استخدام التحويل الموجي المتقطع لإخفاء نص ضمن فيديو

Using Discrete Wavelet Transformation to Hide Text in Video

د.عمَّار سعد الريماوي

1- المقدمة Introduction:

من أهم فوائد شبكة الإنترنت سهولة نشر البيانات ونقلها عبر الشبكة، ولكن من نقاط ضعفها إمكانية تغيير البيانات مما يتطلب حماية هذه البيانات.

وتعد الوسائط الرقمية هي الوسيلة الأكثر شعبية وأكثر استخداماً في الإنترنت، لذلك أصبحت الوسيلة الأهم في إخفاء البيانات، وتم تنفيذ تقنيات عديدة لهذا الغرض.

إن إخفاء البيانات هو فن وعلم يبدأ من كتابة الرسائل المخفية لتبدو طبيعية على الجميع باستثناء المرسل والمتلقي[1].

بشكل عام يتم تضمين البيانات في ملف وسائط مثل الصور أو الفيديو أو الصوت ومن ثم إرسالها عبر شبكة الانترنت ويتم استقبالها من خلال المتلقي ليستخرج هذه البيانات واستعادتها بشكلها الحقيقي.

2- هدف البحث Research Propose

إن تطور شبكة الانترنت واستمرار نقل البيانات، جعلنا نبحث عن الطرق الأكثر أمناً لنقل هذه البيانات وخصوصاً الحساسة منها.

وأصبح تشفير البيانات قبل نقلها ضمن الوسائط (صورة –صوت –فيديو) عبر شبكة الانترنت يوفر لها جزءاً من الحماية والإخفاء يوفر لها جزءاً إضافياً ولكن لم تعد هذه الوسائل كافية مما تطلب اللجوء لوسيلة جديدة باستخدام تشفير متقدم وإخفاء بطريقة جديدة.

3- دراسة مرجعية Research Methods

قدمت أبحاث عديدة لإخفاء نص ضمن ملفات الفيديو منها:

قام شرما ديباك وغواتام اثوسا بتحويل الملف النصي إلى شكل ثنائي واستخدام تجزئة البيانات لتشفير الملف واستخدام دالة البعثرة لتحديد بكسل من الصفوف والأعمدة وثم تضمين حرف في جزء المركبة اللونية ذات اللون الأحمر في الإطار الأول، ثم حرف واحد في الإطار الثاني في جزء المركبة اللونية ذات اللون الأخضر، ثم حرف واحد في الإطار الثالث في جزء المركبة اللونية ذات اللون الأزرق وهكذا حتى نهاية الأحرف [2].

قام شيروبا وابينايا بقراءة النص المراد إخفاءه بايت تلو الآخر ومن ثم تم تحويل كل بايت إلى الترميز الثنائي والقيام بعملية التشفير باستخدام XOR على جميع بايتات الملف ومن ثم توزيع البتات باستخدام طريقة البت الأقل أهمية LSB في إطارات الفيديو [1].

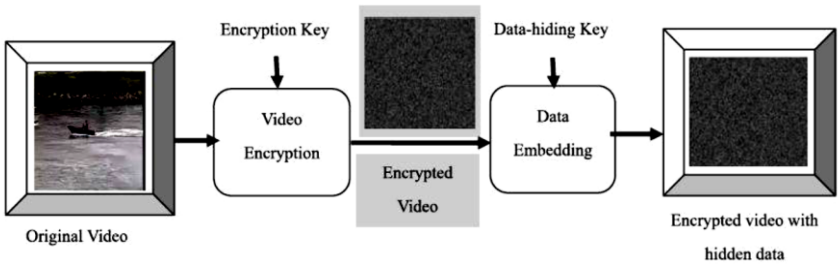
قام بهجت ابلاشا وديفيير اشيش بتحويل النص إلى ثنائي واختيار بلوكات محددة من الفيديو ومن ثم إخفاء النص ضمن إطارات محددة من الفيديو وذلك باستخدام طريقة البت الأقل أهمية LSB [3].

قام كومول وسوميت بقياس طول الملف ومن ثم استخدام خوارزمية التشفير BlowFish لتشفير النص وتحويل النص إلى الترميز الثنائي ومن ثم البحث عن مكان محدد عن طريق استخدام LSB البت الأقل أهمية [4].

الاخفاءSteganography :

كلمة Steganography هي كلمة يونانية Stegano وتعني التغطية أو السرية، والكلمة Graphia وتعني الكتابة ليصبح المصطلح الكتابة المحجوبة " Covered Writing".

وبالتالي فان مصطلح Steganography يعني فن وعلم إخفاء المعلومات السرية ضمن معلومات غير ذات أهمية ظاهرياً، وبالتالي لا أحد يعلم بالمعلومات الأصلية السرية غير الطرفين المعنيين (المرسل والمستقبل) والذين يملكون مفاتيح خاصة للتضمين والاستخراج[8].



الشكل -1- آلية عمل نظام الإخفاء [9]

بالاعتماد على الشكل أعلاه يمكن القول إن هناك ملف (فيديو مثلاً) (Cover signal)، إضافة إلى رسالة أخرى سرية (Embedded data) مخبأة بأسلوب ما ضمن هذا الملف عن طريق مفاتيح خاصة (Stegano keys) [5].

أنواع الخفاء:

هناك نوعين أساسيين لعملية الإخفاء[6] [4]:

1- الإخفاء الهش (Fragile):

في هذا النوع من الإخفاء عند أي تعديل لبنية الملف يتم تخريب المعلومات المخفية ضمنه، وبالتالي زوالها.

2- الإخفاء المتين (Robust):

في هذا النوع لا يمكن تدمير المعلومات المخفية بسهولة عند إجراء بعض التعديلات على الملف الحامل، ولكن يمكننا القول إن كمية التعديلات الواجب إجراؤها لتخريب المعلومات المخبأة ستؤدي أيضاً إلى تخريب الملف المضيف.

طرق الاخفاء[3]:

أ) الإخفاء ضمن صورة

يتم استخدام بيانات الصورة لتحتوي بيانات المعلومات السرية وبحيث تكون غير من ملحوظة من العموم.

ب) الإخفاء ضمن الصوت

تستخدم هذه التقنية بيانات الصوت لإخفاء المعلومات من خلال تغيير ترددات الصوت بحيث لا يؤثر على الصوت المسموع.

ج) الإخفاء ضمن الفيديو

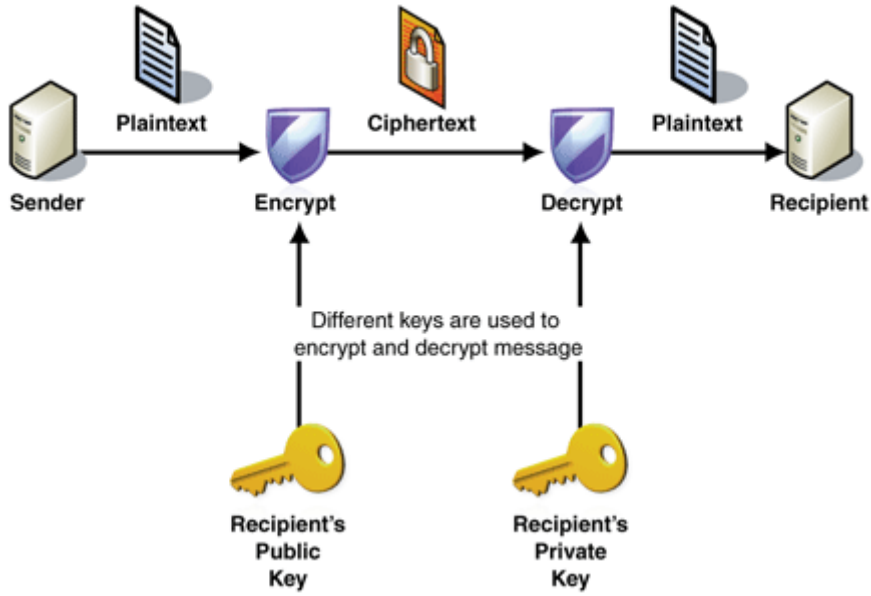
يتألف الفيديو من مجموعة صور وصوت. مما يتيح اخفاء بيانات بحجوم كبيرة.

د) الإخفاء ضمن النص

يتم إخفاء البيانات السرية في النص عن طريق استخدام أحرف الرسالة الأصلية فمثلاً يوضع الحرف الأخير من كل كلمة مختارة بشكل جيد لتشكيل كلمات الرسالة المخفية[7].

التشفير Encryption:

يُعرَّف التشفير بأنه عملية تحويل المعلومات إلى شيفرات غير مفهومة (تبدو غير ذات معنى) لمنع الأشخاص غير المُرخَّص لهم من الاطلاع على المعلومات أو فهمها، ولهذا تنطوي عملية التشفير على تحويل النصوص العادية إلى نصوص مُشفَّرَة، يستخدم في التشفير بشكل عام طرائق رياضية لتوليد النص المشفر، هناك العديد من خوارزميات التشفير للقيام بذلك [9].



الشكل -2- آلية عمل التشفير غير المتناظر

أهداف التشفير:

يوجد أربعة أهداف رئيسية وراء استخدام علم التشفير وهي كالتالي

1- السرية أو الخصوصية (Confidentiality) :

تعني حماية البيانات من جميع الأشخاص ما عدا الذين صرح لهم بالاطلاع عليها واستخدامها.

2- تكامل البيانات (Integrity) :

تعني حماية البيانات من التغيير (حذف أو إضافة أو تعديل) من قبل الأشخاص غير المصرح لهم بالتغيير.

3- إثبات الهوية (Authentication) :

تعني طريقة إثبات هوية المتعامل مع البيانات (المصرح لهم).

4- عدم الجحود (Non-repudiation) :

تعني عدم السماح بتغير هوية الشخص وذلك لمنعه من إنكار المهام الموكلة له.

الطريقة المقترحة Proposed Method

1- عملية التشفير:

قمنا بعملية إخفاء نص بعد تشفيره ووضعه ضمن مركبة الإضاءة وذلك باختيار إطارات محددة من ملف فيديو.

بالنسبة لعملية التشفير فتمت على عدة مراحل:

- في المرحلة الأولى نقوم بعملية الإزاحة بمقدار 10 وفق مفتاح محدد على أسكي النص.
- في المرحلة الثانية نقوم بالتبديل بين النص بعد قياس طوله والقيام بالتبديل باتجاه الداخل حتى نهاية النص.
- في المرحلة الثالثة نقوم بتحويل النص إلى ثنائي ويتم ذلك عن طريق تبديل البت الأول في كل حرف إلى قيمة عكسية، ومن ثم تبديل البتات من الثاني وحتى الرابع بالبتات من الخامس وحتى السابع، ويترك الثامن على حاله، فيصبح لدينا نص مشفر بشكل متقن.

النص قبل التشفير

abcdefghijklmnopqrstuvwxyz

النص بعد التشفير

klmnopqrstuvwxyzabcdefghij

الشكل -6- المرحلة الأولى من التشفير

النص قبل التشفير

klmnopqrstuvwxyzabcdefghij

النص بعد التشفير

yzwxuvstqropmnklghefcdabij

الشكل -7- المرحلة الثانية من التشفير

النص قبل التشفير

yzwxuvstqropmnklghefcdabij

النص بعد التشفير

0!@1PA`Qpa□q□□"□B3RCbSrc2#

الشكل -8- المرحلة الثالثة من التشفير

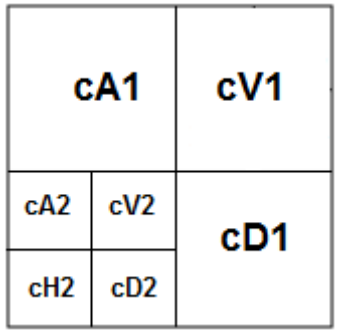
2- عملية التضمين:

قمنا بقراءة الفيديو من نوع avi ومدة الفيديو 21 ثانية ومعدل الإطارات 30 إطار في الثانية وعدد الإطارات 630 وأبعاد الإطار الواحد 120*160 وتم اختيار إطارات محددة وفق مفتاح محدد والتي سيتم إخفاء النص بداخلها وبعده قمنا بتحويل كل إطار من الإطارات المختارة إلى صيغة YUV والتي تمتاز بسهولة العودة إلى صيغة RGB وأيضاً العين لا

تتحسس للتغيرات التي تطرأ عليها وقمنا باختيار مركبة الإضاءة ومن ثم طبقنا عليها التحويل الموجي ليكون الخطأ المرتكب أصغرياً كما يلي:

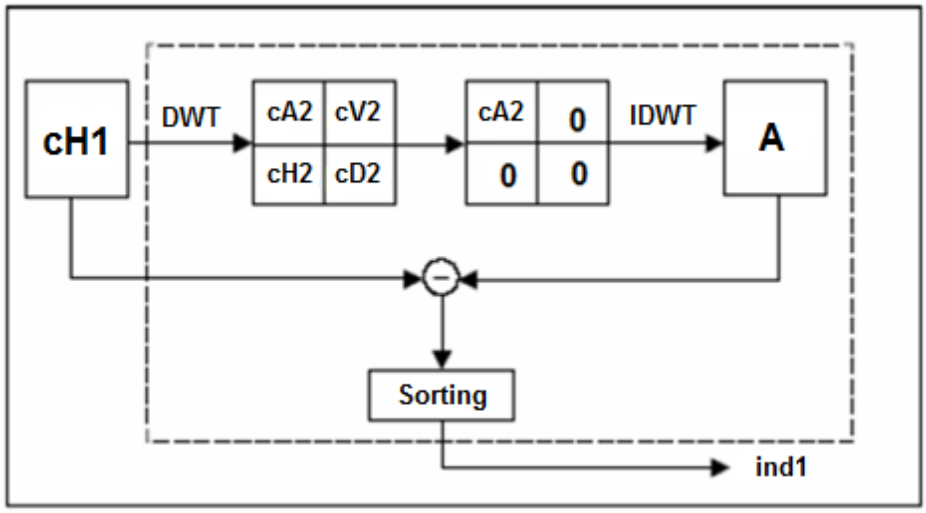
أ. نطبق التحويل الموجي DWT على الإطارات المختارة فنحصل على الأقسام الأربعة في كل إطار cA1,cH1,cV1,cD1.

ب. نطبق التحويل الموجي DWT على قسم الترددات منخفضة–المرتفعة cH1 فنحصل على الأقسام الأربعة cA2,cH2,cV2,cD2



الشكل –9– تطبيق التحويل الموجي على مستويين

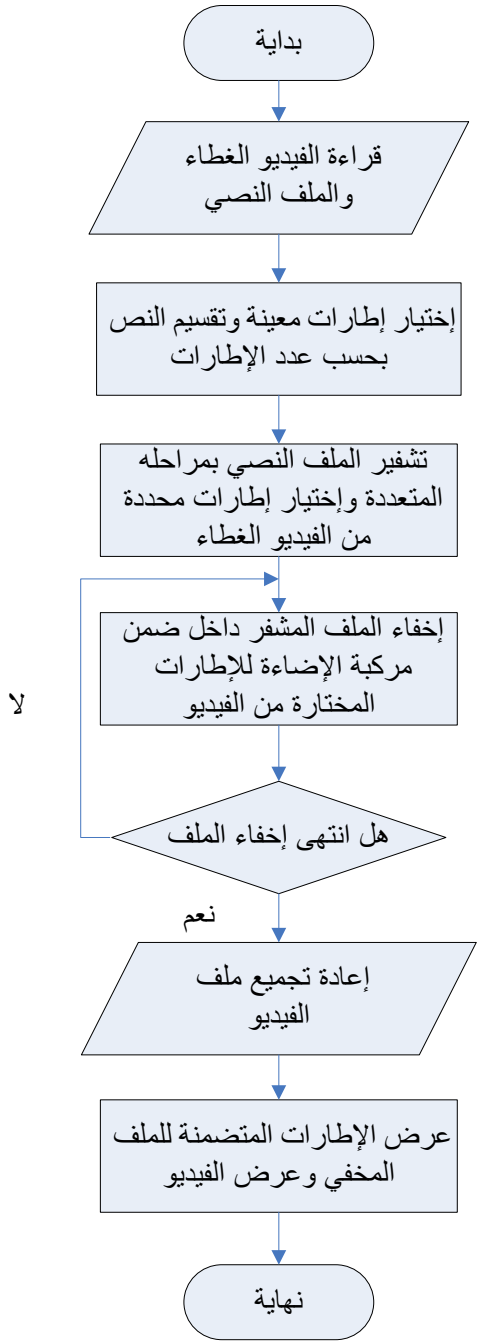
ت. نضمن النص في cH1 كمايلي:



الشكل –10– طريقة حساب الأماكن التي يمكن تضمين النص فيها

- نعيد تشكيل الأقسام بالشكل cA2،0،0،0 ونحسب التحويل الموجي العكسي لها IDWT فنحصل على A.
- نحسب الفرق بين cH1 و A بالقيمة المطلقة ind=|cH1| - |A|.
- نرتب العناصر ind تصاعدياً ind1=sort(ind) للحصول على الترددات المنخفضة في هذا الجزءcH1 .
- نضمن النص في cH1 في الأماكن المحددة بـ ind1.

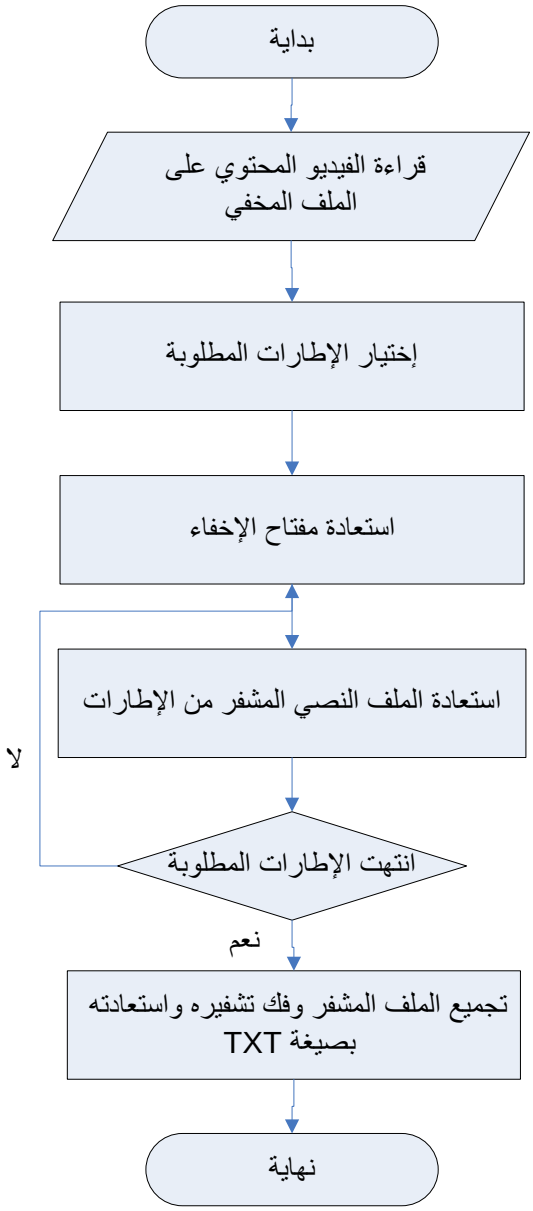
ث. نحسب التحويل الموجي العكسي مرتين فنحصل على الإطار المتضمن للنص وبنفس الطريقة لباقي الإطارات ثم نقوم بتجميع الإطارات وتشكيل الفيديو المتضمن للنص المشفر.



الشكل -11- المخطط الخوارزمي لعملية إخفاء الملف

3- مرحلة الاستخراج:

1. نستخرج الإطارات المحددة والتي تحتوي النص المخفي والمشفر من ملف الفيديو ونقوم بتحويلها لصيغة YUV ونستخرج مركبة الإضاءة.
2. نطبق التحويل الموجي DWT على مركبة الإضاءة فنحصل على الأقسام الأربعة cA1,cH1,cV1,cD1.
3. نطبق التحويل الموجي على cH1 فنحصل على الأقسام الأربعة cA2,cH2,cV2,cD2.
4. نعيد تشكيل الأقسام بالشكل cA2،0،0،0 ونحسب التحويل الموجي العكسي لها IDWT فنحصل على A1.
5. نحسب الفرق بين cA2 و A1 بالقيمة المطلقة ind=|cH1| - |A1| .
6. نرتب العناصر ind تصاعدياً ind1=sort(ind).
7. نستخرج النص المتواجد في cH1 ضمن الأماكن المحددة بـ ind1.
8. ننفذ مراحل فك التشفير على الملف وذلك بشكل عكسي لطريقة التشفير وذلك للحصول على أجزاء الملف من كل إطار.
9. نقوم بتجميع أجزاء الملف للحصول على الملف الأصلي.



الشكل -11- المخطط الخوارزمي لعملية استعادة الملف المخفي

تم استخدام عدة مقاييس للدراسة [5] [6] وهي:

1- نسبة الخطأ في الإطار Mean Square Error(MSE)

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(f_{ij}-g_{ij})^2$$

حيث:

هما الصف والعمود بالنسبة للإطار الغطاءM,N

هي الوحدة الصورية من الإطار الغطاء قبل الاخفاءfij

هي الوحدة الصورية من الإطار بعد اخفاء النص داخلهاgij

2- معدل الإشارة إلى الضجيج Signal to Noise Ratio(SNR) وهو مقدار بين 0 و100 يعبر عن علاقة الإطار الأصـــلي W والإطار الذي يحتوي النص المخفي Ŵ ويعطى بالعلاقة الراضية التالية:

$$SNR(W,\hat{W}) = 10\log_{10}\frac{\sum_{i=1}^{N} w_i^2}{\sum_{i=1}^{N}(W_i-\hat{W}_i)^2}$$

3- معدل طاقة الإشارة إلى الضجيج Peak Signal to Noise Ratio(PSNR) وهو مقدار بين 0 و100 يعبر عن علاقة الإطار الأصـــلي f(m,n) والإطار الذي يحتوي النص المخفيf'(m,n) ويعطى بالعلاقة الراضية التالية:

$$PSNR = 20\log_{10}[255/RMSE]$$

Where

$$RMSE = \sqrt{\frac{1}{M*N}\sum_{i=1}^{M}\sum_{j=1}^{N}[\tilde{f}(m,n)-f(m,n)]^2}$$

4- الترابط Normalized Correlation و هو مقدار بين 0 و 1 يعبر عن الفرق ببن الوضـــوح بين الإطـار الـذي يحتوي على النص المخفي ŵ والإطـار العادي w ويعطى بالعلاقة الراضية التالية:

$$\rho(w,\hat{w}) = \frac{\sum_{i=1}^{N} w_i \hat{w}_i}{\sqrt{\sum_{i=1}^{N} w_i^2}\sqrt{\sum_{i=1}^{N} \hat{w}_i^2}}$$

5- Time زمن قياس تنفيذ الكود المخصص للإخفاء.

تقييم الطريقة المقترحة Proposed Method Evaluation

تم مقارنة الطريقة المقترحة مع الطريقة الموجودة في المرجع [3] والتي اعتمدت ملف فيديو من نوع avi وتم فيها تقسيم الفيديو إلى عدة إطارات وفق مفتاح محدد وتم تشفير الملف بطريقة RSA الإخفاء بطريقة LSB.

'Frames	Frames	SNR	PSNR	MSE	CORR	Time
'Frame1	**Frame1**	37.22	48.08	1.00	0.9999	0.285
'Frame2	**Frame2**	39.33	47.42	1.17	0.9998	0.492
'Frame3	**Frame3**	37.86	47.61	1.12	0.9997	0.435
'Frame4	**Frame4**	39.93	48.05	1.01	0.9999	0.437
'Frame5	**Frame5**	38.72	47.26	1.22	0.9997	0.462
'Frame6	**Frame6**	38.05	47.48	1.16	0.9996	0.486

جدول -1- النتائج للطريقة المقترحة وعلى عدة إطارات محددة

حيث Frame تمثل الإطار قبل الإخفاء و'Frame تمثل الإطار بعد الإخفاء

الشكل –12– قبل وبعد تنفيذ الإخفاء للإطارات المحددة في الطريقة المقترحة

'Frames	Frames	SNR	PSNR	MSE	CORR	Time
'Frame1	Frame1	35.28	46.14	1.57	0.9941	1.360
'Frame2	Frame2	37.18	45.27	1.92	0.9993	1.414
'Frame3	Frame3	35.54	45.29	1.92	0.9994	1.489
'Frame4	Frame4	37.16	45.27	1.93	0.9993	1.494
'Frame5	Frame5	36.71	45.25	1.93	0.9992	1.434
'Frame6	Frame6	36.72	46.14	1.57	0.9991	1.466

جدول –2– النتائج للطريقة في المرجع [3] وعلى عدة إطارات محددة

حيث Frame تمثل الإطار قبل الإخفاء وFrame' تمثل الإطار بعد الإخفاء

تم قياس جودة الإطارات المستخرجة عن طريق حساب Correlation وPSNR وMSE وTIME بين الإطار المضمن والإطار بعد التضمين وحصلنا على نتائج الطريقة المقترحة الموضحة بالجدول –1– ونتائج الطريقة الواردة بالمرجع[3] موضحة بالجدول –2– وكانت نتائج الطريقة المقترحة أفضل بالنسبة لهذه مقياس.

الشكل –13– قبل وبعد تنفيذ الإخفاء للإطارات المحددة في طريقة المرجع [3]

Frames Our−Ref	Frames Our−Ref	SNR Our−Ref	PSNR Our−Ref	MSE Our−Ref	CORR Our−Ref	Time Our−Ref
'Frame1	Frame1	1.94	1.94	−0.57	0.0058	−1.075
'Frame2	Frame2	2.15	2.15	−0.75	0.0005	−0.922
'Frame3	Frame3	2.32	2.32	−0.80	0.0003	−1.054
'Frame4	Frame4	2.77	2.78	−0.92	0.0006	−1.057
'Frame5	Frame5	2.01	2.01	−0.71	0.0005	−0.972
'Frame6	Frame6	1.33	1.34	−0.41	0.0005	−0.98

الجدول-3- مقارنة بين نتائج الطريقتين

يوضـــح هذا الجدول الفرق بين الطريقة المقترحة والطريقة الواردة بالمرجع [3] والتي تؤكد جودة الطريقة المســتخدمة بكل المقاييس، والقيم الســالبة في الجدول أيضــاً تعطي نتائج إيجابية للطريقة المقترحة لأن هذه القيم تعبر عن الوقت Time والخطأ المرتكب MSE فكلما كان الوقت Time أصــغر كانت الطريقة أســرع وكلما كان الخطأ المرتكب MSE أصغر كلما كانت الطريقة أدق.

1. مقاومة الهجومات:

قمنا بتنفيذ عدة هجومات على إطارات الفيديو المتضمن النص المشفر بالطريقة المقترحة و بالطريقة الواردة بالمرجع [3] وهي ضجيج من النوع Gaussian(0,0.0001) و ضجيج من النوع Salt& pepper(0.01) و ضجيج من النوع Speckle(0.001).

ثم قمنا بحساب PSNR وحساب الترابط Normalized Correlation بينهما وكانت النتائج على الشكل التالي:

الشكل –14– قبل وبعد تنفيذ الهجمات للإطارات المحددة في الطريقة المقترحة

PSNR Gaussian F,'F	**PSNR** Salt & pepper F,'F	**PSNR** Speckle F,'F	**correlation** Gaussian F,'F	**Correlation** Salt & pepper F,'F	**Correlation** Speckle F,'F
40.11	24.38	40.88	0.9994	0.9783	0.9995
37.18	24.95	40.10	0.9997	0.9897	0.9993
39.45	24.37	39.39	0.9995	0.9832	0.9995

39.50	24.93	37.91	0.9996	0.9898	0.9995
39.46	24.57	38.01	0.9996	0.9877	0.9994
39.37	24.84	38.81	0.9995	0.986	0.9994

الجدول–4– نتائج الهجمات للطريقة المقترحة

PSNR Gaussian F,'F	**PSNR** Salt & pepper F,'F	**PSNR** Speckle F,'F	**correlation** Gaussian F,'F	**Correlation** Salt & pepper F,'F	**Correlation** Speckle F,'F
39.17	24.58	39.76	0.9993	0.9795	0.9994
37.34	24.86	38.68	0.9996	0.9897	0.9995
39.01	23.49	39.00	0.9994	0.9796	0.9994
39.07	24.57	37.71	0.9996	0.9877	0.9994
39.09	24.61	38.55	0.9995	0.9853	0.9994
39.13	24.95	35.88	0.9997	0.9932	0.9995

الجدول–5– نتائج الهجمات للطريقة في المرجع [3]

تم احتساب العلاقات بالمقارنة بين الإطارات F قبل حدوث الهجمات والإطارات 'F بعد الهجمات.

الشكل –15– قبل وبعد تنفيذ الهجمات للإطارات المحددة في الطريقة المرجع [3]

PSNR Gaussian (our-ref)	**PSNR** Salt & pepper (our-ref)	**PSNR** Speckle (our-ref)	**correlation** Gaussian (our-ref)	**Correlation** Salt & pepper (our-ref)	**Correlation** Speckle (our-ref)
0.9400	−0.2000	1.1200	0.0001	−0.0012	0.0001
−0.1600	0.0900	1.4200	0.0001	0.0000	−0.0002
0.4400	0.8800	0.3900	0.0001	0.0036	0.0001
0.4300	0.3600	0.2000	0.0000	0.0021	0.0001

0.3700	−0.0400	−0.5400	0.0001	0.0024	0.0000
0.2400	−0.1100	2.9300	−0.0002	−0.0072	−0.0001

الجدول-6- مقارنة بين نتائج الطريقتين

تم تنفيذ هجمات محددة على الطريقة المقترحة والنتائج موضحة بالجدول −4− وتنفيذ هجمات محددة على الطريقة في المرجع [3] والنتائج موضحة بالجدول −5− وأيضاً كانت النتائج أفضل للطريقة المقترحة.

كما يبين الجدول −6− الفروقات بين الطريقتين حيث نلاحظ أن طريقتنا المقترحة أفضل من الطريقة الواردة في المرجع [3]

Text	Gaussian		Salt & pepper		Speckle	
	PSNR	CORR	PSNR	CORR	PSNR	CORR
our	28.174	0.995	58.890	1.000	19.901	0.970
ref	15.371	0.930	55.534	1.000	16.879	0.955

الجدول-7- الفرق بين الطريقتين بعد التطبيق على النص

تم قياس الترابط و PSNR للملف النصي قبل التضمين وبعد الاستخراج وكما نلاحظ الفرق واضح أن الطريقة المقترحة أفضل من طريقة المرجع [3] كما في الجدول −7−.

2. أثر الضغط:

Text	Jpg 98		Jpg 100	
	PSNR	CORR	PSNR	CORR
our	19.654	0.969	20.911	0.976
ref	11.872	0.881	14.478	0.916

الجدول-8- الفرق بين الطريقتين بعد تنفيذ الضغط واستعادة النص

وعند تنفيذ الضغط على الإطارات المحددة في ملف الفيديو بنسبة 100 و98 نلاحظ أن الطريقة المقترحة أفضل من الطريقة بالمرجع[3].

ملاحظة: تم استخدام برنامج الماتالاب النسخة 10 وكمبيوتر بذاكرة 2 غيغا ومعالج doul core 1.87 غيغا هرتز بنسخة ويندوز 7

5- الاستنتاجات والتوصيات Conclusions and recommendations

1. استخدام ملفات الفيديو للإخفاء أتاح الإمكانية لتخزين نصوص بحجوم كبيرة بسبب استخدام العديد من الإطارات.
2. القيام بالتشفير على ثلاثة مراحل صعب عملية اكتشاف النص واستعادته بشكله الاساسي.
3. لا يمكن ملاحظة الإخفاء بالعين المجردة.
4. المقياس المستخدمة أثبتت كفاءة الخوارزمية المستخدمة.
5. نقترح تطبيق الطريقة المقترحة على ملفات الصـــوت وعلى ملفات أخرى من الفيديو.
6. نقترح استخدام الطريقة المقترحة مع طريقة التجيب المتقطع DCT.

ملخص البحث Abstract

تستخدم تقانة المعلومات في تسيير معظم أعمالنا في الوقت الراهن، مما يتوجب علينا الانتباه إلى ضرورة تأمين معلوماتنا الحساسة (كالحسابات المصرفية أو كلمات المرور أو حقوق ملكية أو أي معلومات هامة يتم نقلها)، وأيضاً يجب تأمين المعلومات ضد الهجمات أو الاختراقات التي تحاول سرقة المعلومات أو تشويهها، ليتم نقلها عبر الشبكة بشكل سري وآمن بعد تشفيرها وإخفاءها.

في بحثنا هذا تم استخدام ملف فيديو كوسط ناقل لإخفاء النص، ومن خلال هذه الطريقة تم توفير الدقة في العرض والموثوقية العالية في نقل البيانات.

قمنا باختيار إطارات محددة من الفيديو وطبقنا التحويل الموجي المتقطع لإخفاء النص المشفر، مما يضمن لنا وصول الملف النصي بالشكل الصحيح وبسرية كبيرة.

الكلمات المفتاحية Keywords

إخفاء، تشفير، تعمية، تضمين، علم الإخفاء، إطار الفيديو.

Abstract

The information technology was managed most of our currently works, that we must pay attention to the Important of security our critical information. Such as (bank accountancies, passwords, or any information during its transfer). We must also secure information against attacks or hacking, which attempts to steal information or damage it in order to be transmitted secretly and safely through network after hiding and encryption it.

In our research, we used a video file as a cover media to hide the text. This method provides a high quality in display and authenticity in data transfer.

We chose specific frames from the video file and we apply DWT to hide the encryption text, which ensure that the text file is delivered correctly and secretly.

Keywords الكلمات المفتاحية

Data Hiding, Cryptography, Steganography, Embedding, Video Frame.

6- المراجع Reference

1- SHERUBHA P, ABINAYA P, 2014, "Concealed Message Transfer Using Lifting Scheme Based On Video Steganography", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 3, 485-489p.

2- GAUTAM A, SHARMA D, 2014, "An Approach To Hide Data In Video Using Steganography", International Journal of Research in Engineering and Technology, Vol. 3, 164-168p.

3- BHAGAT A, DHEMBHARE A, 2015, "An Efficient and Secure Data Hiding Technique – Steganography", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, 941-949p.

4- KOMAL P, SUMIT U, HITESH G, 2013 "Information Hiding using Least Significant Bit Steganography and Blowfish Algorithm" International Journal of Computer Applications, Vol. 63, 24-28p.

5- ATASSI Y, 2011, "Robust Watermarking Algorithm", Journal of Al-Baath University, Vol. 33, 119-146p.

6- HAJJARA S, ABDALLAH M, HUDAIB A, 2009, "Digital Image Watermarking Using Localized Biothogonal Wavelets", European Journal Of Scientific Research, vol 26, 594-608p.

7- EL-ZOUKA, H A, 2010, "Distortion Free Steganography System Based on Genetic Algorithm ", Journal of Information Hiding and Multimedia Signal Prossing, vol. 2, 11-16p.

8- HAMAMI, A H, 2008, "Information Hidings, Steganography and watermark". Ethraa for Publishing and Distribution, Jordan, 550p.

9- STALLINGS, W, 2005, "Cryptography and Network Security Principles and Practices". Prentice Hall, USA, 592p.

10- KAUR M, KAUR A, 2014, " Improved Security Mechanisam of text in Video by using Steganographic Technique: A Review", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 4, 216-220p.