Design and Implemented of an Algorithm for Covered Writing on a Video File (mov)

Raed R. A-Naima — **Technical College / Mosul**

Sarah B. Al-Naima — **Technical Teaching Organization / Mosul**

ABSTRACT

In this research, video file type (mov) is used to hide an English text. This method offered high accuracy and secure for data transitions. First, frames are extracted from video file. Then on algorithm has been designed and implemented to hide and extract the text message. Hiding process concerns with converting the text into corresponding codes, then store these codes inside the basic color panel of video file and exactly on the fourth order after floating point of every pixel. Extracting process concerns with inversing the whole process of hiding. Experimental results demonstrated success of hiding process.

The designed algorithm has been implemented using Matlab (ver. 7) on P4 computer.

Keywords: Covered Writing, Video File.

تصميم وتمثيل خوارزمية للكتابة المغطاة على ملف فيديو (mov)

رائد رافع عمر النعمة — *الكلية التقني/ الموصل*

سارة بشير علي النعمة — *هيئة التعليم التقني / الموصل*

تاريخ استلام البحث:٢٠١٠/8/16 **تاريخ قبول البحث:٢٠١٠/١١/10**

الملخص

في هذا البحث تم استخدام ملف فيديو من نوع mov كوسط ناقل لإخفاء النصوص، وقد وفرت هذه الطريقة الدقة الشديدة في العرض والأمنية العالية في نقل البيانات. حيث تم تقطيع ملف الفيديو إلى مجموعة من الصور الثابتة، وبعدها تم تصميم وتمثيل خوارزمية لإخفاء واسترجاع الرسالة النصية. تم الإخفاء بتحويل أي رسالة نصية إلى مجموعة من الرموز وخزنها داخل لوحة الألوان الرئيسية لملف الفيديو وبالتحديد عند الرقم العشري الرابع بعد الفارزة العشرية لكل وحدة لونية. أما الإسترجاع فكان بعكس عملية الإخفاء، فقد تم استرجاع رموز الرسالة النصية من ملف الفيديو وإعادتها إلى صيغتها الأصلية. أثبتت النتائج العملية نجاح عملية التغطية.

تم تمثيل الخوارزمية باستخدام لغة ماتلاب (الإصدار 7) وعلى حاسبة نوع P4.

الكلمات المفتاحية: الكتابة المغطاة، ملف فيديو.

1. المقدمة Introduction

ان استخدام الاتصالات السرية بواسطة رسائل مرمزة كان موضوع التطبيق العملي عبر التاريخ القديم والحديث فعند إرسال يوليوس قيصر رسائله إلى زعيمه كان يستخدم الشفرة الهجائية ليضمن عدم معرفة ما في الرسالة حال وقوعها في أيدي العدو.

وفي الحروب الحديثة تم استخدام الرموز والشفرات لضمان عدم تسرب المعلومات السرية إلى العدو، فضلا عن استعمال الرموز والشفرات من قبل الوكالات الأمنية لعدد من الحكومات والجيش والسلك الدبلوماسي لغرض إجراء الاتصالات. وهناك أيضا استعمالات أخرى فعدد كبير من الاتصالات التجارية ترسل عن طريق السلك أو أي وسط ناقل أخر على هيئة رموز لتقليل كلفة وحجم الرسائل [1].

لا يخفى بأن هنالك بحوث اهتمت بعملية تغطية بيانات نصية بداخل بيانات نصية [2]، وبحوث أخرى اهتمت بعملية تغطية بيانات نصية بداخل بيانات صورة نوع BMP [1]. وهناك بعض المصادر التي تكلمت عن الإخفاء في مجال الفيديو عن طريق الوصول إلى frames المكونة لملف الفيديو [3] أو حتى المكونة لملف كليب VideoClip [4]. أما هذا البحث فقد اهتم بتطوير عملية تغطية بيانات نصية بداخل ملف فيديوي بعد تقطيعه إلى صور.

2. نظام التغطية Steganography

كلمة (Steganography) مشتقة من اللغة الإغريقية وتتألف من مقطعين(Steganos) وتعني مغطاة أو سرية و (Graphy) وتعني الكتابة أو الرسم وهما معا يعنيان مصطلح الكتابة المغطاة (covered writing) [5]. ويمكن تعريف الـ (Steganography) على أنه علم وفن الاتصال بطريقة تخفي وجود هذا الاتصال أي نقل البيانات خلال بيانات أخرى تستخدم كمضيف (Host) أو حامل (Carrier) غير مؤذية كناقلات لتلك البيانات وبطريقة لا تسمح لأي عدو أو مراقب بان يكتشف أن هناك بيانات سرية [6]. والإخفاء يهتم بسرية محتويات الرسالة إضافة إلى تحقيق سرية الاتصال وعندما يشك المتطفل بوجود معلومات مخفية فأنه يحاول أن يفك أو يدمر أو يغير الرسالة ثم يرسلها إلى المستلم الذي يعلم كيف يفسرها.

فالكتابة المغطاة هي إخفاء الرسائل السرية ضمن رسالة أخرى تبدو غير مؤذية أو ناقل (Carrier) يمكن أن يكون الناقل أي شيء يستخدم لنقل المعلومات، مثلا خشب أو لوحة أقراص، كعوب أحذية مجوفة، صور مطبوعة، صور صغيرة جدا أو ترتيبات كلمة [2]. تتضمن النواقل الرقمية البريد الألكتروني (E-Mail)، الصوت (Audio)، الصور والرسائل الفيدوية [7].

3. الإخفاء في ملفات الفيديو الرقمية Hiding in Digital Video Files

كما ذُكِر في الفقرة السابقة، هناك ملفات عديدة في الحاسوب من الممكن استخدامها كوسط لإخفاء الرسالة السرية ومن هذه الأوساط هي الصور الثابتة التي يتألف منها ملف الفيديو والمعروفة (frames) بذلك يمكن إخفاء المعلومات في الصور، فلإخفاء المعلومات يتم تضمين الرسالة من خلال اختيار مكان الضوضاء والتي لا تلفت النظر حيث يكون هناك اختلاف في اللون الطبيعي في هذه المناطق بكثرة.

بصورة عامة فان الحاسوب يتعامل مع ملف الفيديو على أنه مجموعة من الصور. ويتعامل الحاسوب مع الصورة على أنها منظومة ثنائية الأبعاد كل موقع فيها يمثل نقطة أو ما يعرف بالـ (Pixel) وهي أصغر وحدة لتمثيل موقع معين على الشاشة، وكلما زاد عدد هذه الوحدات الصورية (Pixels) ضمن حدود ثابتة ازداد تقارب هذه الصورة من الواقع في تحسس العين البشرية لحقائق هذه الصورة وهذا ما يسمى (Resolution)، والتجمع لهذه النقاط بقيمها الخاصة من الألوان وتدعى بـ RGB وهي مختصر (Red, Green, Blue) يكون لنا الصورة المرئية بحيث يمكن للعين المجردة إدراكها في الصور فلتمثيل كل نقطة من نقاط المصفوفة يكون من خلال استخدام ثلاث من الوحدات

الخزنيه أو ما يدعى بالبايت، حيث يمكن لنا من الألوان الرئيسية الثلاث أن نحصل على مزيج لوني بحيث يخصص بايت واحد لكل لون من الألوان [8].

إن الصور التي تتكون من ثمانية أرقام ثنائية تعتبر كل وحدة صورية هي مؤشر (index) لكل وحدة لونية في لوحة الألوان الأساسية. وهذه القيم تمثل شدة الإضاءة في تلك النقطة اعتمادا على الألوان الأساسية (RGB). لذلك استُخدمت شدة كل لون من الألوان الأساسية لكل وحدة صورية كحاوٍ للرسالة، وقد رُمِّزت معلومات الرسالة إلى أرقام عشرية ثم خُزنت بإضافة كل رقم عشري من الرسالة إلى الرقم العشري الأقل أهمية من شدة اللون. حيث أن الأرقام العشرية الأخرى تحتوي على معلومات كافية لتمثيل اللون الصحيح لتلك الوحدة الصورية، وعند تغيير الرقم العشري الأقل أهمية لا يؤثر ذلك على الصورة بشكل ملحوظ.

4. الخوارزمية المقترحة Proposed Algorithm

قدمت هذه الخوارزمية مسار جديد في الكتابة المغطاة. حيث استخدمت ملف فيديو نوع mov كناقل لنص سري. ولهذه الطريقة ميزات عديدة، فهي فتحت طريق لتغطية البيانات لأنواع أخرى من الصور وعدم الإنغلاق على أنواع معينة، وفتحت طريقا آخر لتغطية كمية كبيرة من البيانات داخل وسط فيديوي بدلا من تحديد حجم البيانات المخزونة بحجم وسط ناقل صغير الحجم، كما استفادت هذه الطريقة من عملية تقطيع ملف الفيديو إلى مجموعة من الصور الثابتة والقيام بخزن البيانات في لوحة الألوان الرئيسية الثلاثة التي تشكل ألوان الصورة مما أتاح مساحة خزنية أكبر من الصور التي تحوي تدرج لوني واحد (مثل الصور ذات التدرج الرمادي).

4.1 عملية إخفاء الرسالة Message Hiding Process

مرت عملية إخفاء الرسالة داخل ملف الفيديو بالخطوات التالية:

الخطوة الأولى: إدخال نص الرسالة.

الخطوة الثانية: ترميز أحرف الرسالة إلى أرقام عددية عشرية بحيث كل حرف يقابله ثلاثة أرقام عددية عشرية، مثلا: a=097 ، b=098 ، c=099 ، .....

الخطوة الثالثة: تقطيع ملف الفيديو إلى صور ثابتة (frames).

الخطوة الرابعة: تصفير العمود ذو المرتبة العشرية الأدنى – وهو هنا العمود الرابع بعد الفارزة العشرية – لكل رقم في لوحة الألوان الرئيسية (الأحمر، الأزرق والأخضر)، وبحسب المعادلات رقم 1 ، 2 و 3:

$$map_{i,1}=(fix(map_{i,1}\times 1000))/1000 \quad \ldots(1)$$

$$map_{i,2}=(fix(map_{i,2}\times 1000))/1000 \quad \ldots(2)$$

$$map_{i,3}=(fix(map_{i,3}\times 1000))/1000 \quad \ldots(3)$$

حيث:

map هي لوحة الألوان الرئيسية

i عداد صفوف مصفوفة *map*

fix إيعاز إقتصاص العدد الصحيح وتصفير الكسر العشري

الخطوة الخامسة: القيام بحشر الأرقام الترميزية للرسالة بالمرتبة الأدنى التي تم تصفيرها في الخطوة السابقة وبحسب المعادلات رقم 4 ، 5 و 6:

$$map_{i,1}(new) = map_{i,1}(old) + x_i \times 0.0001 \quad \ldots (4)$$

$$map_{i,2}(new) = map_{i,2}(old) + x_{i+n} \times 0.0001 \quad \ldots (5)$$

$$map_{i,3}(new) = map_{i,3}(old) + x_{i+2n} \times 0.0001 \quad \ldots (6)$$

حيث:

map هي لوحة الألوان الرئيسية

i عداد صفوف مصفوفة *map*

x مصفوفة الأرقام المرمزة للرسالة

n عدد صفوف مصفوفة *map*

الخطوة السادسة: إعادة دمج وتجميع ملف الفيديو بعد إخفاء النص فيه.

4.2 عملية إسترجاع الرسالة Message Recovery Process

مرت عملية إسترجاع الرسالة من ملف الفيديو بالخطوات التالية:

الخطوة الأولى: تقطيع ملف الفيديو إلى صور ثابتة (frames).

الخطوة الثانية: القيام بسحب الأرقام الترميزية للرسالة من المرتبة الأدنى لكل رقم في لوحة الألوان الرئيسية وبحسب المعادلات رقم 7 ، 8 و 9:

$$y_i = round((map_{i,1} \times 1000) - fix(map_{i,1} \times 1000)) \times 10 \quad \ldots (7)$$

$$y_{i+n} = round((map_{i,2} \times 1000) - fix(map_{i,2} \times 1000)) \times 10 \quad \ldots (8)$$

$$y_{i+2n} = round((map_{i,3} \times 1000) - fix(map_{i,3} \times 1000)) \times 10 \quad \ldots (9)$$

حيث:

map هي لوحة الألوان الرئيسية

i عداد صفوف مصفوفة *map*

n عدد صفوف مصفوفة *map*

y ستحوي الأرقام المرمزة للرسالة بعد تطبيق المعادلات

round إيعاز إقتصاص العدد الصحيح وإلغاء الكسر العشري

الخطوة الثالثة: إعادة تجميع رموز الرسالة إلى ثلاثة أرقام ليقابل كل منها حرفا معروفا وبحسب المعادلة رقم 10:

$$y2_j = y_i \times 100 + y_{i+1} \times 10 + y_{i+2} \quad \ldots (10)$$

حيث:

y2 ستحوي الأرقام المرمزة للرسالة مقسمة كل ثلاثة أرقام على حدة

j عداد لحروف الرسالة المرمزة

i عداد صفوف مصفوفة *map*

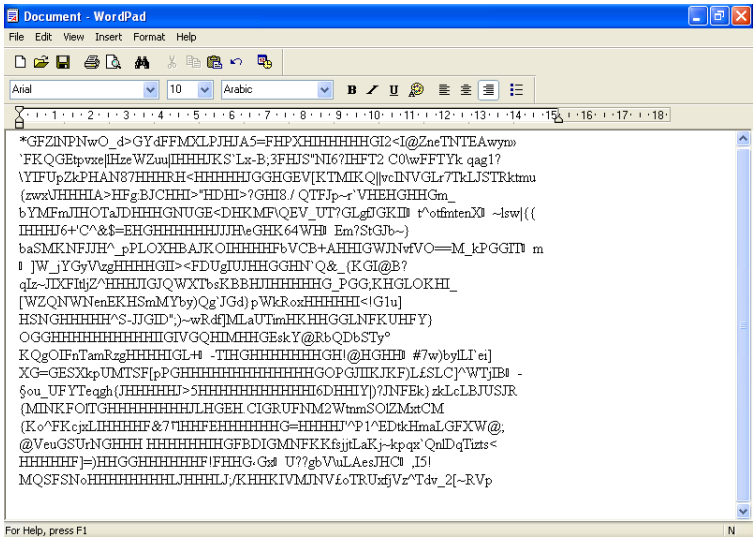
y ستحوي الأرقام المرمزة للرسالة بعد تطبيق المعادلات

الخطوة الرابعة: إستعادة الحروف حسب رموزها من الأرقام المسترجعة في الخطوة السابقة.

الخطوة الخامسة: ممكن إعادة دمج وتجميع ملف الفيديو بعد سحب البيانات منه.

5. النتائج Results

طبقت عملية الاخفاء على عدة نصوص باللغة الإنكليزية. حيث يتم إدخال النص إما يدويا، أو عن طريق نسخه من ملف خارجي ونقله إلى البرنامج. الشكل رقم (1) يبين نموذج يحتوي على نصوص إنكليزية عشوائية (حروف ورموز) تم إخفاءها داخل ملف فيديو.



شكل رقم (1): صورة تحتوي على نموذج من نصوص إنكليزية (حروف ورموز) تم إخفاءها داخل ملف فيديو

ولغرض قياس كفاءة الإخفاء، تم استخدام مقياس قمة نسبة الاشارة الى الضوضاء Peak Signal to Noise ratio (PSNR) والتي تقيس مدى دقة الاخفاء وعدم تمييز النص المخفي في الصورة بالعين البشرية. بالنسبة لاخفاء الصور فمقياس الدقة يتضمن حساب مربع الخطأ والمعرف بالمعادلتين التاليتين [9]:

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(f_{ij} - g_{ij})^2 \quad \dots (11)$$

$$PSNR\,in\,dB = 10\,Log_{10}\frac{L^2}{MSE} \quad \dots (12)$$

حيث:

MSE حساب مربع الخطأ

M,N هما الصف والعمود بالنسبة للصورة الغطاء

f_{ij} هي الوحدة الصورية من الصورة الغطاء قبل الاخفاء

g_{ij} هي الوحدة الصورية من الصورة بعد اخفاء النص داخلها

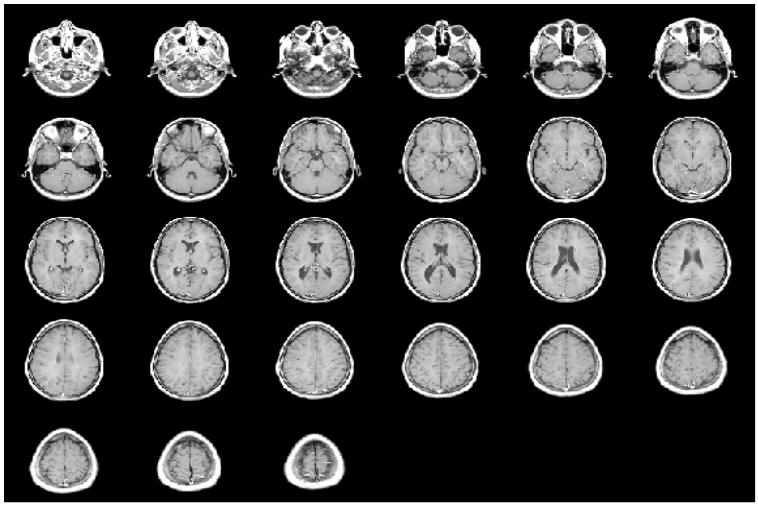
L هي مستوى قمة الاشارة وتساوي 255.

الجدول (1) يوضح قيمة PSNR بعد تطبيق عملية الاخفاء على صور ملف فيديو لعدة نصوص، ولقد رتبت النصوص تصاعديا حسب حجمها (حيث أن تسلسل كل نص يدل على مضاعفات حجم النص الأول).

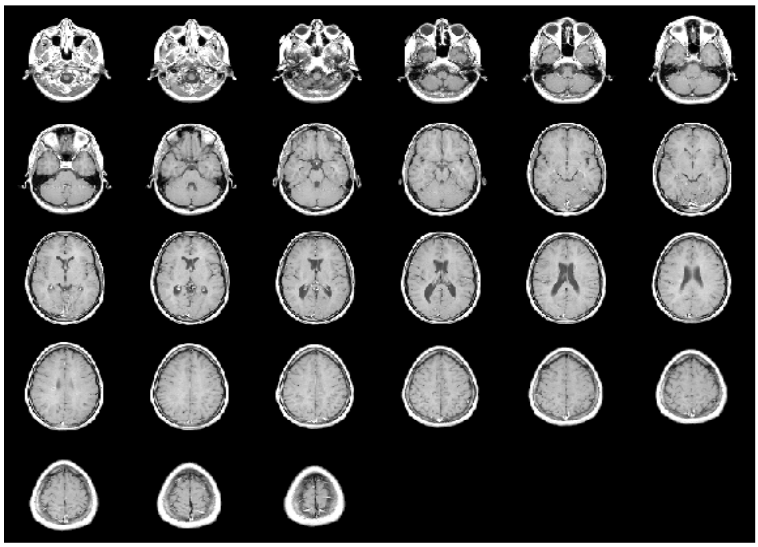
جدول 1: مقياس PSNR للوحة الألوان الرئيسية على ملف فيديو ولنصوص مختلفة

Text Order	Included pixels	PSNR in DB	Included Frames
1	16384	38.8993	1
2	32768	44.3313	2
3	49152	48.3594	3
4	65536	50.7761	4

الواضح من الجدول (1) انه بزيادة طول حجم النصوص المخفية تزداد قيمة PSNR زيادة قليلة وذلك بسبب زيادة عدد الـ Frames المستخدمة في الإخفاء بحسب طول النص المخفي (وهو من مضاعفات حجم النص الأول). أيضا لا يمكن لأي شخص تمييز وجود نص داخل صورة Frame الفيديو، والأشكال التالية (1 و 2) توضح 27 صورة ثابتة (Frame) يتكون منها ملف الفيديو (والذي يمثل حركة الرنين المغناطيسي لدماغ الإنسان) مرتبة أفقيا بحسب تسلسل عرضها قبل عملية إخفاء وبعده.

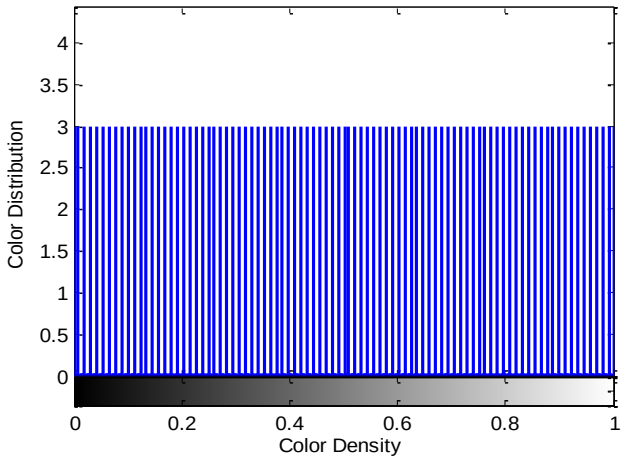


شكل رقم (1): صور ملف الفيديو قبل عملية الإخفاء

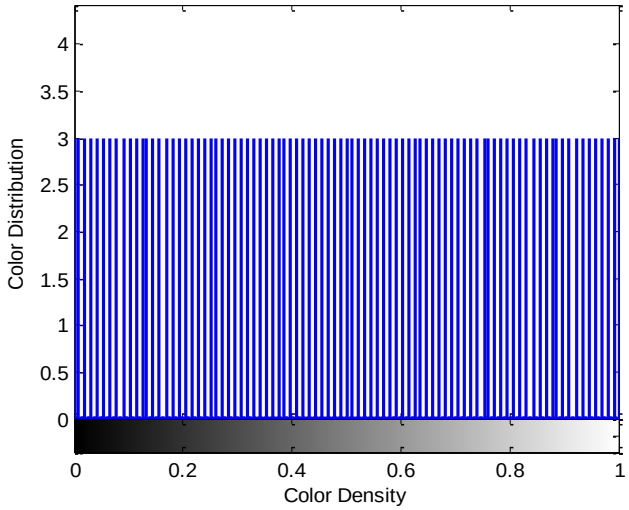


شكل رقم (2): صور ملف الفيديو بعد عملية الإخفاء

الشكلان السابقان أظهرا عدم وجود أي إختلاف ظاهر بالعين المجردة قبل إجراء عملية الإخفاء وبعدها. ولا يخفى أن حركة ملف الفيديو ستشكل عائقا أكبر لتمييز أي إختلاف – رغم عدم ظهوره – مما يعطي أمنية أكبر لنقل البيانات المخفية. الشكل (3 و 4) يبينان مخطط توزيع قيم البيانات (Histogram) للألوان الرئيسية في لوحة ألوان ملف الفيديو قبل وبعد عملية إخفاء النص الأخير عند عرضهما في برنامج Matlab.

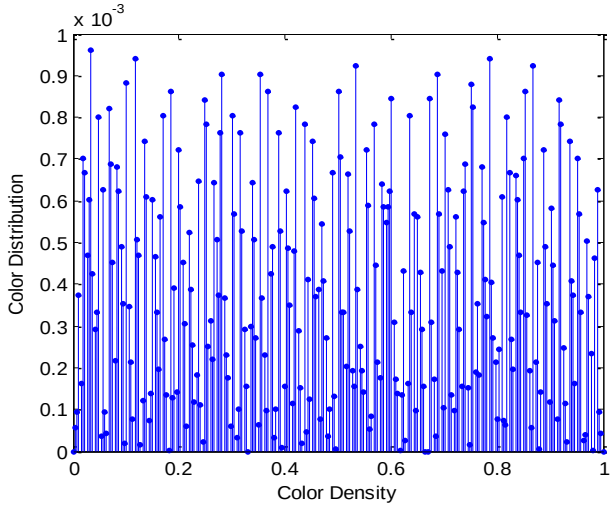


شكل رقم (3): مخطط توزيع قيم الألوان الرئيسية الثلاثة لملف الفيديو قبل عملية الإخفاء



شكل رقم (4): مخطط توزيع قيم الألوان الرئيسية الثلاثة لملف الفيديو بعد عملية الإخفاء

ويلاحظ من الشكلين السابقين أن الفرق غير واضح ومن الصعب جدا تمييزه على الرغم من وجوده، وهذا يدل على قوة الخوارزمية المستخدمة في الإخفاء والتي تمنع كشف حالة التغطية وتغير قيم البيانات حتى عند استعراض مخطط توزيع قيم الألوان (Histogram). بينما الشكل (5) يظهر أن هناك فعلا بيانات مخفية بداخل مخطط توزيع قيم البيانات – وهو فرق بسيط جدا – بعد طرح قيم لوحة الألوان الرئيسية قبل وبعد عملية الإخفاء.



شكل رقم (5): ظهور البيانات بشكل واضح في لوحة الألوان الرئيسية لملف الفيديو

يبين الشكل رقم (5) وجود بيانات مخزونة أو مخفية بداخل لوحة الألوان الرئيسية، حيث أن الفرق قد ظهر بعد الفارزة العشرية بأربعة مراتب. لهذا كان من الصعب جدا تمييزه في مخطط توزيع قيم الألوان لملف الفيديو.

6. الإستنتاجات Conclusions

قدم هذا البحث مسار جديد في الستيكانوكرافي حيث استخدم ملف فيديو كناقل لنص سري، وتم من خلال هذا البحث التوصل إلى الكثير من النتائج المفيدة:

- إستخدام الألوان الرئيسية الثلاث التي تشكل ألوان الصورة في عملية الإخفاء وفر مساحة خزنية أكبر من إستخدام تدرج لوني واحد فقط.
- يمكن الإستفادة من المساحة الخزنية الكبيرة التي يوفرها ملف الفيديو لإخفاء بيانات ذات حجم أكبر.
- حركة عرض ملف الفيديو ستشكل عائقا أكبر لتمييز أي إختلاف مما يعطي أمنية أكبر لنقل البيانات المخفية.
- مقياس دقة الإخفاء أثبت كفاءة الخوارزمية المستخدمة.
- مخططات توزيع قيم البيانات للألوان الرئيسية في لوحة ألوان ملف الفيديو أثبتت الصعوبة الشديدة في ظهور الفرق، حيث أن إخفاء البيانات قد تم في العمود الرابع بعد الفارزة العشرية.
- بالإمكان إجراء تغطية لبيانات تتكون من أرقام عشرية ولا يشترط تحويلها إلى بيانات رقمية.

المصادر

[1]. شهد عبدالرحمن، ايلاف اسامة، "تطبيق نظام التغطية على الصور الملونة من نوع (BMP)"، المؤتمر العلمي الأول لتقانة المعلومات، كلية علوم الحاسبات والرياضيات/جامعة الموصل، 23-22 كانون الأول 2008.

[2]. د .دجان بشير، د.أحمد سامي، ياسين حكمت، "الإخفاء في النص بأستخدام ميزة تكامل البيانات"، المؤتمر العلمي الأول لتقانة المعلومات، كلية علوم الحاسبات والرياضيات/جامعة الموصل23-22 كانون الأول 2008.

[3]. Aelphaeis M., "Steganography FAQ", Zone-H Unrestricted Information, © Copyright Zone-H.Org 2006.

[4]. Doërr, G. and J.L. Dugelay, A guide tour of video watermarking. Signal Processing: Image Commun., 18: 263-282. DOI: 10.1016/S0923-5965(02)00144-3, 2003.

[5]. Mohammed A., "Image Steganography by Mapping Pixels to Letters", Journal of Computer Science 5 (1): 33-38, 2009, ISSN 1549-3636.

[6]. R. Sridevi, Dr. A. Damodaram, Dr. Svl. Narasimham, "Efficient Method Of Audio Steganography By Modified Lsb Algorithm And Strong Encryption Key With Enhanced Security", Journal of Theoretical and Applied Information Technology, 2009.

[7]. Krzysztof S., Igor M., Wojciech M., "Steganographic Routing in Multi Agent System Environment", Journal of Information Assurance and Security 2 (2007) 235-243.

[8]. The MathWorks Inc., "Image Processing Toolbox For Use with MATLAB", Ver.7, 2004, MA, USA.

[9]. Qi, Hairong; Snyder, Wesley E. & Sander, William A., 2002; “Blind Consistency-Based Steganography for Information Hiding in Digital Media”. Multimedia and Expo, 2002. ICME '02. Proceedings. 2002 IEEE International Conference on Vol. 1, p.: 585- 588.