إخفاء البيانات في الصور الرقمية

م.عهد خليل صافي د.لينا مراد

الملخص

يتناول هذا البحث إخفاء البيانات في الصور الرقمية باعتباره أحد الأساليب المتقدمة في أمن المعلومات، ضمن إطار علم التورية الرقمية(Steganography) ، الذي يهدف إلى إخفاء وجود البيانات لا مجرد محتواها. انطلق البحث من الحاجة الملحة إلى وسائل حماية أكثر تعقيداً تواكب تطور التهديدات السيبرانية، وقدّم خوارزمية هجينة متقدمة تدمج بين ضغط البيانات، وخوارزمية هامينغ لتصحيح الأخطاء، والتشفير المتماثل، بالإضافة إلى تقنيتي التحويل المويجي المتقطع (DWT)والبت الأقل أهمية (LSB) تم تنفيذ الخوارزمية عملياً وتحليل أدائها باستخدام مؤشرات معيارية مثل PSNR وMSE، حيث أثبتت التجارب كفاءتها العالية من حيث مقاومة التحليل الإحصائي، وزيادة سعة الإخفاء، والمحافظة على جودة الصورة البصرية.

الكلمات المفتاحية: التورية الرقمية ،إخفاء البيانات'الصور الرقمية، خوارزمية الهجينة ، التحويل المويجي(DWT) ،البت الأقل أهمية(LSB).

Hiding Data in Digital Image

Abstract

This research investigates the domain of data hiding within digital images as a critical approach to contemporary information security, specifically through the lens of digital steganography. Unlike cryptographic techniques that obscure content, steganography conceals the existence of the data itself. The proposed research introduces a hybrid algorithm that integrates data compression, hamming error correction, symmetric encryption, and dual embedding using both Discrete Wavelet Transform (DWT) and Least Significant Bit (LSB) substitution. The algorithm was implemented and evaluated under standard performance metrics such as Peak Signal-to-Noise Ratio (PSNR) and Mean Squared Error (MSE). Experimental outcomes indicate superior performance in terms of visual imperceptibility, resistance to statistical attacks, and high embedding capacity.

Keywords: Digital Steganography, Data Hiding, Digital Images, Hybrid Algorithm, Discrete Wavelet Transform (DWT), Least Significant Bit (LSB).

1-المقدمة:

مع التطور السريع في تقنيات الاتصال وتبادل المعلومات، أصبحت حماية البيانات الرقمية أحد أبرز التحديات التي تواجه الأفراد والمؤسسات. لم تعد التهديدات الأمنية محصورة في الوصول غير المصرّح به، بل تطورت لتشمل اعتراض البيانات وتحليلها والتلاعب بها بوسائل معقدة. في هذا السياق، ظهرت التورية الرقمية(Steganography) كفرع متخصص من علوم أمن المعلومات، يركّز على إخفاء وجود البيانات ذاتها داخل وسائط متعددة، بما يجعل اكتشافها أمراً بالغ الصعوبة حتى باستخدام التحليل المتقدم.

وعلى خلاف التشفير، الذي يُحوّل البيانات إلى صيغة غير مقروءة ولكن قابلة للاشتباه، تهدف التورية إلى جعل البيانات "غير مرئية" كلياً ضمن وسيط مثل صورة أو ملف صوتي، دون أي مؤشر على وجودها. هذا يجعل من التورية خياراً مثالياً في الحالات التي يُشكّل فيها وجود التشفير بحد ذاته خطراً أو دافعاً للهجوم.

تُعد الصور الرقمية من أكثر الوسائط استخداماً في عمليات الإخفاء، لما تتميز به من انتشار واسع، وبنية بيانات غنية تسمح بتضمين معلومات دون التأثير الملحوظ على الجودة. بناءً على ذلك، تختلف تقنيات الإخفاء باختلاف خصائص الصورة، وحجم البيانات، ومتطلبات السرية ومدى تحمل الوسيط للتغييرات[27] [1] .

2- هدف البحث:

يهدف هذا البحث إلى تقديم معالجة منهجية لمفاهيم إخفاء البيانات داخل الصور الرقمية، من خلال تحليل ومقارنة بين أشهر الخوارزميات في هذا المجال مثلLSB ، DWT، DCT، وخوارزميات أكثر تطوراً تعتمد على الذكاء الاصطناعي والتعلم العميق. كما يقترح البحث خوارزمية هجينة

جديدة، تدمج بين ضغط البيانات، وتقنيات التصحيح والتشفير، وخطوات متعددة للإخفاء، بهدف تحقيق توازن بين سعة الإخفاء، الشفافية البصرية، ومستوى الأمان ضد محاولات الاكتشاف والتحليل.

3- التورية الرقمية(Digital Steganography) :

تُعرّف التورية الرقمية بأنها تقنية تُستخدم لإخفاء وجود المعلومات نفسها ضمن وسائط رقمية (مثل الصور، الصوت، الفيديو، النصوص)، بحيث لا يُثير الملف المعدّل أي شك لدى الأطراف غير المعنيين.

بعكس التشفير الذي يُظهر وجود بيانات مشفّرة ويهدف إلى إخفاء المعنى، فإن التورية تُخفي وجود البيانات بالكامل. هذا يجعلها مفيدة في بيئات تتطلب سرية قصوى دون لفت الانتباه، مثل الاتصالات السرية، وتأمين البيانات الحساسة، وحماية الملكية الفكرية .

- التورية في الصور الرقمية:

الصور تُعد أكثر الوسائط استخداماً في التورية الرقمية، **لعدة أسباب:**

- سهولة تداولها وتنوع تنسيقاتها.
- قدرتها على احتواء كميات كبيرة من البيانات دون أن تُظهر تشوهاً مرئياً.
- وجود قنوات لونية مثل RGB تسمح بتوزيع البيانات بشكل متوازن وغير ملحوظ[7].

4-الخوارزميات الكلاسيكية المستخدمة في التورية:

في هذا القسم، نقدم **تحليلاً نقدياً للخوارزميات الكلاسيكية المستخدمة في إخفاء البيانات الرقمية(Steganography)** ، مع التركيز على مزايا وعيوب كل خوارزمية، الفروق بينها، وعلاقتها بالخوارزمية المقترحة في هذا البحث.

1.4 خوارزمية البت الأقل أهمية (Least Significant Bit – LSB) :

تُعد LSB من أبسط وأكثر الخوارزميات شيوعاً، حيث تعتمد على استبدال البت الأخير في كل بايت من بيانات الصورة ببت من الرسالة السرية. في الصور الملونة، يمكن استخدام القنوات الثلاث (Red, Green, Blue) لزيادة السعة دون تشويه مرئي ملحوظ.

- **الميزات** :سهلة التنفيذ، سعة عالية لإخفاء البيانات.
- **العيوب** :قابلة للكشف باستخدام التحليل الإحصائي، ضعيفة ضد الهجمات.
- **التحليل النقدي** :مناسبة للتطبيقات التي تتطلب **سعة كبيرة وسهولة تنفيذ**، لكنها غير ملائمة للتطبيقات الحساسة للأمان[9] [11] .

2.4 التحويل المويجي المتقطع(Discrete Wavelet Transform – DWT) :

يقوم DWT بتحويل الصورة من المجال المكاني إلى المجال الترددي، مما يسمح بإخفاء البيانات في الترددات العالية التي يصعب ملاحظتها بصرياً.

- **الميزات** :مقاومة أعلى للهجمات، تأثير بصري منخفض.
- **العيوب** :يتطلب حسابات أكثر تعقيدًا مقارنة بخوارزميةLSB
- **التحليل النقدي** :أفضل من LSB للتطبيقات التي تتطلب **متانة ضد التعديلات أو الضغط البسيط**، لكنه أقل كفاءة من حيث سهولة التنفيذ[12] .

3.4 التحويل الجيبي(Discrete Cosine Transform – DCT) :

يُستخدم غالباً في صورJPEG ، حيث يتم تقسيم الصورة إلى كتل وتطبيق تحويل DCT عليها، ثم تُخفى البيانات في معاملات التردد الأقل أهمية.

- **الميزات** :مناسب للصور المضغوطة ويحافظ على الجودة البصرية.
- **العيوب** :سعة أقل مقارنة بـLSB ، ويتطلب معالجة إضافية للصور.
- **التحليل النقدي** :ملائم للتطبيقات التي تتطلب **توافقًا مع ضغطJPEG** ، لكنه أقل كفاءة من حيث السعة مقارنة بخوارزميات المجال المكاني.

4.4 الإخفاء العكسي(Reversible Data Hiding – RDH) :

تمكن هذه التقنية من استرجاع الصورة الأصلية بعد استخراج البيانات دون أي فقدان، وتستخدم في التطبيقات التي تتطلب حفظ كامل لمحتوى الغلاف الأصلي مثل الصور الطبية أو الوثائق القانونية.

- **الميزات** :فقدان صفر، مناسب للتطبيقات الحساسة.
- **العيوب** :سعة أقل مقارنة بالخوارزميات الأخرى، تعقيد أعلى في التنفيذ.

التحليل النقدي :الخيار الأمثل للتطبيقات التي تتطلب **سلامة البيانات المطلقة**، لكنه أقل كفاءة في السعة والسرعة[45] .

4.4 الإخفاء بالتعلم العميق (Deep Learning-based Steganography)

تعتمد على الشبكات العصبية لإخفاء واستخراج البيانات بدون تدخل يدوي.

- **الميزات** :مرونة عالية، قوة ضد الهجمات المتقدمة.
- **العيوب** :تحتاج موارد حسابية كبيرة وبيانات تدريب واسعة.
- **التحليل النقدي** :مناسبة للتطبيقات الحديثة التي تتطلب **أماناً عالياً ومرونة في التعامل مع أنواع متعددة من البيانات**، لكنها غير مناسبة للتطبيقات ذات الموارد المحدودة . [18] [19]

المقارنة العامة بين الخوارزميات:

الخوارزمية	أفضل استخدام	سهولة التنفيذ	الأمان	السعة
LSB	التطبيقات غير الحساسة للأمان	سهلة	منخفض	عالية
DWT	تطبيقات مقاومة للتعديلات	متوسط	جيد	متوسطة
DCT	الصور المضغوطة(JPEG)	متوسط	متوسط	منخفضة
RDH	التطبيقات الحساسة للبيانات	صعب	عالي	منخفضة
Deep Learning	التطبيقات الحديثة والمرنة	صعب جدًا	عالي	عالية

الخلاصة:

يعتمد اختيار الخوارزمية على **متطلبات التطبيق** :السعة، الأمان، سهولة التنفيذ، والموارد المتاحة. الخوارزمية المقترحة في هذا البحث **تستفيد من نقاط القوة في هذه الخوارزميات مع تحسين الأمان والسعة لتطبيقات محددة**، مما يعزز كفاءتها مقارنة بالطرق التقليدية.

4- الدراسات السابقة في مجال إخفاء البيانات الرقمية

شهد مجال إخفاء البيانات الرقمية تطوراً كبيراً خلال العقدين الأخيرين، حيث ركز الباحثون على **تعزيز كفاءة الإخفاء، زيادة السعة التخزينية، تحسين الأمان، والحفاظ على جودة الصورة**، مع الحد من فرص كشف البيانات المخفية. على الرغم من التقدم الملحوظ، تظهر الحاجة إلى **تحليل نقدي للفجوات البحثية وإبراز العلاقة بين الخوارزميات التقليدية والحل المقترح في هذا البحث**، وهو ما سنتناوله فيما يلي.

1. تحسينات خوارزمية البت الأقل أهمية(LSB Enhancements)

- **Ker (2005)** قدم خوارزمية LSB Matching لتجاوز القيود التقليدية، من خلال تعديل قيمة البيكسل بزيادة أو نقصان واحد بدل الاستبدال المباشر.

أدخل مفهوم Embedding Efficiency لموازنة السعة التشويشية واحتمالية الكشف.

تحليل نقدي :تقلل هذه الطريقة الأثر الإحصائي، لكنها ضعيفة أمام الهجمات الإحصائية المعقدة الحديثة.

الفجوات البحثية :الحاجة لتطوير مقاومة قوية للتحليل الإحصائي وتوسيع التطبيق للصور الملونة[9] [10] [11] .

- **Koppola (2009)** استخدم التعديل التكيفي على الصور الملونةRGB ، مع اختيار مواقع الإخفاء بناءً على الخصائص المحلية للصورة.

تحليل نقدي :حسّن السعة والشفافية، لكن التعقيد الحسابي مرتفع.

الفجوات البحثية :تعميم النتائج على أنواع مختلفة من الصور يحتاج مزيداً من الدراسة.

- **Singh & Agarwal (2010)** دمجوا LSB مع تحسينات أمنية مثل التشفير المسبق والاختيار العشوائي لمواقع الإخفاء.

تحليل نقدي :توفر توازناً بين السعة والأمان وجودة الصورة، إلا أن الاعتماد على مفتاح سري يزيد من التعقيد.

الفجوات البحثية :لم يتم دراسة فعالية الخوارزمية ضد هجمات التحليل الإحصائي المتقدمة أو معالجة الصور المتكررة.

2. دمج تقنيات التحويل والتشفير:

- **Ahmed Badrani (2013)** دمج DWT مع LSB لإخفاء البيانات في الترددات المنخفضة مع تشفير إضافي.

تحليل نقدي :تعزيز الأمان وجودة الصورة، لكن يزيد التعقيد الحسابي.

الفجوات البحثية :غياب المقارنات الكمية مع أساليب حديثة مثل التعلم العميق، وعدم تحليل الفجوات البحثية بشكل كامل.

- **Wisam Munir (2017)** تعديل عشوائي للبيكسلات بدعم مفتاح سري.

تحليل نقدي :أمان محسّن، لكنه محدود على مجموعات صغيرة من الصور.

الفجوات البحثية :عدم اختبار الأداء على أحجام وصور متنوعة، نقص التحليل الكمي.

- **Swati Bhargava & Manish Mukhija (2019)** دمج LSB و DWTوRSA
تحليل نقدي :أمان عالي، لكن مكلفة حسابيًا، وتأثير الأداء لم يتم تقييمه بشكل شامل.
الفجوات البحثية :الحاجة لتقييم الأداء الكمي على مجموعات بيانات أكبر[14] .

3. تقنيات التشفير المتقدمة معLSB

- **Sana Haimour (2021)**

دمج تشفير التدفق الفوضوي (Chaotic Stream Cipher) معLSB [15]

- **AES (2020)** تشفير البيانات مسبقًا باستخدام معيار AES مع توزيع غير منتظم داخل الصورة.

تحليل نقدي :تعزيز أمان المعلومات، لكن يزيد التعقيد الحسابي.

الفجوات البحثية :لم يتم دراسة التوازن بين السعة والأمان بشكل كمي، ولا مقارنة الأداء مع طرق حديثة(2022–2025)

4. التقنيات الحديثة والمتقدمة:

- **تقسيم الملفات على عدة صور :(2020)** زيادة أمان الإخفاء عبر توزيع البيانات على صور متعددة.

- **Wang et al. (2021)** نموذج Hybrid Deep Autoencoder مع LSB لزيادة السعة وجودة الصورة(PSNR ~48 dB) [18]

- **Liu (2022)** دمج LSB مع ChaCha20 لتحقيق مقاومة عالية لهجمات التحليل واسترجاع بيانات دقيق.

- **Al-Faydi (2023)** مطابقة ذكية بين البيكسلات دون تعديل فعلي، مما أتاح جودة صورة مثالية وعدم إمكانية الكشف إحصائياً.
- **Mustafa M. Abd Zaid (2024)** LSB مزدوجة الطبقات مع RC4 لتحقيق توازن بين الجودة والأمان[21] .
- **Raiyan & Kabir (2025)** إطار SCReedSolo يجمع بينLSB ، تشفيرFernet ، وتصحيح الأخطاءReed–Solomon ECC [22]

تحليل نقدي :توفر هذه الطرق أماناً عالياً، مقاومة للتحليل الإحصائي، وتحسن جودة الصورة، لكنها مكلفة حسابياً وتحتاج مجموعات بيانات كبيرة للتدريب والتحليل.

الفجوات البحثية :تقييم الأداء في سيناريوهات متعددة، دراسة مقاومة الهجمات المتقدمة، وتحليل كمي مقارنة بأساليب تقليدية وحديثة

جدول المقارنة النقدية للخوارزميات السابقة:

الخوارزمية	الوصف	الفوائد	نقاط الضعف	الفجوات البحثية / الملاحظات البحثية
LSB Enhancement	تحسين البتات الأقل أهمية لتضمين البيانات	بسيطة وسهلة التنفيذ، قدرة عالية على الإخفاء، تأثير منخفض على جودة الصورة	عرضة لهجمات إحصائية بسيطة، متانة منخفضة ضد	ضعف المقاومة ضد التحليل الإحصائي، الحاجة لتطبيقات عامة على صور ملونة

	معالجة الصور			
الحاجة لمقارنة كمية مع طرق حديثة، مقاومة الهجمات	أكثر تعقيداً في التنفيذ، قدرة معالجة أقل	متانة أعلى ضد الضغط، أمان محسّن	تعديل معاملات DCTفي صور JPEG	DCT-Based Hiding
تقييم الأداء على مجموعات بيانات متنوعة، مقاومة الهجمات العملية	مكثف حسابياً، يحتاج بيانات تدريب كبيرة	أمان مشدد، متكيف مع بيانات معقدة	الشبكات العصبية لتعلم أنماط الإخفاء	Deep Learning-Based Hiding
تقييم شامل لمقاومة التحليلات الإحصائية، تحسين الأداء في الصور الكبيرة	أكثر تعقيدًا منLSB ، قدرة أقل مقارنة ببعض الطرق	توازن جيد بين القدرة والمتانة، مقاومة لهجمات معالجة الصور	إخفاء البيانات في معاملات المويجات	Wavelet Transform-Based Hiding
دراسة مقاومة الهجمات الحديثة، تقييم الأداء الكمي مع طرق حديثة	قدرة محدودة، تنفيذ معقد	إعادة بناء مثالية، أمان ومتانة عالية	استرجاع الصورة الأصلية بعد استخراج البيانات	Reversible Data Hiding

الخلاصة النقدية:

تحليل الدراسات السابقة يوضح أن **كل مجموعة خوارزميات لها مزاياها وعيوبه** .معظم الأعمال ركزت على تحسين السعة والأمان، لكن **الفجوات البحثية المهمة لا تزال قائمة:**

1. مقاومة الهجمات الإحصائية والتحليلات المتقدمة.
2. التقييم الكمي الشامل لمقارنة الخوارزميات الحديثة.(2022–2025)
3. اختبار الأداء على مجموعات بيانات متنوعة وأحجام صور مختلفة.
4. تحليل العلاقة بين الخوارزميات التقليدية والحديثة والخوارزمية المقترحة في هذا البحث.

يهدف هذا البحث إلى **سد هذه الفجوات** عبر تقديم خوارزمية تجمع بين مزايا LSB و DWT والتشفير الحديث، مع تبسيط التعقيد الحسابي، لتحقيق **توازن مثالي بين السعة والأمان وجودة الصورة**، بما يعزز القيمة العلمية مقارنة بالأعمال المنشورة سابقاً.

5- الخوارزمية المقترحة:

1- الهدف من الخوارزمية المقترحة :

تهدف الخوارزمية المقترحة إلى تطوير نهج هجين لإخفاء البيانات داخل الصور الرقمية من خلال دمج تقنيات التحويل الموجي المتقطع (DWT) مع التشفير. يُعتمد في هذه الطريقة على تشفير البيانات أولاً، مما يرفع من مستوى الأمان، ثم يتم تضمينها في المكونات عالية التردد مثلcH الناتجة عن تحويلDWT ، عبر تعديل البتات بما يتوافق مع البيانات الثنائية المشفرة. بعد الإخفاء، يُعاد تشكيل الصورة بواسطة التحويل العكسي(Inverse DWT) ، لتبدو كالصورة الأصلية ولكنها تحتوي على معلومات سرية مخفية.

عند الحاجة إلى استخراج البيانات، يتم تطبيق DWT مجدداً لاستخراج البتات من القنوات المناسبة، ثم يتم فك التشفير وفك شفرة هامينغ لاستعادة النص الأصلي.

يرتكز هذا النهج الهجين على **ثلاثة أهداف رئيسية:**

1. **تعزيز الأمان** :من خلال التشفير المسبق للبيانات لضمان وصولها فقط للمستخدمين المصرح لهم.
2. **زيادة كفاءة التضمين** :عبر ضغط البيانات لتقليل تأثيرها على جودة الصورة.
3. **رفع مستوى الإخفاء** :باستخدام تقنيات تجعل من الصعب اكتشاف أو استخراج البيانات بدون المعرفة اللازمة.

2- الخوارزميات المستخدمة :

يعتمد النموذج المقترح لإخفاء البيانات على مجموعة من الخوارزميات المتكاملة التي تضمن الأمان، والكفاءة، والدقة، وتشمل ما يلي:

خوارزمية هامينغ (Hamming Code) :

تُستخدم هذه الخوارزمية للكشف عن الأخطاء وتصحيحها عند نقل أو تخزين البيانات، عبر إدراج بتات إضافية (Parity Bits) تحدد موقع الخطأ وتصححه تلقائياً وتم اعتمادها نظراً لقدرتها على تحسين موثوقية النظام باستخدام عدد محدود من البتات الإضافية مقارنةً بغيرها من خوارزميات تصحيح الأخطاء.

خوارزمية التشفير المتماثل:

يُستخدم هذا النوع من التشفير لحماية البيانات المخفاة من خلال تشفيرها وفك تشفيرها باستخدام نفس المفتاح، ما يعزز سرية المحتوى ويمنع قراءته في حال اكتشافه.

التحويل المويجي المتقطع (DWT) :

تقنية تحليل زمني–ترددي تسمح بتقسيم الصورة إلى مكونات منخفضة وعالية التردد باستخدام مرشحات low–pass و high–pass، مما يتيح تضمين البيانات في المناطق ذات التأثير البصري الأقل، مع الحفاظ على جودة الصورة.

التحويل المويجي العكسي (IDWT) :

هو العملية المعاكسة لـDWT ، تُستخدم لإعادة بناء الصورة الأصلية بعد تضمين البيانات المخفية، مع المحافظة على مظهرها العام دون تغيير ملحوظ.

الخوارزمية الهجينة:

تجمع هذه الخوارزمية بين تقنيات متعددةDWT، تقنية أقل البتات أهمية(LSB) ، ضغط البيانات (Zlib)، التشفير باستخدام مكتبةFernet ، وخوارزمية هامينغ. ويهدف هذا الدمج إلى تحقيق:

- أمان مرتفع من خلال التشفير.
- تقليل حجم البيانات وتحسين السعة باستخدام الضغط.
- تصحيح الأخطاء للحفاظ على موثوقية البيانات.
- جودة بصرية عالية من خلال استخدام DWT وLSB

3- خطوات عمل الخوارزمية المقترحة

تتبنى الخوارزمية المقترحة نهجاً هجينياً يجمع بين **التشفير**، **ضغط البيانات**، **وتحويل المويجات (Wavelet Transform)**مع **طريقة البت الأقل أهمية (Least Significant Bit – LSB)** لإخفاء الرسائل داخل الصور الرقمية، بما يضمن **أماناً عالياً**، **سعة كبيرة**، **وجودة صورة مرتفع** الخطوات موضحة أدناه بأسلوب أكاديمي نقدي:

الخطوة 1: توليد أو تحميل مفتاح التشفير (Encryption Key Generation/Loading)

- يُعد مفتاح التشفير الركيزة الأساسية لحماية الرسائل.
- يتم التحقق أولاً من وجود ملف المفتاح(encryption.key)
  - **إذا وُجد** ⟵تحميل المفتاح المستخدم لتشفير وفك تشفير الرسائل.
  - **إذا لم يُوجد** ⟵توليد مفتاح جديد باستخدام مكتبة **Fernet** من مكتبة **cryptography**، ثم حفظه للاستخدام المستقبلي.

- هذه الخطوة تضمن **ثبات المفتاح وأمان العملية، مع الحد من الوصول غير المصرح به.**

الخطوة 2: تحضير الرسالة للتضمين(Message Preprocessing)

- تُشفّر الرسالة النصية بالمفتاح المحمّل أو المولد لتصبح غير قابلة للقراءة بدون المفتاح الصحيح.
- بعد التشفير، تُضغط الرسالة باستخدام مكتبة **zlib** لتقليل حجمها، ما يعزز **كفاءة التضمين ويحافظ على جودة الصورة.**
- هذه الإجراءات تعكس **التوازن بين الأمان وسعة الإخفاء.**

الخطوة 3: تضمين الرسائل داخل الصورة(Data Embedding)

تتم العملية باستخدام **نهج هجينيDWT–LSB**

1. تحويل الصورة إلى **تدرج رمادي (Grayscale)** لتسهيل المعالجة الرقمية.
2. تحويل الصورة إلى مصفوفة رقمية باستخدام **NumPy**
3. **دمج الرسالة المشفرة والمضغوطة في الترددات العالية** باستخدام مكتبة **PyWavelets**، حيث تكون التغيرات أقل وضوحاً بصرياً.
4. بالتوازي، استخدام **LSB** لاستبدال أقل بت في كل بكسل بقيم من الرسالة، مما يزيد من **سعة البيانات المخفية ويصعّب كشفها.**

الخطوة 4: حفظ الصورة المدمجة(Saving the Embedded Image)

- تحويل المصفوفة المعدلة إلى صورة باستخدام مكتبة **Pillow**
- حفظ الصورة في المسار المحدد، ما يضمن **سلامة البيانات المخفية وإمكانية استرجاعها بدقة لاحقاً.**

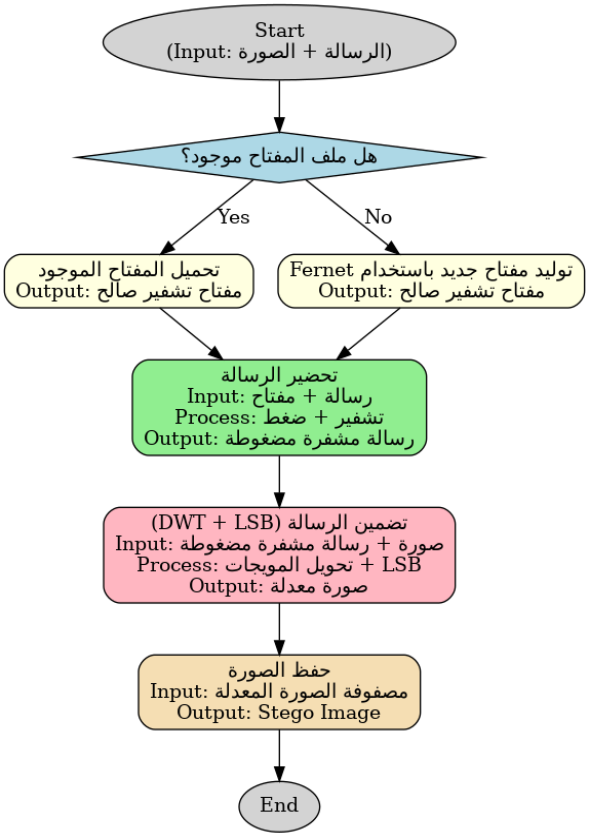
التحليل الأكاديمي للخطوات:

1. **التشفير والضغط** :توفر حماية قوية للرسائل مع تحسين السعة التخزينية.
2. **دمج DWT و LSB**: يحافظ على جودة الصورة ويصعّب اكتشاف البيانات المخفية.
3. **حفظ الصورة** :يضمن استرجاع الرسالة بدقة مع الحفاظ على سلامة الصورة الأصلية.

إنشاء جدول Input / Process / Output

المرحلة	المدخلات(Inputs)	العمليات(Process)	المخرجات (Outputs)
توليد/تحميل المفتاح	ملف مفتاح (إن وجد) أو نظام توليد جديد	تحميل أو توليد مفتاح باستخدامFernet	مفتاح تشفير صالح
تحضير الرسالة	الرسالة النصية + مفتاح	تشفير الرسالة + ضغطها باستخدامzlib	رسالة مشفرة مضغوطة
التضمين (DWT + LSB)	صورة + رسالة مشفرة مضغوطة	تحويل المويجات + تضمينLSB	مصفوفة صورة معدلة
حفظ الصورة	مصفوفة صورة معدلة	تحويل إلى صورة وحفظ باستخدامPillow	صورةStego

المخطط الانسيابي :



4- تحليل النتائج:

بعد إتمام عملية الإخفاء الرقمي للبيانات داخل الصور باستخدام تقنيات مختلفة، من الضروري إجراء تحليل دقيق للصور الناتجة لضمان أن عملية الإخفاء قد تمت بنجاح دون التأثير الكبير على جودة الصورة الأصلية. يهدف هذا التحليل إلى تقييم مدى تأثير عملية الإخفاء على الخصائص

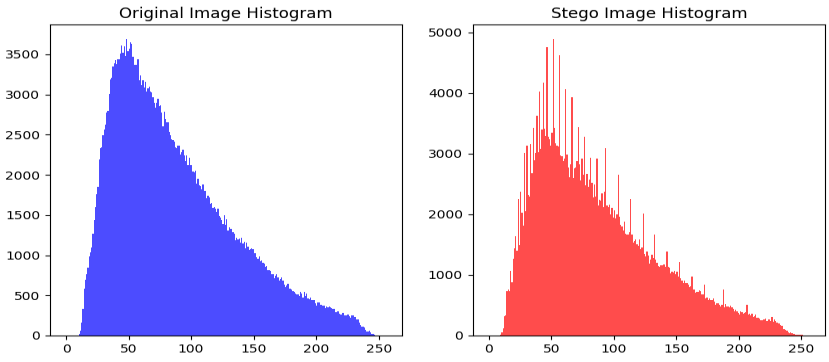
البصرية للصورة، مثل توزيع القيم اللونية أو الرمادية، والتغيرات في تفاصيل الصورة التي يمكن أن تكون مؤشراً على وجود بيانات مخفية.

في هذا السياق، يتضمن التحليل عدة مراحل، بما في ذلك مقارنة الصورة الأصلية بالصورة المخفية، وفحص توزيع القيم اللونية باستخدام الهستوجرام، بالإضافة إلى تحليل المعاملات المويجية التي توفر معلومات دقيقة حول التغيرات التي طرأت على ترددات الصورة المختلفة، يساهم هذا التحليل في التأكد من أن عملية الإخفاء لم تُحدث تغييرات ملحوظة يمكن كشفها بسهولة، مما يضمن بقاء البيانات المخفية آمنة وغير قابلة للكشف من قبل الأطراف غير المخولة.

الشكل (4-1) : Visual Comparison

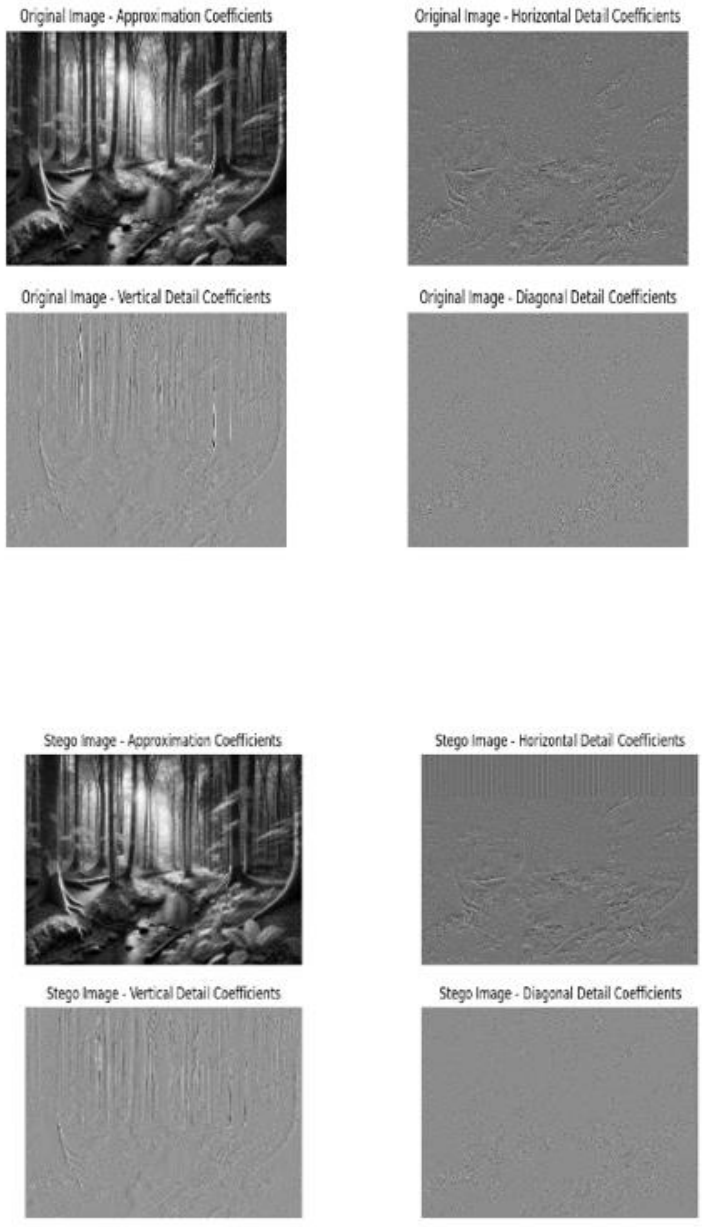
- ✓ في الشكل (4-1) تبدو الصورة الأصلية و الصورة المخفاة متطابقة بالنسبة للعين المجردة، إلا أن هذا يعتبر مؤشراً جيداً على أن عملية الإخفاء تمت بنجاح دون التأثير الواضح على جودة الصورة،

إذا كانت الفروق غير مرئية، فهذا يعني أن المعلومات المخفية قد أُدرجت بشكل غير ملحوظ، وهو هدف رئيسي في تقنيات الإخفاء الرقمي.



الشكل (4-2): Histogram Analysis

✓ يظهر الشكل (4-2) توزيعاً قياسياً للبيكسلات بالاعتماد على تدرجات اللون الرمادي، هذا التوزيع يعكس المحتوى الطبيعي للصورة دون أي تشويش أو تعديل، في الصورة التي تحتوي على البيانات المخفية يظهر بعض التغييرات في التوزيع مقارنة بالصورة الأصلية و تكون هذه التغييرات طفيفة أو ملحوظة بناءً على الطريقة التي تم بها إخفاء البيانات، إما التوزع في الصورة المخفية يظهر توزيعاً مشابهاً جداً للصورة الأصلية، ولكن مع وجود بعض التغييرات الطفيفة. هذه التغييرات تشير إلى أن عملية الإخفاء قد أثرت بشكل طفيف على توزيع القيم الرمادية، ولكن ليس بشكل كبير لدرجة أن يتم اكتشافها بسهولة، أي تغييرات كبيرة قد تشير إلى أن الإخفاء أثر على القيم الرمادية للصورة، مما قد يجعل الإخفاء أكثر قابلية للاكتشاف من خلال تحليل الهستوجرام. ومع ذلك، إذا كانت التغييرات طفيفة، فهذا يشير إلى أن الإخفاء كان فعالاً في الحفاظ على التوزيع الأصلي.



الشكل(4-3): Wavelet Coefficient Analysis

- ✓ **تحليل معامل المويجات:**

معاملات التقريب(Approximation Coefficients) :

تظهر الصورة المخفية معاملات تقريب مشابهة جداً للصورة الأصلية، هذا يشير إلى أن البنية الأساسية للصورة لم تتأثر بشكل كبير بعملية الإخفاء.

التفاصيل الأفقية(Horizontal Detail Coefficients) :

تظهر الصورة المخفية تفاصيل أفقية مشابهة لتلك الموجودة في الصورة الأصلية، أي اختلافات هنا كانت طفيفة، مما يعني أن الإخفاء لم يؤثر بشكل كبير على التفاصيل الأفقية.

التفاصيل العمودية (Vertical Detail Coefficients) :

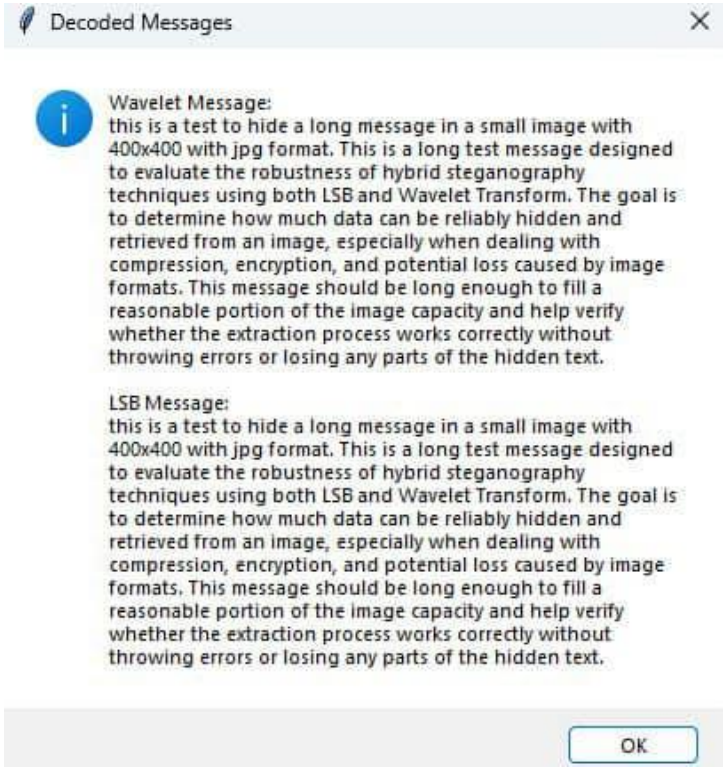
التفاصيل العمودية في الصورة المخفية مشابهة أيضاً للصورة الأصلية، وهذا يعني أن الحواف والتفاصيل العمودية لم تتأثر كثيراً بعملية الإخفاء.

التفاصيل القطرية (Diagonal Detail Coefficients):

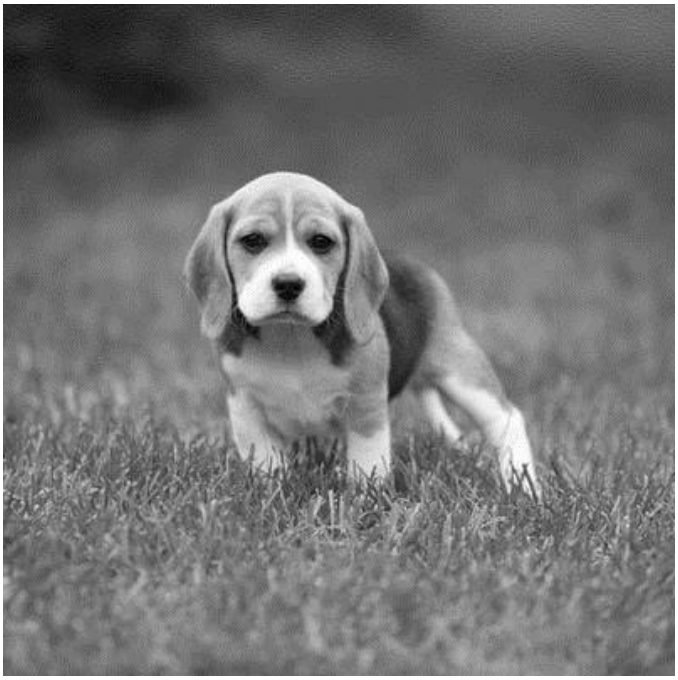
مثل المعاملات الأخرى، التفاصيل القطرية في الصورة المخفية مشابهة لتلك الموجودة في الصورة الأصلية، مما يشير إلى أن التأثير على هذه التفاصيل كان طفيفاً.

بعد الانتهاء من إعداد الخوارزمية الهدينة قمنا بتجريب نص كبير مع صورة صغيرة بصيغة JPEG بأبعاد 400*400 وكانت النتائج مرضية إلى حد كبير وموضحة في الأشكال التالية:

الشكل (4-4) :الصورة قبل التنفيذ



الشكل (4–5) النص الذي استخدمناه



الشكل (4-6) خرج الخوارزمية

ملاحظة : الصورة بالأبيض والأسود كون الخوارزمية هجينة مع خوارزمية DWT حيث خرج هذه الحوارزمية دوماً هو صور رمادية وهذه أحد نقاط القوة ضمن هذه الخورازمية حيث من الصعب تمييز البسكلات التي تحمل النصوص المورية.

تأثير خوارزمية الإخفاء الهجينة على الصور (LSB+DWT)

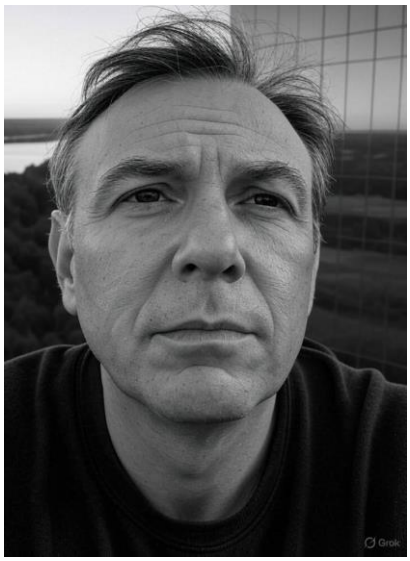
هذا المستند يوضح النتائج المتوقعة لتطبيق خوارزمية الإخفاء الهجينة التي تجمع بين (LSB,DWT) على أنواع مختلفة من الصور.

الفكرة الأساسية:

تعتمد على تغيير البت الأقل أهمية في البكسل لإخفاء البيانات ، وبالتالي LSB : تقنية التغيير غير ملحوظ بالعين المجردة.

تعتمد على تحويل المويجات،حيث يتم توزيع البيانات المخفية،DWT: تقنية معاملات الترددن وغالباً ماينتج عنها صورة رمادية أقل وضوحاً.

التقنية الهجينة: مزيج بين الطريقتين لتوفير قوة أعلى في الإخفاء مع الحفاظ على جودة الصورة.



الشرح التفصيلي للنتائج:

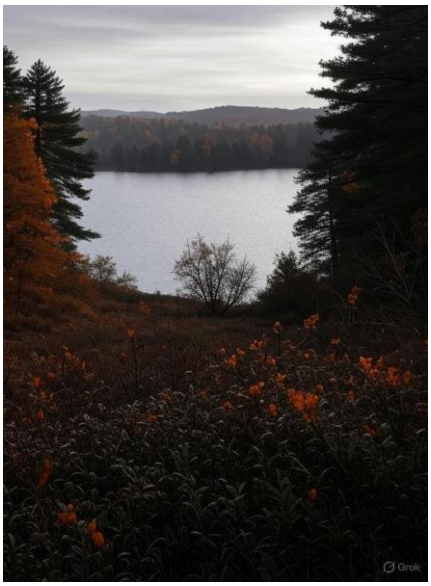
وجه الإنسان:

قبل التنفيذ : صورة ملونة طبيعية بملامح واضحة لايوجد فرق ملحوظ.

LSB بعد : لايوجد فرق ملحوظ.

DWT بعد : تتحول إلى صورة رمادية، ملامح الوجه أقل وضوح.

بعد التهجين : صورة رمادية أنعم مع فقدان بسيط في التفاصيل



الشرح التفصيلي للنتائج:

منظر طبيعي:

قبل التنفيذ : ألوان زاهية (سماء، أشجار، جبال)

LSB بعد: لاتغيير ملحوظ.

DWT بعد: تتحول إلى رمادي،السماء تبدو أنعم.

بعد التهجين: رمادي بتفاصيل أقل ونعومة أعلى.

الشرح التفصيلي للنتائج:

جسم – مبنى :

قبل التنفيذ : صورة ملونة بخطوط واضحة وحادة.

LSB بعد: مثل الأصل تقريباً.

DWT بعد: تتحول إلى رمادي، الحواف تبقى واضحة لكن التفاصيل أقل.

بعد التهجين: رمادي مع فقدان للتباين والحدة.

الخلاصة:

توفر توازناً جيداً بين إخفاء البيانات وحماية(LSB+DWT) الخوارزمية الهجينة جودتها البصرية والصور النهائية غالباص ماتكون رمادية وأقل حدة، لكن من الصعب على العين المجردة اكتشاف وجود بيانات مخفية

الخاتمة :

يشكّل إخفاء البيانات في الصور الرقمية أحد المسارات البحثية الحيوية في مجال أمن المعلومات، خاصةً في ظل التطور المتسارع لأساليب الهجوم وكشف البيانات. ومن خلال هذا البحث، تم استعراض وتحليل أبرز التقنيات الكلاسيكية والحديثة في التورية الرقمية، مع التركيز على خوارزمياتLSB ، DWT، DCT، والخوارزميات المستندة إلى الذكاء الاصطناعي، إضافةً إلى تقييمها وفق معايير الأداء والأمان وسعة الإخفاء.

انطلاقًا من التحديات العملية المرتبطة بفعالية الإخفاء وسريته، تم اقتراح خوارزمية هجينة تدمج بين ضغط البيانات، تصحيح الأخطاء باستخدام كود هامينغ، التشفير المتماثل، وتقنيتي LSB وDWT، وقد أظهرت هذه الخوارزمية نتائج واعدة على صعيد تحقيق توازن دقيق بين الشفافية البصرية، متانة الإخفاء، وسعة التخزين.

أظهرت النتائج التجريبية كفاءة النموذج المقترح من خلال تحليلات بصرية وإحصائية ومعاملات ترددية، حيث تمت عملية الإخفاء دون تأثير ملحوظ على جودة الصور، مع صعوبة الكشف عن البيانات المخفية بالطرق التقليدية. كما ساهم دمج خوارزميات التشفير وتصحيح الأخطاء في رفع مستوى الموثوقية والأمان.

وبناءً على هذه المعطيات، يمكن اعتبار هذا البحث خطوة أولية نحو تطوير نماذج أكثر ذكاءً وتطورًا في إخفاء البيانات، تواكب متطلبات السرية العالية وتعقيدات الهجمات الرقمية الحديثة. كما تفتح الخوارزمية المقترحة آفاقًا واسعة للبحث المستقبلي، خاصةً في اتجاه التورية القائمة على التعلم

العميق، والتحسين التلقائي لجودة الصور، وتكييف أساليب الإخفاء مع طبيعة البيانات والوسائط المستخدمة.

المراجع

[1] M. Warkentin, M.B. Schmidt, E. Bickering، Steganography and Steganalysis, Premier reference Source–Intellectual Property Protection for Multimedia Information technology, Chapter XIX, 2008

[2] N.N. El-Emam, hiding a large amount of data with high security using steganography algorithm, Journal of Computer Science 3 (2007) 223-232

[3] M. Chen, N. Memon, E.K. Wong, Data hiding in document images, in: H. Nemati (Ed.). Premier Reference Source–Information Security and Ethics: Concepts, Methodologies, Tools and Applications, New York: Information Science Reference, 2008, pp. 438-450.

[4] A. Ker, "Steganalysis of LSB matching in greyscale images," IEEE Signal Process Letter, vol. 12, no.6, pp. 441– 444, Jun. 2005.

[5] Koppola, R. R., (2009), "A High Capacity Data-Hiding Scheme in LSB-Based Image Steganography", M.Sc. Thesis Presented to Akron University.

[6] Singh, S. and Agarwal, G., (2010), "Use of Image to Secure Text Message with the Help of LSB Replacement", International Journal of Applied Engineering Research, Din Digul Vol. 1No.1.

أحمد حامد صالح البدراني في تشفير وإخفاء المعلومات في الصور الرقمية باستخدام التحويل المويجي[7]

وتقنية lsb في المؤتمر العلمي الخامس 2013 في كلية علوم الحاسوب والرياضيات مجلة الرافدين.

[8] Wesam Monir Saqer, Steganography within LSB and Second LSB with Randomness Depending on Indicators Using Secret Key,2017 The Islamic University – Gaza, Research and Postgraduate Affairs, Faculty of Information Technology

Master of Information Technology

[9] Hide Image and Text Using LSB, DWT, and RSA Based on Image Steganography– 2019 - Swati Bhargava, Manish Mukhija. (Modern Institute of Technology and Research Centre

[10] Enhancing Image Steganography Using Chaotic Stream Cipher for Secure Data Hiding – 2021. Sana Haimour,Mohammad Rasmi AL-Mousa,Rashiq R. Marie

[11] Data Hiding Using Specific Pixel Sequence with AES Encryption – 2020.

[12] A Novel Technique for Hiding a File in Multiple Images Using Segmented Map – 2020.

[13] Wang, J., Li, Y., & Zhao, M. Hybrid Deep Autoencoder for High Capacity Image Steganography. (2021).

[14] Liu, H., Zhang, Q., & Sun, Y. Secure Steganography Using LSB and ChaCha20 Pre-encryption Scheme. (2022).

[15] Al-Faydi, T. A. Improved LSB image steganography with high imperceptibility based on cover–stego matching. (2023).

[16] Zaid, M. M. A., Jawad, M. M., & Abass, H. S. LSB Steganography using Dual Layer for Text Crypto-Stego. - ISCKU 2024 – International Scientific Conference of Knowledge University. (2024).

[17] Raiyan, M. T., & Kabir, M. A. SCReedSolo: A Secure and Robust LSB Image Steganography Framework with Randomized Symmetric Encryption and Reed–Solomon Coding. (2025).

[18] "Cryptography and Network Security: Principles and Practice" by William Stallings 2022.

[19] "Steganography in Digital Media: Principles, Algorithms, and Applications" by Jessica Fridrich

[20] "Information Hiding: Steganography and Watermarking-Attacks and Countermeasures" by Neil F. Johnson, Zoran Duric, and Sushil Jajodia

[21] "A Survey of Steganography Techniques" by Souvik Bhattacharyya and Gautam Sanyal

[22] A discrete wavelet transforms based technique for image data hiding, Ahmed A. Abdelwahab; Lobna A. Hassaan 2023

[23] Reversible Data Hiding, Nirwan Ansari 2019