description
id	INTEGER PRIMARY KEY	Unique identifier for each user
username	TEXT	Stores the username
password	TEXT (Encrypted)	Stores the hashed password

شكل 1.2: جدول يوضع هيكلة الداتا



شكل 2.2: واجهة SQLCipher [22]

خلاصة

في هذا الفصل، استعرضنا الأدوات البرمجية المستخدمة في تطوير المشروع، بما في ذلك لغة البرمجة بايثون والمكتبات الأساسية التي تدعم الوظائف الأمنية، الرسومية، وإدارة البيانات. تم اختيار هذه الأدوات بناءً على كفاءتها، توافقها، ودعمها لمتطلبات المشروع. توفر هذه البنية البرمجية أساسًا قويًا لبناء نظام آمن وفعال. في الفصل التالي، سنتناول تصميم وتنفيذ الواجهة الرسومية للمستخدم (GUI)، حيث سنوضح كيفية تفاعل المستخدم مع النظام، والعناصر التفاعلية التي تتيح إدارة الوظائف الأمنية بشكل مرئي وسهل الاستخدام.

الفصل الثالث : تصميم النظام وتطبيقه

المقدمة

برنامج **SecureShield** هو أداة متكاملة لتأمين البيانات من خلال تقنيات التشفير المختلفة، بما في ذلك AES وRSA بالإضافة إلى إخفاء البيانات في الملفات الصوتية .(Steganography) يتميز البرنامج بواجهة سهلة الاستخدام تتيح للمستخدمين تشفير وفك تشفير النصوص والصور والملفات الصوتية.

صفحة تسجيل الدخول (Login)

يبدأ البرنامج بصفحة تسجيل الدخول كما هو موضح في الصورة **Screenshot_1.png**:

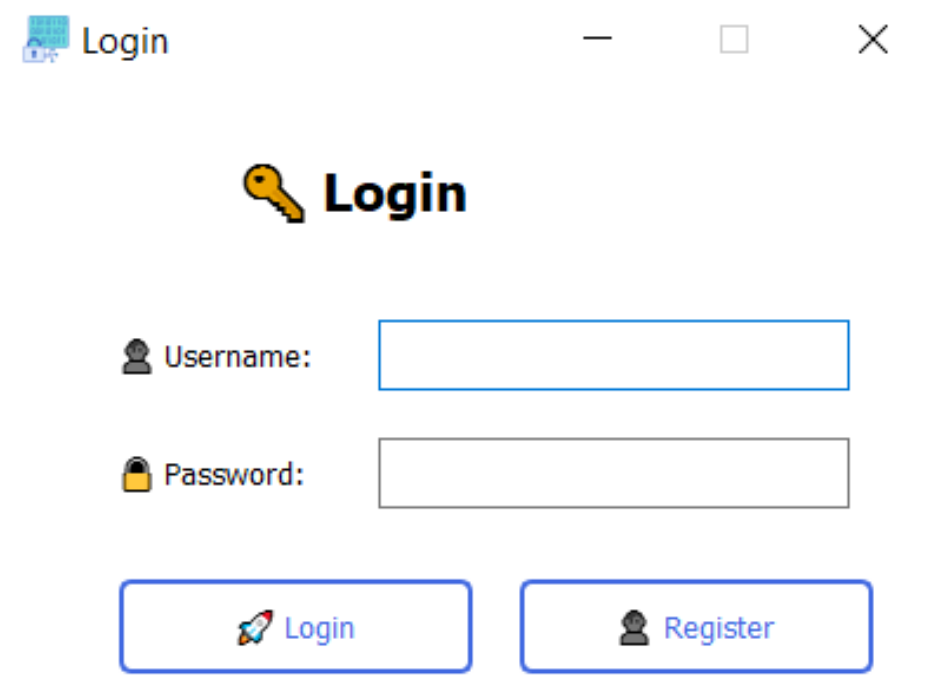
- **حقل اسم المستخدم (Username)**: لإدخال اسم المستخدم.
- **حقل كلمة المرور (Password)**: لإدخال كلمة المرور.
- **زر تسجيل الدخول (Login)**: للدخول إلى النظام.
- **زر التسجيل (Register)**: لإنشاء حساب جديد.

واجهات البرنامج الرئيسية

1. واجهة تشفير النصوص باستخدام AES

كما في الصورة 2.3:

- **حقل إدخال المفتاح (Enter the KEY)**: لإدخال مفتاح التشفير.



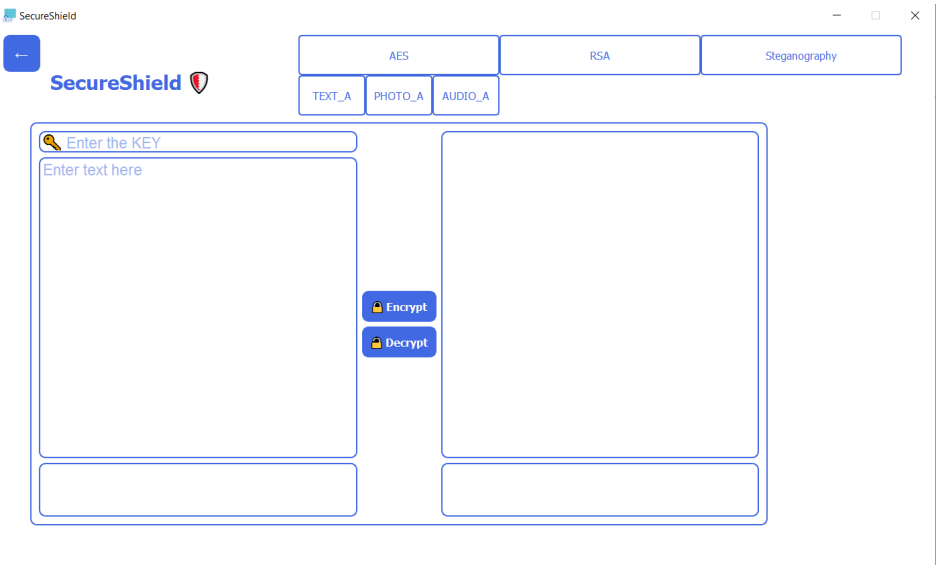
شكل 1.3: واجهة الدخول

- **حقل إدخال النص (Enter text here)**: لإدخال النص المراد تشفيره أو فك تشفيره.
- **خيارات التشفير (AES, RSA, Steganography)**: لتحديد خوارزمية التشفير.
- **أزرار التشفير وفك التشفير (Encrypt/Decrypt)**: لتنفيذ العملية المطلوبة.

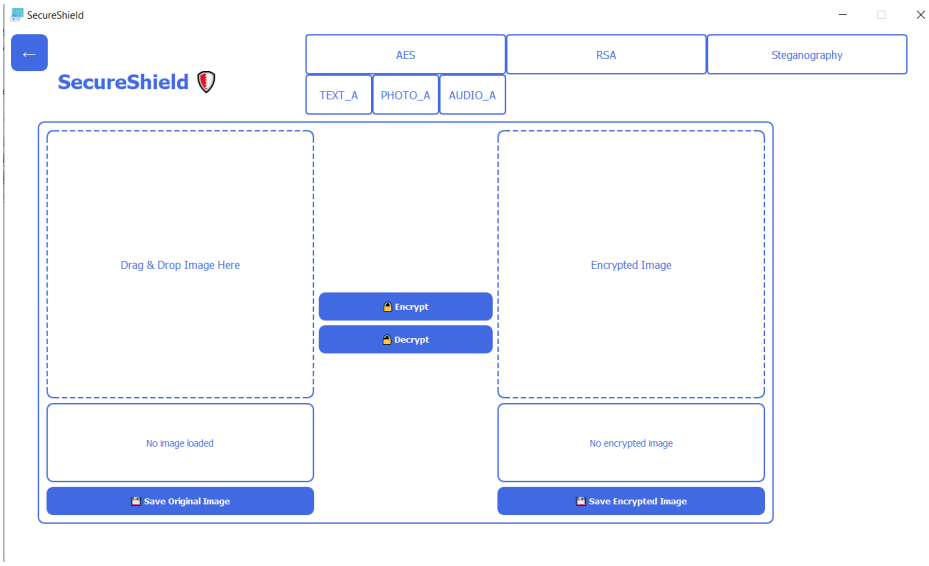
2. واجهة تشفير الصور باستخدام AES

كما في الصورة 3.3:

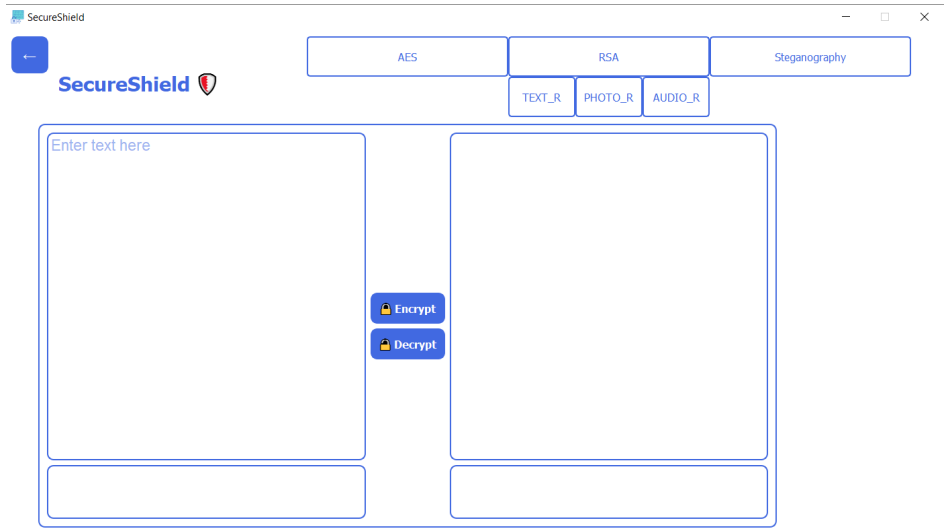
- **منطقة سحب وإسقاط الصورة (Drag & Drop Image Here)**: لتحميل الصورة.
- **خيار التشفير أو فك التشفير (Encrypt/Decrypt)**: لتحديد العملية.
- **حالة الصورة (No image loaded)**: تظهر عند عدم تحميل صورة.
- **أزرار الحفظ (Save Encrypted Image, Original Image)**: لحفظ الصورة الأصلية أو المشفرة.



شكل 2.3: واجهة تشفير النصوص باستخدام AES



شكل 3.3: واجهة تشفير الصور باستخدام AES



شكل 4.3: واجهة تشفير باستخدام RSA

3. واجهة تشفير النصوص باستخدام RSA

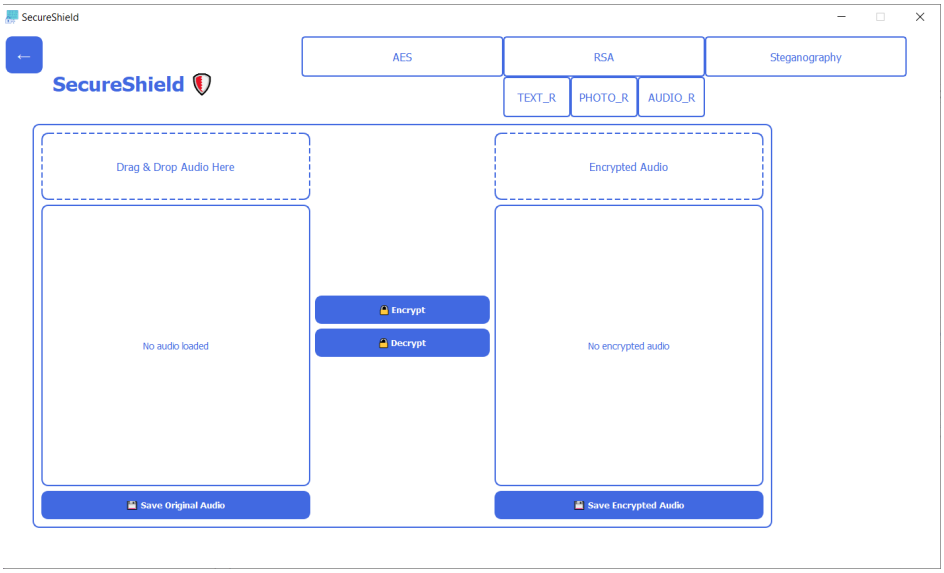
كما في الصورة 4.3:

- **حقل إدخال النص (Enter text (here**: لإدخال النص المراد تشفيره أو فك تشفيره.
- **خيارات التشفير (AES, RSA) Steganography**: لتحديد الخوارزمية.
- **أزرار التشفير وفك التشفير (Encrypt/Decrypt)**: لتنفيذ العملية.

5. واجهة تشفير الملفات الصوتية باستخدام AES وRSA

كما في الصور 5.3

- **منطقة سحب وإسقاط الملف الصوتي (Drag & Drop Audio (Here**: لتحميل الملف الصوتي.
- **حالة الملف الصوتي (No audio (loaded**: تظهر عند عدم تحميل ملف صوتي.
- **أزرار الحفظ (Save Audio, Original Encrypted Audio)**: لحفظ الملف الأصلي أو المشفر.
- **خيارات التشفير (AES, RSA) Steganography**: لتحديد الخوارزمية.



شكل 5.3: واجهة تشفير باستخدام RSA

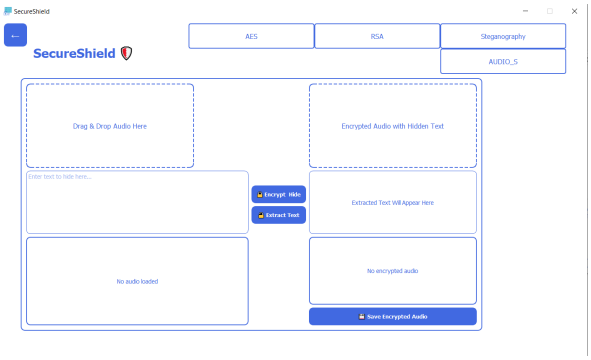
4. واجهة إخفاء النصوص في الملفات الصوتية (Steganography)

كما في الصور audio: stega

- منطقة سحب وإسقاط الملف الصوتي (Drag & Drop Audio Here): لتحميل الملف الصوتي.
- حقل إدخال النص (Enter text to hide here...): لإدخال النص المراد إخفائه.
- أزرار التشفير (Encrypt Text, Hidden with Add Hide): لإخفاء النص في الملف الصوتي.
- منطقة عرض النص المستخرج (Extracted Text Will Appear Here): لعرض النص المستخرج من الملف الصوتي.
- أزرار الحفظ (Save Encrypted Audio): لحفظ الملف الصوتي المشفر.

الخاتمة

يوفر برنامج **SecureShield** حلاً شاملاً لتأمين البيانات عبر تقنيات متعددة، مما يجعله أداة مثالية للأفراد والمؤسسات الذين يسعون إلى حماية معلوماتهم الحساسة. يتميز البرنامج بواجهات سهلة



شكل 6.3: واجهة إخفاء النصوص في الملفات الصوتية

الاستخدام تدعم تشفير النصوص والصور والملفات الصوتية بكفاءة عالية.

الخلاصة العام

في ظل التطورات المتسارعة في تكنولوجيا المعلومات وزيادة التهديدات الإلكترونية، أصبحت حماية البيانات الرقمية من أولويات أمن المعلومات. ومن بين أبرز هذه التهديدات نجد عمليات سرقة البيانات، والتجسس الإلكتروني، والاختراقات التي تستهدف الوسائط المتعددة مثل الصور، والفيديوهات، والملفات الصوتية.

جاء هذا المشروع كاستجابة عملية لهذه التحديات، من خلال تصميم وتطوير تطبيق سطح مكتب يُمكّن المستخدم من تشفير بياناته الحساسة باستخدام خوارزميات تشفير قوية مثل RSA وAES، مع دمج هذه التقنيات بتقنيات التخبئة (Steganography) التي تهدف إلى إخفاء البيانات داخل وسائط رقمية أخرى بطريقة تجعل اكتشافها شبه مستحيل.

يُوفّر المشروع طبقتين من الحماية:

التشفير لحماية محتوى البيانات.

الإخفاء لحماية وجود البيانات نفسها.

وقد تم استخدام لغة بايثون إلى جانب مجموعة من المكتبات الحديثة مثل Crypto, PyQt5، OpenCV، وSQLite، لتوفير تجربة استخدام آمنة وسلسة.

يشكّل هذا المشروع محاولة عملية لتعزيز أمن المعلومات من خلال تطوير تطبيق سطح مكتب يدمج بين تقنيات التشفير والإخفاء لحماية البيانات الحساسة مثل النصوص، الصور، والصوتيات. تم الاعتماد على خوارزميات قوية مثل RSA وAES إلى جانب تقنيات التخبئة (Steganography) لإضافة طبقة مزدوجة من الأمان. يهدف التطبيق إلى تسهيل عملية حماية البيانات للمستخدم العادي بطريقة فعالة وآمنة.

وفي ظل التطور المتسارع في مجال الذكاء الاصطناعي، تفتح هذه التقنيات آفاقًا مستقبلية واعدة لتعزيز أمان البيانات بشكل ذكي وتلقائي، مما قد يسهم في تطوير أدوات أكثر فاعلية واستجابة للتهديدات الحديثة.

المراجع

[1] A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*. CRC Press, .1996

[2] D. R. Stinson and M. Paterson, *Cryptography: Theory and Practice*, 4th ed. CRC Press, .2018

[3] C. H. Bennett and G. Brassard, ``Quantum Cryptography: Public Key Distribution and Coin Tossing," in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, ,1984 pp. –175.179

[4] W. Bouras, *Security Mobile Inspired Quantum Cryptography*, Unpublished work, .2025

[5] ``Elliptic Curve Cryptography: A Basic Introduction." Accessed: Mar. ,20 .2025 ,(2025) [Online]. Available: https://blog.boot.dev/cryptography/elliptic-curve-cryptography/.

[6] A. Guesmi *et al.*, ``Challenges and Innovations in Multimedia Encryption and Information Security," *TechScience*, ,2023 https://www.techscience.com/cmc/special_detail/multimedia-encryption.

[7] S. Li *et al.*, ``Multimedia Encryption: A Brief Overview," in *Multimedia Security Technologies for Digital Rights Management*, Springer, ,2009 pp. –295 .312 [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-642-02900-4_16.

[8] T. Morkel, J. H. P. Eloff, and M. S. Olivier, ``An Overview of Image Steganography," in *Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA)*, .2005

[9] OpenBuff Project, *OpenBuff: Open-Source Encryption and Steganography Software*, .2024 [Online]. Available: https://example.com/openbuff.

[10] StegHide Project, *StegHide: A Steganography Tool for Hiding Data in Images and Audio*, .2024 [Online]. Available: https://packages.debian.org/stable/steghide.

[11] SilentEye Project, *SilentEye: Steganography Tool for Hiding Data in Images and Audio*, .2024 [Online]. Available: https://silenteye.v1engineering.com/.

[12] IDRIX, *VeraCrypt: Open-source Disk Encryption Software*, .2024 [Online]. Available: https://www.veracrypt.fr/.

[13] M. Lutz, *Learning Python*, 5th ed. O'Reilly Media, .2013

[14] D. Beazley and B. K. Jones, *Python Cookbook*, 3rd ed. O'Reilly Media, .2013

[15] M. Summerfield, *Rapid GUI Programming with Python and Qt: The Definitive Guide to PyQt Programming*. Prentice Hall, .2007

[16] P. Mishra, *Python Cryptography Cookbook*. Packt Publishing, .2019

[17] G. Bradski and A. Kaehler, *Learning OpenCV: Computer Vision with the OpenCV Library*, 2nd ed. O'Reilly Media, .2016

[18] W. McKinney, *Python for Data Analysis*, 2nd ed. O'Reilly Media, .2017

[19] *PyDub Project*. [Online]. Available: https://github.com/jiaaro/pydub.

[20] M. Owens, *The Definitive Guide to SQLite*. Apress, .2010

[21] *DB Browser for SQLite*. [Online]. Available: https://sqlitebrowser.org/.

[22] *SQLCipher*. [Online]. Available: https://www.zetetic.net/sqlcipher/.