دراسة وتحسين أداء خوارزميات الإخفاء ضمن ملفات الفيديو

الباحث: م. حسن أحمد ميلاد + د. علي ذياب

قسم التحكم الآلي والحواسيب

كلية الهندسة الميكانيكية والكهربائية – جامعة البعث

ملخص البحث

في الآونة الأخيرة، ازدادت أهمية الاتصالات عبر الإنترنت بشكل سريع لذلك أصبح أمن البيانات قضية مهمّة، حيث يوجد العديد من المتطفلين الذين يرغبون في الوصول إلى البيانات الخاصة بالآخرين وسرقتها أو تعديلها. ونتيجة ذلك ظهر إخفاء المعلومات كوسيلة لإخفاء وجود بيانات سرية داخل غلاف آخر. يمكن أن يكون هذا الغلاف رسوماً متحركة أو صوتاً أو فيديو. يعد استخدام الفيديو كغطاء لإخفاء البيانات السريّة أكثر أماناً ضد هجمات القراصنة مقارنة بالوسائط المتعددة الأخرى نظراً لتعقيدها النسبي مقارنة بالأنواع الأخرى، وبسبب التعدد في الإطارات مقارنة بالصور الذي يتيح إخفاء كمية كبيرة من البيانات السرية، بالإضافة الى أن انتشار الفيديو عبر الإنترنت أمر شائع جداً. وبالتالي لن يكون هناك شك من المتسللين بوجود معلومات سرية مخبأة ضمن هذه الفيديوات.

في هذا البحث تم القيام بإخفاء صورة داخل مقطع فيديو حيث تمثل الصورة المخفاة الرسالة السرية المراد إرسالها. في البداية، يتم ضغط الصورة السرية باستخدام خوارزمية Deflate، ويتم تشفير معلومات العنوان ثم يتم إخفاء معلومات الرأس دائما في الإطار الأول ويتم إخفاء البيانات السرية في العدد المحدد من إطارات الفيديو بعد تطبيق خوارزمية مثالية للعثور على أفضل الإطارات للإخفاء. وبالتالي فإن الخوارزمية تقدم أمان إضافي يقلل من فرصة اكتشاف الرسالة المخفية. كما تقدم نسبة MSE (متوسط مربع الخطأ) وPSNR (نسبة الإشارة إلى الضجيج) أفضل مقارنة مع الأبحاث الأخرى.

الكلمات المفتاحية: إخفاء المعلومات بالفيديو، Deflate، LSB، المتانة، MSE، PSNR.

Study and enhancing the performance of hiding steganography algorithms inside video files

ABSTRACT

In recent times, the importance of the communication over the Internet has increased rapidly. Accordingly, data security becomes a vital issue, as there are many hackers empting to accessing private data of others and steal or modify them. Hence, hiding information appeared as a way to hide the existence of secret data within another cover. This cover could be an image, audio and video. Using the video as a cover to hide secret data is safe against hacker attacks compared to other multimedia due to its relative complexity compared to other types and due to the redundancy of data that allow it to be included in a large amount of secret data in addition to the fact that video streaming over the Internet is very common and therefore it is unlikely that be suspicious of hackers.

In this paper, an image is hidden within a video. First, the secret image is compressed using an algorithm Deflate, the header information is encrypted and then the header is hidden in the first frame , the secret data are hidden into selected number of video frames after finding an optimal algorithm to find the best frames for hiding. Therefore, there is an extra safety. thus, reduces the chance that the hidden message being detected. This offers the best ratio MSE (Mean Square Error) and PSNR (Peak Signal to Noise Ratio) Compared to other methods.

Keywords: Video Steganography, Deflate, LSB, Robustness, MSE, and PSNR.

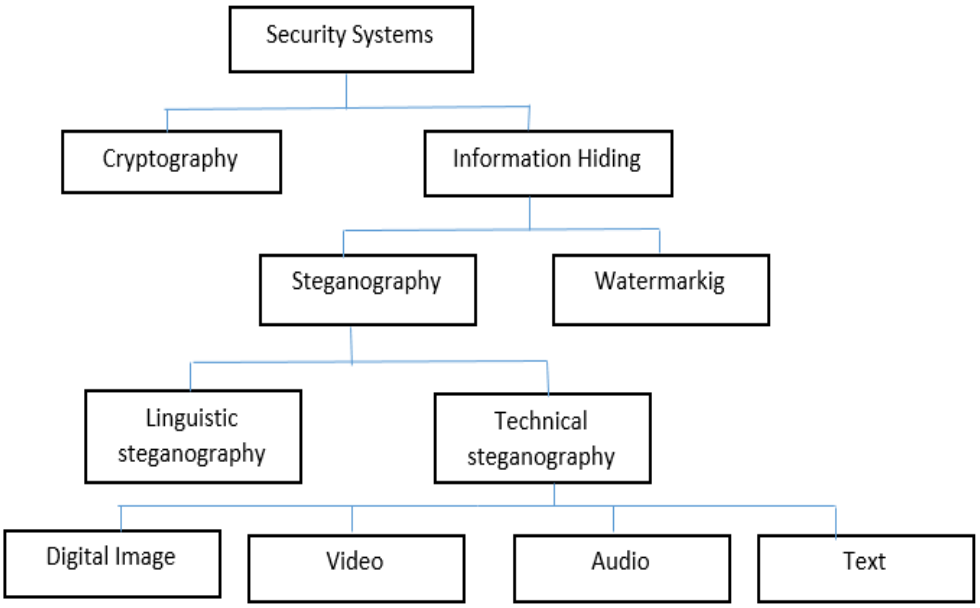
1. مقدمة

يشير مصطلح Steganography الى حماية المعلومات والبيانات المتداولة عبر شبكة الإنترنت من العبث والتخريب والتبديل، أو من أي خطر يهددها مثل وصول أي شخص غير مخول للوصول إليها والعبث ببياناتها والاطلاع عليها، وذلك من خلال توفير الوسائل والطرق اللازمة لحمايتها من المخاطر الداخليّة والخارجيّة، وموضوع أمن المعلومات هو موضوع قديم، ولكن زادت الحاجة والطلب عليه مع انتشار استخدام الإنترنت والاعتماد عليه في كافة مجالات الحياة، مما تطلب نقل البيانات والمعلومات عبر الشبكات المتعددة، كما أتاح انتشار شبكات التواصل الاجتماعي الحاجة الملحّة لذلك.

تهدف تقنية الإخفاء التي سيتم الحديث عنها إلى إخفاء المعلومات المهمة (المعلومات السرية) داخل بيانات أخرى (الفيديو الغلاف) بطريقة لا تؤثر على الغلاف، وبحيث لا تثير أي شبهة أو شك يؤديان إلى كشف الحقيقة، والغرض من عملية الإخفاء هذه ألا يعلم المهاجم بوجود هذه البيانات، تظهر البيانات المختلطة (الغلاف بعد إخفاء البيانات السرية داخله) والتي تسمى "Stego Objects" للنظام المرئي البشري Humman Visual System(HVS) كقطعة واحدة من البيانات لأن HVS لن يكون قادراً على اكتشاف أن هناك تغييراً بسيطاً في بيانات الغلاف. يمكن أن يكون هذا الغلاف أي نوع من ملفات الوسائط مثل النصوص والصوت والصورة والفيديو.

1.1- الإخفاء والتشفير

يجب أن نوضح في البداية الاختلاف الأساسي بين إخفاء المعلومات Information Hidingوالتشفير cryptography . يعرّف إخفاء المعلومات: هو فن إخفاء وجود البيانات عن طريق إخفاءها في غلاف آخر. أما التشفير (الترميز): هو عملية تحويل الرسالة الى شكل اخر لا يمكن فك تشفيرها دون وجود مفتاح سري. لتحسين أمن نظام المعلومات يمكن الجمع بين إخفاء المعلومات والتشفير. بشكل عام تتكون أنظمة الأمن من التشفير وإخفاء المعلومات كما هو موضّح الشكل (1):



الشكل (1) *تصنيف الإخفاء* في أنظمة أمن المعلومات

2.1- معايير الاخفاء

أي نظام إخفاء معلومات ناجح يجب أن يأخذ في الاعتبار ثلاثة معايير مهمة جداً وهي: السعة، عدم الإدراك، والمتانة.

•السعة (capacity)

تعبر عن كمية البيانات السرية التي يمكن إخفاؤها في الغلاف دون التأثير عليها.

• عدم الادراك(Imperceptibility)

للوصول إلى كفاءة دمج عالية نحتاج إلى معدل تعديل منخفض في الغلاف وجودة عالية لبيانات الغلاف عندها لن يكون هناك شك بوجود بيانات سرية وبالتالي فإن هذا يقلل من فرصة المهاجم في العثور على البيانات المخفية. يمكن ضبط ذلك عن طريق قياس قيم MSE و PSNR.

أي أن أي تشويه لبيانات الغلاف بعد عملية الإخفاء سيزيد من انتباه المهاجمين.

في علم الإخفاء التقليدي تكون العلاقة عكسية بين قدرة الإخفاء وخاصية عدم الإدراك. حيث أن زيادة سعة البيانات السرية تؤدي إلى تقليل جودة مقاطع الفيديو الغلاف.

وبالتالي ينبغي النظر في كلا العاملين بحيث نحقق أكبر سعة ممكنة بأقل تأثير على جودة الفيديو.

يتم اختيار هذه العوامل بالاعتماد على خوارزمية إخفاء المعلومات ومتطلبات المستخدم.

• المتانة (Robustness)

يعتبر نظام الاخفاء قوياً عندما يستطيع المتلقي استخراج البيانات السرية من الغلاف بشكل صحيح دون أي تشويه أو نقص في البيانات. لذلك يقيس هذا العامل قدرة الخوارزمية على مقاومة الهجمات ومعالجة الإشارات التي يمكن أن تكون إشارات ضوضاء أو مرشحات أو ضغط.

هذه الأهداف التي حرص الباحثين على تطبيقها تم تهديدها من قبل المهاجمين بواسطة عدد من الهجمات، وهي الهجمات الفعالة والهجمات غير الفعالة.

الهجمات غير الفعالة (Passive Attacks)

يكون هدف للمهاجم في هذا النوع من الهجمات جمع المعلومات فهو لا يقوم بتعديل المعلومات أو بالتسبب بأي أذى للنظام الحاسوبي.

تعتبر الهجمات المهددة للسرية هجمات غير فعالة وهي هجمات من الصعب جدا التقاطها حتى يكتشف المرسل أو المستقبل بتسرب معلومات سرية تخصه.

الهجمات الفعالة (Active Attacks)

يتسبب هذا النوع من الهجمات بتغيير المعلومات أو بأذى النظام الحاسوبي.

إن هذه التهديدات ينجم عنها مخاطر كبيرة جعلت قضية أمن المعلومات وتبادلها عبر الشبكة من القضايا التي تشغل اهتمام الباحثين نظرا للأهمية الفائقة والمتزايدة لتقنيات المعلومات في شتى المجالات في وقتنا الحاضر.

اذ لا بد من عملية السعي لمواجهة هذه التهديدات وذلك بإيجاد التقنيات المناسبة وتطويرها للحد من الأخطار المحتملة الناتجة عن هذه التهديدات بل والتخلص منها.

3.1- بعض الدراسات السابقة:

اسم الدراسة	ملخص الدراسة	النتائج
A New Method for Image Steganography Using LSB and MSB [13]	استخدام المجال المكاني للإخفاء بالاعتماد على MSB،LSB . يستخدم MSB فقط للمقارنة ويتم الاخفاء في LSB.	أعطت الطريقة المقترحة تغيرات أقل على الصورة الغطاء PSNR=42.01 MSE= 0.0071

Image Steganography using Two's Complement [5]	أخذ المتمم الثنائي لعناصر الصورة. تبديل مواقع البتات اختيار 4 عناصر الصورة من الصورة الغطاء. اخفاء كل زوج من البتات السرية في LSB 2.	استخدام المتمم الثنائي يزيد من المستوى الأمني للخوارزمية. PSNR=59.534 ويمكن إنقاص قيمته بتقليل حجم الرسالة السرية
Image steganography based on complement message and inverted bit LSB subsititution [6]	أخذ المتمم الثنائي للرسالة السرية. إخفاء الرسالة المتممة في عناصر الصورة الغطاء حيث يتم اختيار العناصر الصورة عن طريق مولد أرقام عشوائية.	استخدام صور رمادية للإخفاء 512*512حيث أعطت الخوارزمية psnr=59.65 وتزداد هذه النسبة الى 59.72 عند تطبيق الخوارزمية بواسطة المتمم
new technique of steganography based on location of LSB [2]	الاخفاء في صورتين أو تقسيم الصورة الغلاف الى قسمين. مقارنة كل bit 2 من الرسالة السرية في 2lsb. من عناصر الصورة الأولى اخفاء أماكن التطابق في. القسم الثاني بدءا من الدليل k.	استخدام الصور ملونة للإخفاء يزيد من سعة الاخفاء. مناسب لصور معينة لأنه يعتمد على المطابقة
High PSNR Based Image Steganography [15]	استخدام الصور الملونة كغطاء. تضمين البتات ذات الدليل الفردي بالمصفوفة R ب	استخدام الصور الملونة يزيد من امكانية الاخفاء اعطت الخوارزمية PSNR =40.51

	استخدامLSB. تضمين البتات ذات الدليل الزوجي يالمصفوفة G باستخدام LSB.	
The Improved Image Steganography with Encryption Method and to Overcome the Compression Technique [16]	ضغط البيانات باستخدام خوارزمية shift. تطبيق خوارزمية RSA على البيانات قبل عملية التضمين. تطبيق تابع بعثرة على الصورة الغطاء لتحديد أماكن الاخفاء.	استخدام خوارزمية التشفير يزيد من أمن المعلومات كما أن استخدام خوارزمية ضغط يزيد من سعة الاخفاء
hash based least significat bit technique for video[17]	استخدام ملفات AVI كحامل للملفات وتحديد الإطارات المستهدفة من خلال مولد ارقام عشوائية ثم إخفاء البيانات السرية (الصور) أبعاد الصورة السرية 480*640. .	بينت النتائج أن جودة نظام الاخفاء تنخفض بزيادة المعلمات السرية. أعطت النتائج قيم PSNR=48.56 MSE= 0.42.

2. هدف البحث

1. تطوير خوارزمية إخفاء معلومات تتيح إخفاء أكبر كمية من المعلومات ضمن ملفات الفيديو.
2. تحسين مستوى أمن وحماية المعلومات المرسلة عبر شبكات الانترنت.

3. تطوير خوارزمية اختيار الاطارات الأنسب للإخفاء بحيث تعطي أقل تغيير في الملف الحامل.

3. مواد وطرق البحث

تم تطبيق الطريقة المقترحة بواسطة برنامج Matlab 2015.

يتم عرض الطريقة المقترحة على مرحلتين:

المرحلة الأولى: هي دمج الصورة السرية بعد ضغطها في الفيديو(الإخفاء)

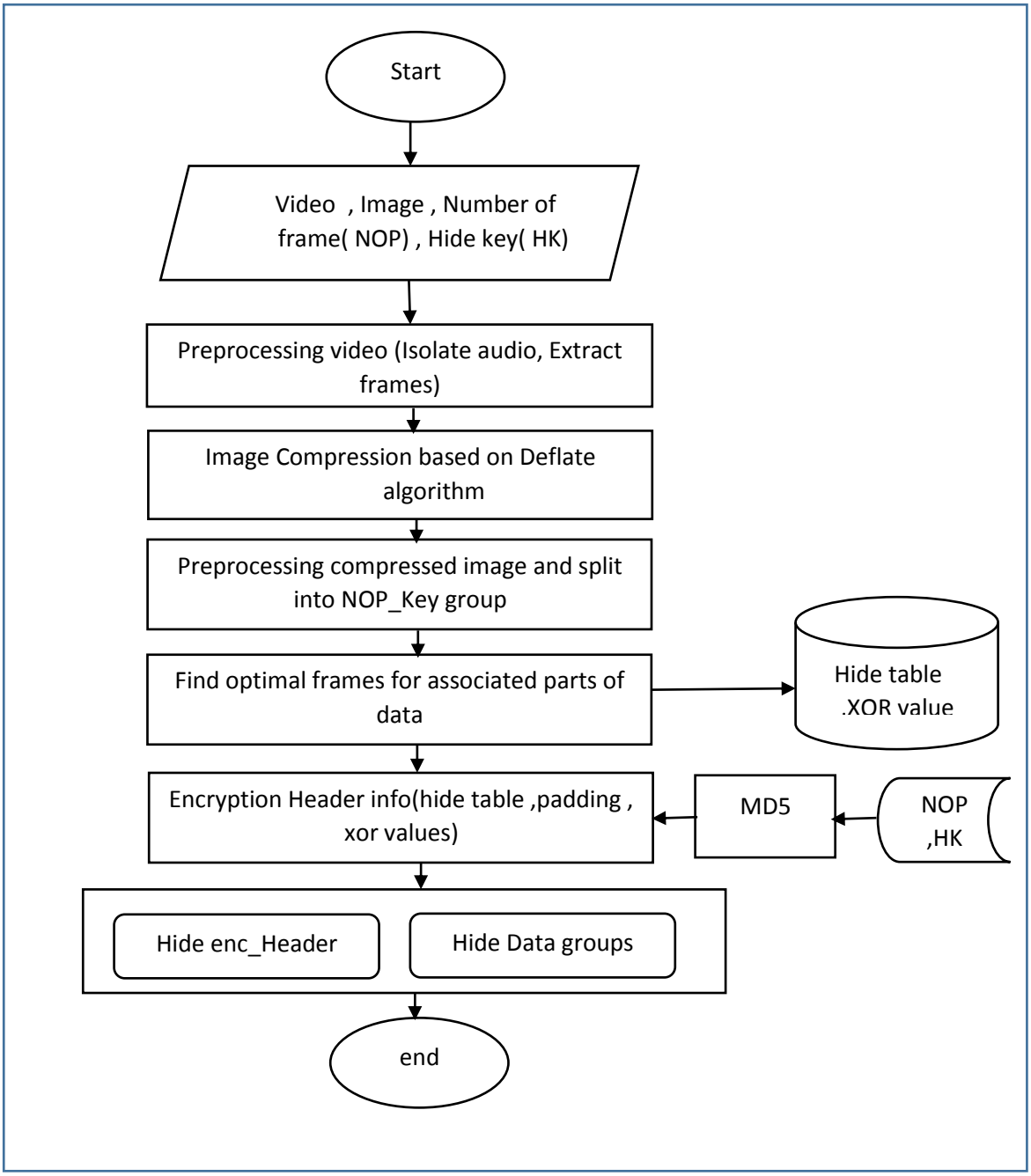
المرحلة الثانية: هي استخراج الصورة السرية من الفيديو

للتأكد من أن العملية تسير بشكل صحيح يتم حساب قيم MSE، PSNR.

1. مرحلة الإخفاء:

سيتم إخفاء صورة RGB (صورة سرية) في مقطع الفيديو، ويبدأ الاخفاء اعتبارا من Hidden Key وهو الموضع (رقم العنصر الصورة) الذي يختاره المرسل في بداية البرنامج.

الشكل 2 يصور مخطط التدفق لمرحلة الإخفاء المقترحة:



الشكل (2) خوارزمية الإخفاء المقترحة

1) المدخلات:

ندخل الصورة المراد إخفاؤها والفيديو الغلاف وقيم المفاتيح:

•HK المفتاح الذي يحدد مكان بدء إخفاء البيانات في الإطار.

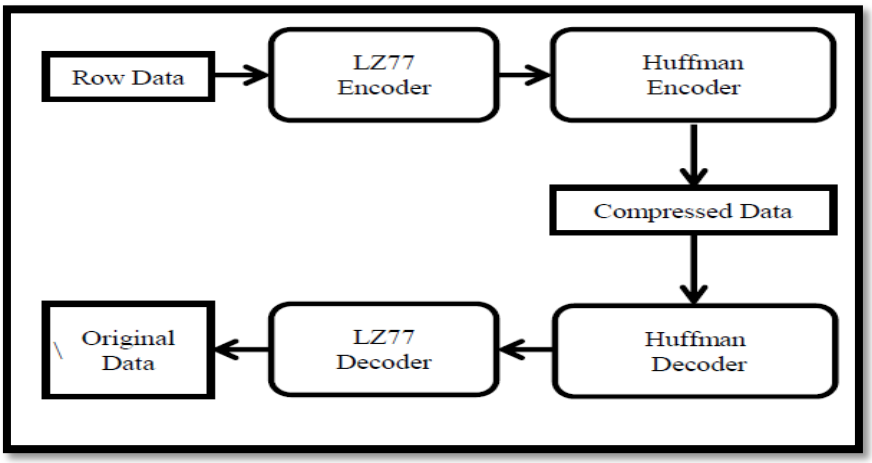
• NOP المفتاح الذي يحدد عدد الإطارات التي سيتم استخدامها للإخفاء.

2) المعالجة المسبقة للفيديو:

في هذه المرحلة سيتم عزل الصوت واستخراج إطارات الفيديو.

3) ضغط الصورة:

سيتم ضغط الصورة السرية بواسطة خوارزمية Deflate الخوارزمية موضحة في الشكل (3):



الشكل (3) خوارزمية Deflate

Deflate عبارة عن خوارزمية لضغط البيانات بدون فقدان على مرحلتين تستخدم مزيجًا من ترميز LZ77 و Huffman. وبالتالي سوف يستفيد من كلا الخوارزميتين.

إنها طريقة ضغط شائعة تم استخدامها في الأصل في برامج Zip و Gzip المعروفة ومنذ ذلك الحين تم تبنيها بواسطة العديد من التطبيقات.

4) المعالجة المسبقة للصورة المضغوطة:

بعد اكتمال الضغط، تتم معالجة الناتج (الصورة المضغوطة) وتحويله إلى نتائج بحيث يصبح قابلاً للقسمة على عدد الإطارات التي تم إدخالها (اضافة هامش للبيانات السرية).

5) البحث عن الإطارات المثلى للإخفاء:

المقصود بالإطارات المثلى هي التي تحقق أقل تغير عند استخدامها لإخفاء مجموعات البيانات، لتوضيح عملية اختيار الاطارات الأنسب للإخفاء نفرض لدينا المدخلات الآتية:

-طول البيانات = 1000.

-عدد الأجزاء / الإطارات التي نريد الإخفاء ضمنها=5

-مفتاح الاخفاء (HK) = 20

يتم توزيع البيانات السرية على عدد الإطارات المراد استخدامها.

في البداية يتم حساب مجموع LSB في كل إطار من الفيديو بدءاً من مفتاح الإخفاء وترتيب هذه القيم تنازلياً ويتم حفظ أدلة الإطارات بعد الترتيب، ثم حساب $p(f_1)$ احتمال ظهور البت [1] في LSB من كل إطار. بنفس الآلية ينم حساب عدد الواحدات في كل مجموعة بيانات وترتيب هذه القيم تنازلياً ويتم حفظ أدلة المجموعات بعد الترتيب، ثم حساب $p(g_1)$ احتمال ظهور البت[1] في كل مجموعة بيانات.بعد انجاز هذا الترتيب يتم إيجاد تقابل بين مجموعات البيانات والاطارات المرتبة تنازلياً وفق احتمال ظهور البت 1.فمثلاً سيتم إخفاء مجموعة البيانات ذات الدليل 4 في الإطار ذو الدليل 8 وهكذا كما هو موضح في الجدول 1.

بعد تحديد الإطارات الأنسب للإخفاء ولتحسين عملية الإخفاء يتم انجاز مرحلة إضافية حيث يتم مقارنة $p(g_1)$ و $p(f_1)$ وفي حال وجود اختلاف كبير بين الاحتمالين، سيتم انجاز عملية NOT لمجموعة البيانات وبالتالي تصبح التغيرات الناتجة عن عملية الإخفاء أقل ما يمكن.

كما هو موضح في الجدول 2 فعند انجاز عملية NOT لمجموعة البيانات ذات الدليل 5 سيصبح $p(g_1)$ =0,55 بدلاً من 0.45 أي أصبح التقارب أكبر مع $p(f_1)$ وبالتالي عملية الإخفاء سينتج عنها تعديل على الإطار أقل من سابقها.

Frame number.	Sum LSB in frames from 2 to last starting from HK (SUM_1F).	Sorted SUM_1F	Index of sorted frames. (Index_F)	Portability of ones in each frame. P(G1)	Sum LSB In each group (SUM_1G).	Sorted SUM_1G.	Index of sorted Groups (Index_G)	Portability of ones in each frame. P(F1)
2	10	195	8	0.975	80	200	4	1
3	160	190	7	0.95	20	170	6	0.85
4	30	160	3	0.8	140	140	3	0.7
5	90	150	6	0.75	200	90	5	0.45
6	150	90	5	0.45	99	80	1	0.4
7	190	30	4	0.15	170	20	2	0.1
8	195	10	2	0.05	3	3	7	0.015

الجدول (1)

Hide_table				Xorvalue	
Index_F	**a=P(F_1)**	**Index_G**	**b=P(G_1)**	**a>.5&b<.5 or <.5&b>.5**	
8	**0.975**	**4**	**1**	**0**	
7	**0.95**	**6**	**0.85**	**0**	
3	**0.8**	**3**	**0.7**	**0**	
6	**0.75**	**5**	**0.45**	**1**	**Reduce difference.**
5	**0.45**	**1**	**0.4**	**0**	

الجدول (2)

7) تشفير معلومات رأس:

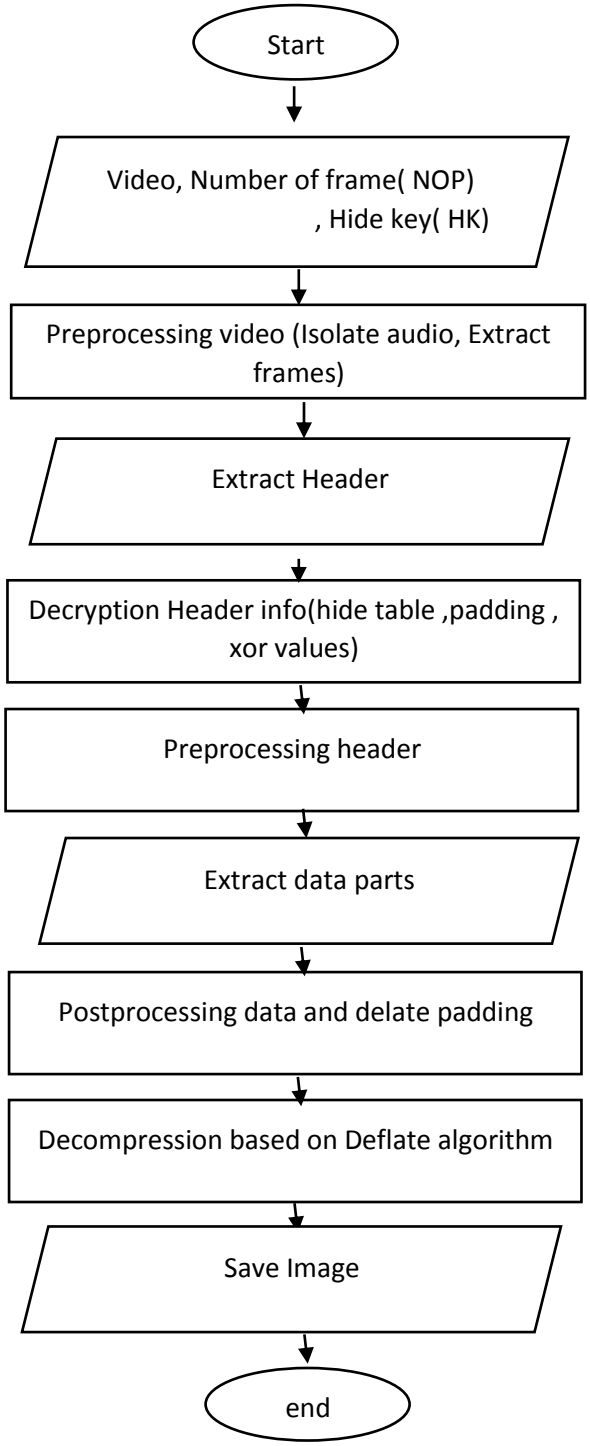
يتم تشفير البيانات اعتمادًا على المفتاح الذي تم إنشاؤه بواسطة خوارزمية md5، والتي تعطي مفتاح تشفير مختلفًا مع أدنى تغيير في الإدخال ممثلة بقيم المفتاحين المحليين. وبالتالي، فإن أي تغيير طفيف في الدخل يعادل تغيير كبير جدًا في الخرج لذلك لن يتمكن المهاجم من اختراق النظام إذا قام بإدخال مفتاح مخفي قريب من المفتاح الأصلي.

8) إخفاء البيانات السرية:

إخفاء الترويسة المشفرة ومجموعات البيانات السرية باستخدام LSB.

ب. مرحلة الاستخراج

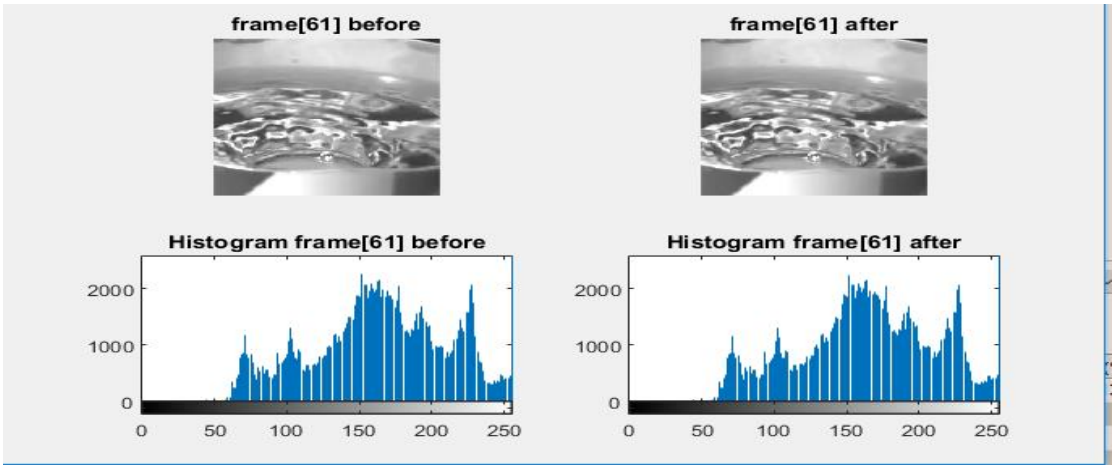
مرحلة الاستخراج هي عكس مرحلة الإخفاء كما هو موضح في الشكل 4.



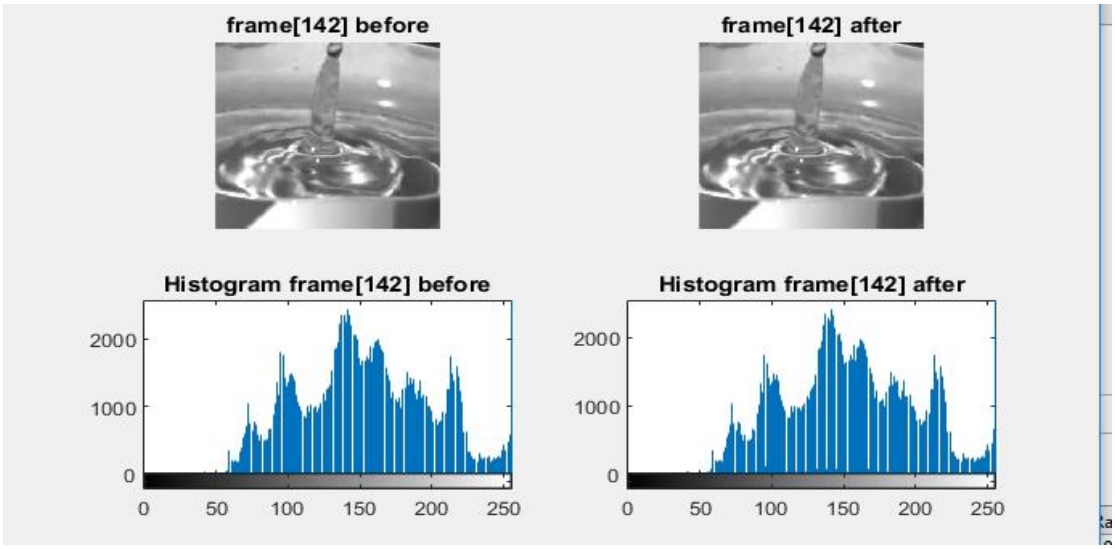
الشكل (4) خوارزمية الاستخراج المقترحة

4. النتائج ومناقشتها:

تم إجراء بعض التجارب لإثبات كفاءة الطريقة المقترحة حيث تتم المحاكاة على Matlab 2015 تم إخفاء صور سرية بحجوم مختلفة ضمن ملفات فيديو تختلف عن بعضها بعدد الإطارات وتم توزيع البيانات السرية على كامل إطارات الفيديو ومن ثم تقييم أداء الخوارزمية من خلال الملاحظة البصرية لعينة عشوائية من الإطارات مأخوذة بعد إخفاء الصورة السرية ضمن الفيديو الغلاف وتقييم الأداء من خلال حساب قيم MSE,PSNR في مختلف الحالات ، من خلال الدراسة التجريبية لاحظنا أن الاختلافات المرئية بين إطارات الغلاف الأصلية وإطارات Stego بالكاد يتم اكتشافها بالعين المجردة بالإضافة إلى ذلك من خلال ملاحظة الرسوم البيانية لإطارات الغلاف الأصلية وإطارات Stego لا يوجد فرق مرئي بينهما كما هو موضح في الشكل 5 والشكل 6.



الشكل 5 مخطط Histograme للإطار 61 قبل الإخفاء وبعده



الشكل 6 مخطط Histograme للإطار 142 قبل الإخفاء وبعده

يعد MSE (متوسط مربع الخطأ) وPSNR (معدل نسبة الاشارة الى الضجيج) قياسين شائعين للجودة لاكتشاف الاختلاف بين فيديو الغلاف والفيديو الناتج عن الإخفاء.

MSE هو متوسط الفرق التربيعي لكل عنصر الصورة بين فيديو الغلاف والفيديو الناتج

$$MSE = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n}\sum_{k=1}^{h}[C(i,j,k)-S(i,j,k)]^2}{m \times n \times h}$$

حيث M و N هما الصفوف والأعمدة في إطار الفيديو على التوالي،(C (i j، s(I,j) قيمة العنصر الصورة في الموضع (i، j) في فيديو الغلاف والفيديو الناتج على التوالي.

يتم التعبير عن PSNR بوحدة ديسيبل ويمكن حسابها باستخدام MSE على النحو التالي:

$$\text{PSNR} = 10*Log_{10}\left(\frac{MAX_C{}^2}{MSE}\right)\ (dB)$$

كلما كانت قيمة PSNR مرتفعة كلما كان التشوه أقل.

تم تطبيق الخوارزمية على مجموعة من الفيديوهات المرجعية المستخدمة في الإخفاء ونعرض في الجدول 3 خصائصها:

Video file	Frame Dimensions	Number of frames(max)
drop.avi	256*240	153
flame.avi	256*240	80
xylophone.avi	320*240	141

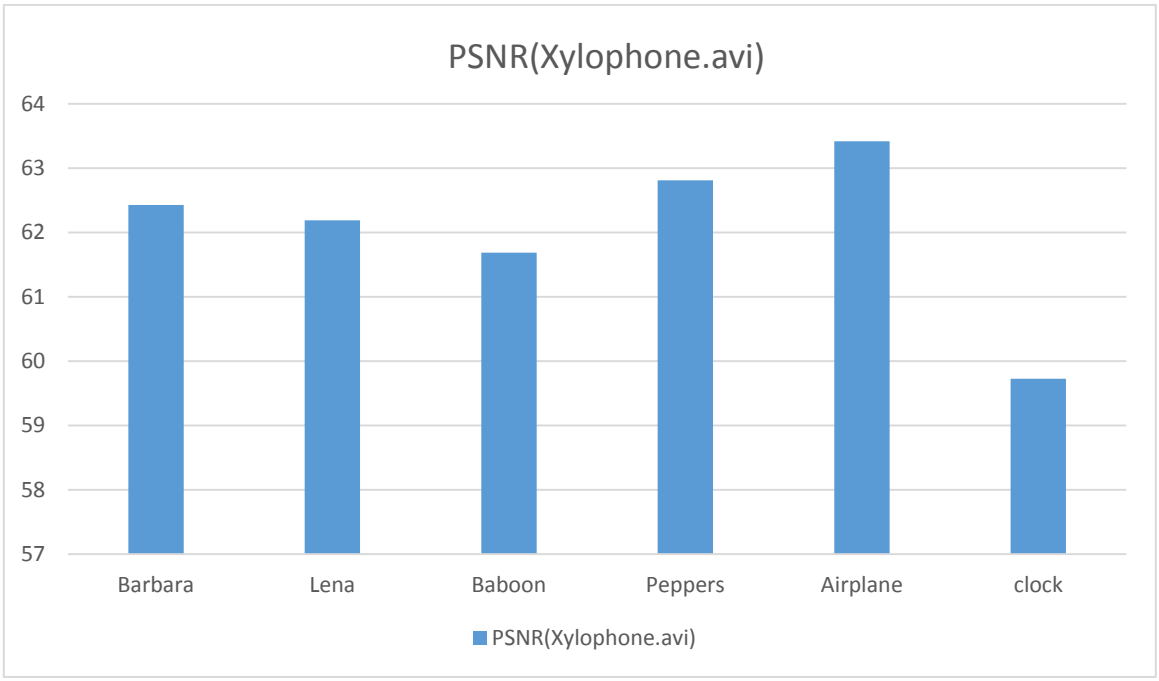
الجدول (3)

يعرض الجدول 4 مجموعة من الصور المرجعية المستخدمة كرسائل سرية وخصائصها:

Secret Image		Image Dimensions	Size(KB)
Colored	Barbara.png	512*512	31.5
	Lena.png	512*512	500
	Baboon.png	512*512	55.4
	Peppers.png	512*512	32
	Airplane.png	512*512	27.2
	Clock.png	768*1024	62.5
Grayscale	Cameraman.png	64*64	2.65
	Cameraman.png	128*128	7.39
	Cameraman.png	158*158	10.5
	Cameraman.png	256*256	37.8

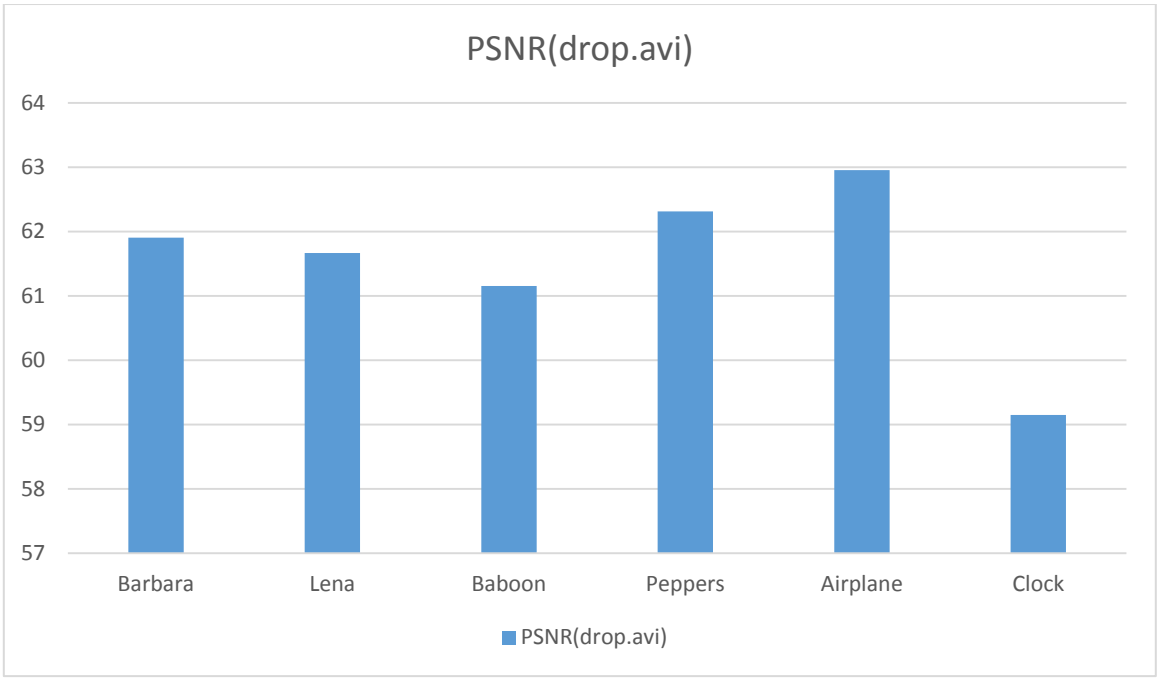
الجدول 4 خصائص الصور المستخدمة في الإخفاء

تم تطبيق الخوارزمية المقترحة من أجل عدة حالات للفيديو الغلاف والرسائل السرية الملونة ويوضح الشكل7 قيمPSNR من أجل عدة حالات للصورة الملونة عند استخدام Xylophone.avi



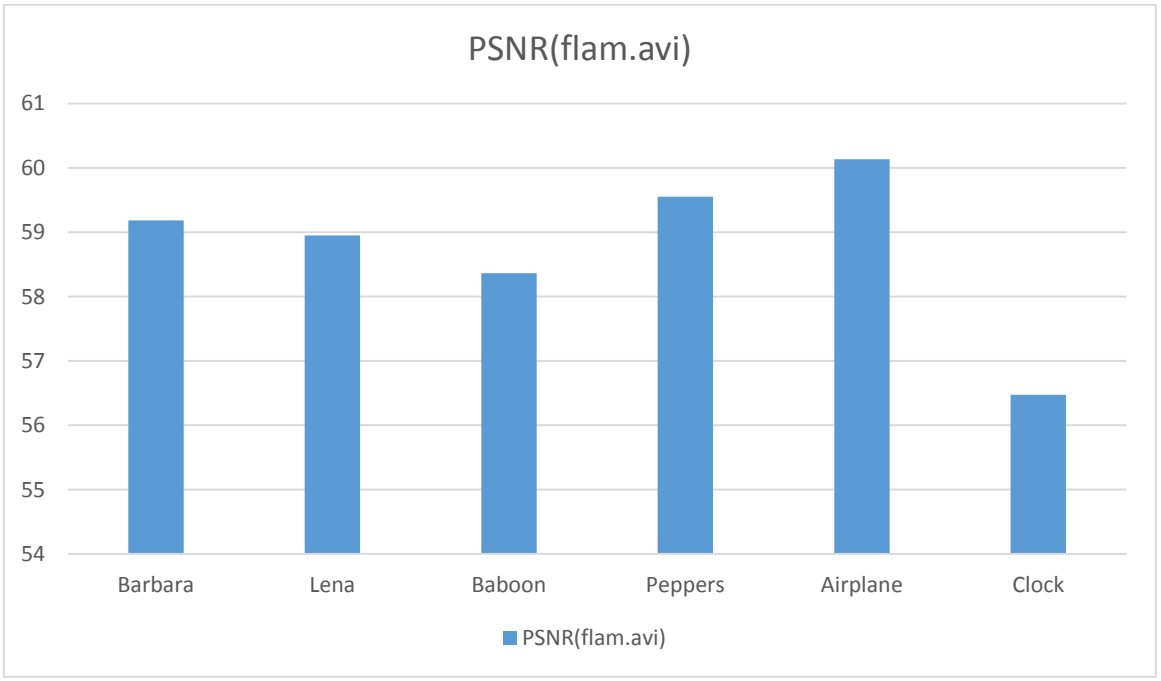
الشكل 7 قيم PSNR من أجل صور ملونة واستخدام Xylophone.avi كملف غطاء

يوضح الشكل8 قيمPSNR من أجل عدة حالات للصورة عند استخدام drop.avi



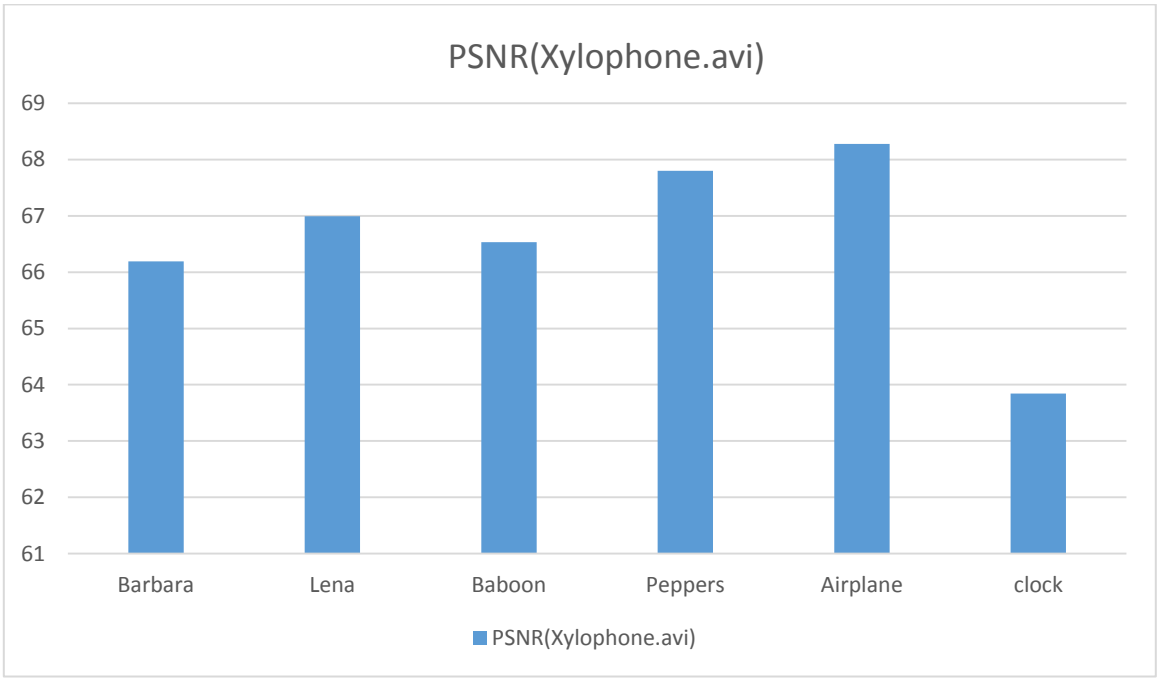
الشكل8 قيم PSNR من أجل صور ملونة واستخدام drop.avi كملف غطاء

يوضح الشكل9 قيمPSNR من أجل عدة حالات للصورة عند استخدام flam.avi



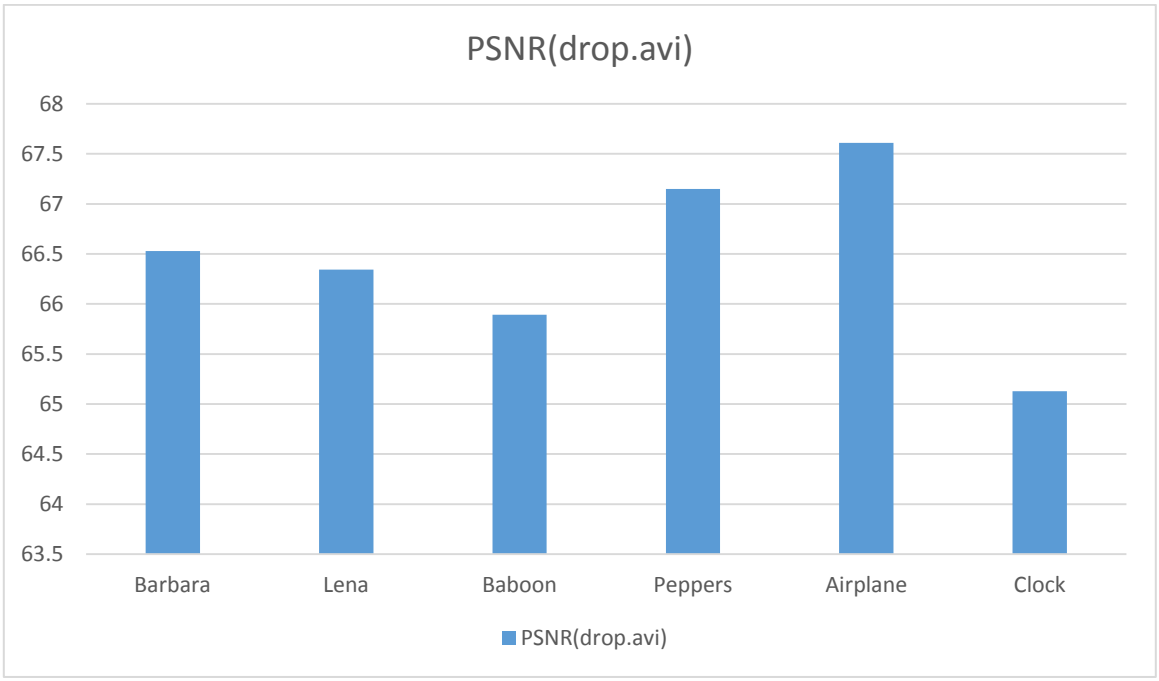
الشكل9 قيم PSNR من أجل صور ملونة واستخدام flam.avi كملف غطاء

تم تطبيق الخوارزمية المقترحة من أجل عدة حالات للفيديو الغلاف والرسائل السرية ويوضح الشكل10قيمPSNR من أجل عدة حالات للصورة الرمادية عند استخدام Xylophone.avi



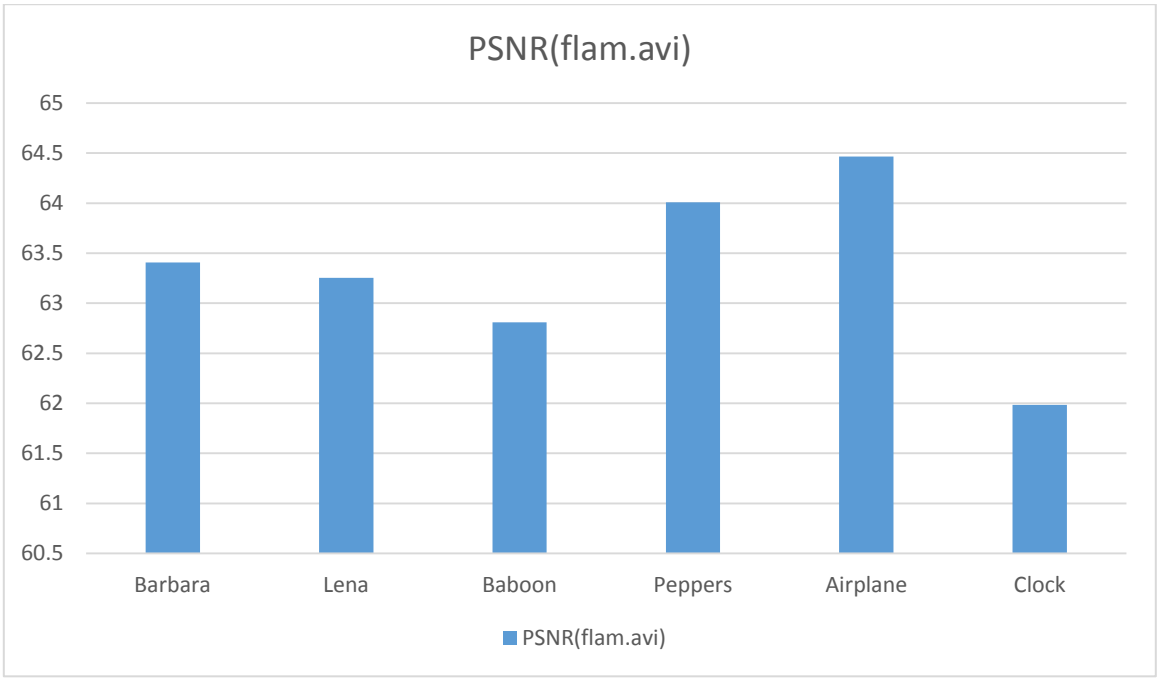
الشكل 10 قيم PSNR من أجل صور رمادية واستخدام Xylophone.avi كملف غطاء

يوضح الشكل 11 قيمPSNR من أجل عدة حالات للصورة عند استخدام drop.avi



الشكل 11 قيم PSNR من أجل صور رمادية واستخدام drop.avi كملف غطاء

يوضح الشكل 12 قيمPSNR من أجل عدة حالات للصورة عند استخدام flam.avi



الشكل 12 قيم PSNR من أجل صور رمادية واستخدام flam.avi كملف غطاء

يعرض الجدول 5 مقارنة النتائج التي توصلنا اليها مع دراسات سابقة

	اسم الدراسة	تاريخ النشر	نتائج الدراسة
1	Robust and Secured Image Steganography using Improved LSB and RC4 Cryptography with Preprocessing Operation	2019	PSNR=52.899
2	Video steganography with steganalysis	2019	PSNR=81.191
4	الطريقة المطبقة		PSNR=83.917

الجدول 5 مقارنة النتائج مع دراسات سابقة

5.الاستنتاجات والتوصيات

في هذا البحث تم تحسين خوارزمية إخفاء المعلومات بهدف إخفاء الصورة الملونة أو الرمادية في مقطع فيديو. يوفر نظامنا ثلاثة مستويات من الأمان: الضغط والتشفير وإخفاء المعلومات، وتظهر النتائج أن النظام البصري البشري (HVS) لن يكون قادرًا على معرفة أن هناك أي تغيير صغير في الفيديو، فالطريقة المقترحة تعطي قيم PSNRوMSE جيدة جدا. بالنسبة للعمل المستقبلي، سوف ندرس توفير خوارزمية إخفاء المعلومات التي تركز على أجزاء خاصة من الفيديو كحامل لإخفاء البيانات بدلاً من استخدام الفيديو بأكمله. ستؤدي مثل هذه الطريقة إلى تحسين جودة مخططات إخفاء المعلومات ومقاومة الهجمات.

6. المراجع

[1] MUSTAFA,R and ELLEITHY, K2017- Compressed and raw video steganography techniques a comprehensive survey and analysis, vol. 76, no. 20

[2] ISMSEEL,O and Al-FARRAJI,I 2017-new technique of steganography based on location of lsb International Journal of Information Research and Review, Vol. 4.

[3] HAYDAR,O and ABOKASSEM, K 2019-Enhancement the Efficiency of Data Hiding Using Data Compression and Dividing Data, vol. 7.

[4] HE,Y and YANG, G 2012- A real-time dual watermarking algorithm of H.264/AVC video stream for video-on-demand service, vol. 66, no.

[5] SHARMA,S and VIRK,I2016-Image Steganography using Two's Complement International Journal of Computer Applications, Vol.145.No.

[6] BHARDWAJ,and SHARMA,V 2016 -Image Steganography Based on Complemented Message and Inverted bit LSB Substitution Procedia Computer Science, Vol.93.

[7] SZABODKA,Z and VANDEVENNE,L 2015-Comparison of Brotli, Deflate, Zopfli, LZMA, LZHAM and Bzip2 Compression Algorithms,Google Inc.

[8] DALVIR,K 2013 -Analysis of Lossless Data Compression Techniques International Journal of Computational Engineering Research,Vol. 03.

[9] GOELRANA,KAUR,M 2013 -A Review of Comparison Techniques of Image Steganography IOSR Journal of Electrical and Electronics Engineering，Vol. 6.

[10] AL-LAHAM,M 2007 -Comparative Study between Various Algorithms of Data Compression Techniques IJCSNS International Journal of Computer Science and Network Security，Vol. 7.

[11] PRATIKSHA,S 2017- A Proposed Novel Architecture for Information Hiding in Image Steganography by using Genetic Algorithm and Cryptography International Conference on Computational Science,Vol. 5.

[12] DANS,P and DANS,A 2017- An Efficient Embedding Technique in Image Steganography Using Lucas Sequence Modern Education and Computer Sience MECS, Vol. 09.

[13] GAURAV,2015- A New Method for Image Steganography Using LSB and MSB International Journal of Recent Research Aspects, Vol 2.

[14] Biswajita Datta, Upasana Mukherjee and Samir Kumar Bandyop1adhyay, "LSB Layer Independent Robust Steganography using Binary Addition", Procedia Computer Science, Vol.85, 2016

[15] PARMAR,B and KUMAR,R 2017-High PSNR Based Image Steganography International Journal on Recent and Innovation Trends in Computing and Communication, Vol.5.

[16] ASHWINI,W and KYASA,N 2017-The Improved Image Steganography with Encryption Method and to Overcome the Compression Technique International Journal of Innovative Research in Computer and Communication Engineering ,Vol. 5.

[17] DASGUPTA,P 2012- hash based least significat bit technique for video, VoL 1.