المجلة العراقية للعلوم الإحصائية

www.stats.mosuljournals.com

نهج جديد للبيانات المشفرة والمقيدة بطريقة EMD

غادة ذنون يونس و ابراهيم فتح الله و رؤى مهدي

قسم علوم الحاسبات ،كلية علوم الحاسبات والرياضيات ، جامعة الموصل ، الموصل ، العراق

معلومات النشر

تاريخ المقالة:
تم استلامه في 23 تموز 2019
تم القبول في 7 تشرين الاول 2019
متاح على الإنترنت في 1 حزيران 2020

الكلمات الدالة:
التشفير

المراسلة:
غادة ذنون يونس
ghadatalee@yahoo.com

الخلاصة

يهدف البحث الى اجراء عملية تشفير للنص المدخل باستخدام طريقة مقترحة للتشفير تسمى Merge Substitution Transposition MST بالاعتماد على جدول مقترح للحروف من اجل دمج طريقتي التعويض والابدال واستخدام طريقة ال Exploiting Modification Direction EMD التي تعتبر من الطرائق الحديثة واعتمدت كطريقة كفوءة من طرائق لاخفاء من اجل اخفاء النص المشفر المدخل للنظام وتضمين هذه البيانات داخل الصورة وارسالها الى جهة المستلم ثم يعمل النظام كجهة استقبال للصورة المرسلة من اجل فك التضمين والحصول على النص المشفر واجراء عملية فك التشفير والحصول على النص الاصلي.

تم العمل على نظام الالوان RGB Image وطبقت الخوارزمية المقترحة باستخدام لغة ماتلاب وحققت الخوارزمية المقترحة حيث كانت النتائج جيدة من خلال استخدام مقاييس الكفاءة المتمثلة بكل من (PSNR,MSE) على الصور الملونة وتم استرجاع النص بالكامل.

DOI: https://doi.org/10.33899/iqjoss.2020.165443 ,

1. المقدمة Introduction

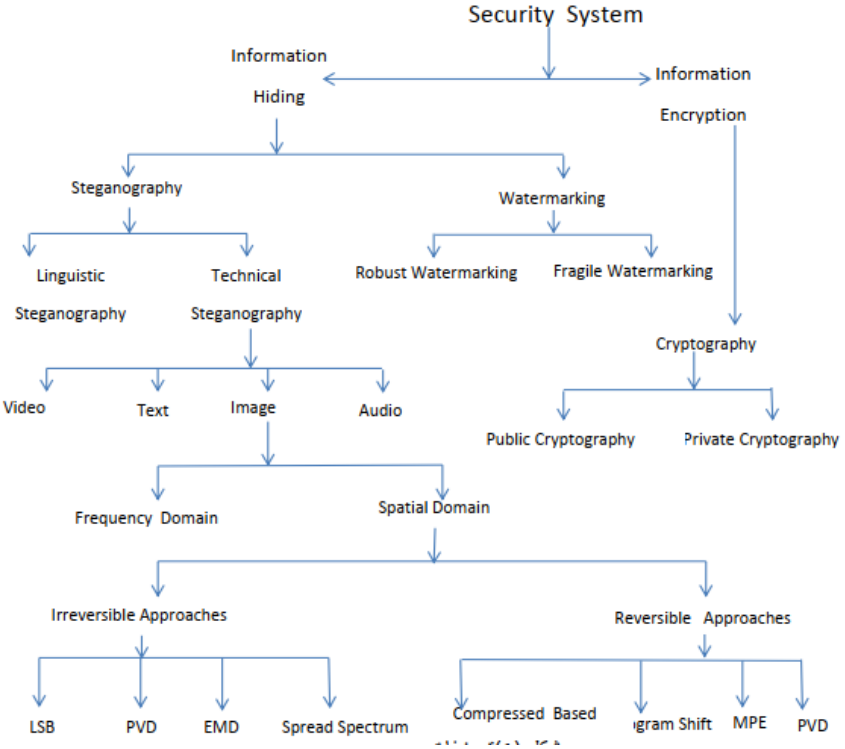
أصبحت عمليه تناقل البيانات عبر الإنترنيت عمليه سهلة نتيجة التطور الكبير في تقنيات الشبكات ،وبات بإمكان الكثيرين الاتصال مع بعضهم البعض بسهوله وسرعه. إلا أن استخدام الانترنيت للاتصال ترافقه مشكلتان : إحداهما توفير الأمنية (security) والأخرى توفير عرض الحزمة (bandwidth) ولان الانترنيت بيئة عامه ومفتوحة فبإمكان أي شخص غير مخول مراقبه معلومات متناقلة بين أي طرفين واعتراضها أو الحصول عليها. هناك تقنيتان لتوفير الأمنية للمعلومات المتناقلة والحفاظ على سريتها: أولهما التشفير(Encryption). ثانيهما الكتابة المغطاة (steganography) إذ يهدف التشفير إلى أعاده صياغة البيانات السرية بواسطة مفتاح التشفير بحيث تبدو غير مفهومه وبلا معنى ولا يمكن إرجاعها إلى أصلها ألا من قبل مالك مفتاح التشفير، لكن هيئه البيانات المشفرة غير المفهومة لا تخفي حقيقة وجود اتصال سري بين طرفين مما يدفع الشخص غير المخول إلى اعتراض تلك البيانات أو فك تشفيرها أو تحطيمها علاوة على ذلك، فأن كثيرا من الحكومات وضعت قوانين تحد من استخدم طرائق التشفير أو منعها بصوره عامه لذا توجهت أنظار الكثيرين نحو استخدام التقنية الثانية (الكتابة المغطاة) للحفاظ على أمنية المعلومات المتبادلة بين طرفين. إذ أنها تقنية تضمين بيانات سرية داخل بيانات أخرى بصورة لا يمكن كشفها بسهولة مما يخفي حقيقة وجود بيانات متناقلة.[1]

2. تقنيه أمنيه المعلومات (Data Security Technique)

يعتبر علم الاختزال من العلوم المهمة في مجال الأمنية و أخفاء المعلومات، وهو يختلف عن التشفير لكنه مكمل له، لان إخفاء البيانات باستخدام طرائق فن الاختزال يقلل من فرصة اكتشاف البيانات المخفية على المخربين، ربما تكون هذه الفرصة معدومة لأنها أعطت طبقة أخرى لحماية البيانات من خلال وضع البيانات المراد إخفاؤها داخل أي غطاء أخر من البيانات (نص، صور، صوت، صوره متحركة)، وبعد إخفاء البيانات داخل الغطاء ينتج غطاء جديد يحتوي على البيانات السرية، ولا يكون مدركا بالعين المجردة لضمان تنقله داخل الشبكة وغير قابل لاستخراج البيانات السرية في حال تم اكتشافه من قبل المخربين .[2].

3. خوارزميات النظام

تلعب تقنيات الشبكة الحديثة دورا مهما في نقل البيانات الرقمية بسرعة مثل الصور والتسجيلات الصوتية والنصوص والمقاطع الفيديو ومع هذا يمكن للمستخدمين غير المصرح لهم الدخول بسهولة والعبث بالبيانات بسبب الطبيعة العامة للشبكة والتقدم الحاصل في ادوات التزوير لذا اصبح آمن البيانات اثناء الارسال والاستقبال اولويه مهمه .[3][4] يوفر نظام الأمنية (Security System) طرائقا عديدة لحماية البيانات المتراسلة عبر الشبكة ، ويمكن بيان نظام الاخفاء (Security System) حسب ما موضح بالشكل(1):-



شكل (1)تصنيفات نظام الاخفاء

ويصنف نظام الاخفاء الى صنفين وهي العلامة المائية (watermarking) وفن الاخفاء (steganography) .

تستخدم العلامة المائية لحماية حقوق الطبع والتأليف وتضمن سلامه البيانات المنقولة وتكون مناسبه للبيانات ذات الاحجام الصغيرة وتوفر قوة ومتانه مقارنه مع نظام الاخفاء (steganography) الذي يستخدم غطاء كبير للبيانات المطلوب اخفاءها مثل الصور والصوت والفيديو. بشكل عام يتم تقييم كفاءة الطرائق المستخدمة بالإخفاء في الصور الرقمية من خلال ثلاث محددات رئيسيه وهي:

1-السعه (اقصر حمولة يمكن تضمينها في صور الغلاف)

2-التناظر(ان تكون الصور الأصلية قريبه من صور الغلاف)

3-الامان (ان تكون صوره الاخفاء مقاومه للهجمات)

لذا نلاحظ ان عمليه تحقيق السعه العالية و التناظر البصري الجيد والامان في ان واحد يعد مشكله بحثيه صعبه . [3][5]

وهناك العديد من اساليب الاخفاء في الصور الرقمية التي قسمت الى قسمين رئيسيين هما

1-الحيز المكاني spatial Domain

2-الحيز الترددي frequency Domain

في الحيز المكاني يتم اخفاء البيانات مباشرة بعد تغيير قيم نقاط الصورة كذلك يحتاج الى عمليات حسابية اقل مقارنه مع الحيز الترددي الذي يعتبر اقل قوة ضد الهجمات ولكن نسبه المعلومات المضمنة فيه تكون اقل ومكلف حسابيا .[4][3]

ويقسم الحيز المكاني الى قسمين رئيسيين:

1- مناهج غير عكسية Irreversible Approaches

2- مناهج عكسية Reversible approaches

تقوم أساليب الكتابة المخفية القابلة للانعكاس بأعادة بناء الصورة الاصلية بعد استخراج الرسالة السريه منها بينما تقدم اساليب الكتابة المخفية غير قابله للانعكاس حمولة عالية بالتضمين وتناظر بصري جيد واسترجاع الرسالة السرية دون ايلاء اهتمام باستعادة الصور الاصلية[3]

وتقسم اساليب الكتابه المخفيه غير قابله للانعكاس الى :

1-LSB(least Significant Bit)
2-PVD(Pixel Value Difference)
3-EMD(Exploiting Modification Direction)
4-Spread Spectrum.[2][3]

4. EMD(Exploiting Modification Direction) :-

تم اقتراح طريقة الEMD من قبل (Zhaug and Wang) في عام (2006) وذلك لغرض التقليل من التغيير الحاصل في الصورة خلال عملية تضمين المعلومات بداخلها. هذه الطريقة تعمل على تقسيم الصورة الى مجاميع متساوية كل مجموعة تحوي على n من البيكسل وذلك لغرض تضمين الأرقام السرية بنظام الترميز ary (2n+1) خلال عملية التضمين سيتم اضافة او طرح (1) من قيمة ألبكسل التي سيتم اختيارها داخل المجموعة. في عام(2007) قدم(Lee) واخرون طريقة جديدة لتحسين طريقة ال EMD اطلق عليها(IEMD) هذه الطريقة حققت نسبه تضمين اكبر بالمقارنة مع الطريقة الاصلية ومن دون التأثير على جوده الصورة التي تحمل الرسالة او التأثير على السرية. في هذه الطريقة الرسالة السرية سيتم تحويلها الى ارقام سريه بنظام ترميز (ary-8) وكل رقم سري يطمر في المجموعة المكونة من البكسل، في هذه الطريقة تم اخفاء كمية كبيرة من البيانات ولكن كانت جودة الصورة اقل من طريقه EMD الاصلية.[6]

تم اقتراح طريقة الـ (opt EMD) من قبل (K.lin) واخرون في عام 2010 حيث وجدوا العلاقة ما بين عدد البكسل (n) في المجموعة وكمية البيانات التي سيتم تضمينها داخل الصورة وذلك لتحسين طريقة الـ (EMD) في اخفاء البيانات، وفي عام 2013 قدم (Kuo) واخرون طريقة جديدة لتحسين خوارزمية الـ EMD وذلك من خلال إخفاء (n+1) بت من الرسالة السرية في n من البكسل في الصورة.[6]

5. خوارزميه الـEMD

تستخدم خوارزميه الـ(EMD) نظام الترميز (2n+1) والتعامل مع صورة رمادية وحسب الخوارزمية التالية:

1. تحديد الصورة كمجموعة من النقاط (group) التي تمثل قيمة (n) اما الرقم السري الذي سيتم تضمينه فيعبر عنه بالرمز"d"، المعادلة رقم (1) تستخدم لغرض حساب قيمه داله الاسترجاع التي يرمز لها بالرمز (f) لكل بكسل داخل المجموعة

$$F=F(g1,g2,g3,.....gn)=[\sum_{i=1}^{n}(g_i * i)\bmod(2n+1)] \quad (1)$$

حيث ان :-

$(g_1,g_2,g_3,.....g_n)$ تمثل قيم النقاط داخل المجموعة .

(n) تمثل عدد البيكسل داخل المجموعة .

2. يتم حساب قيمه f ومقارنتها مع الرقم السري "d" ، اذا كان (d=f) فلا يتم تغيير قيم البيكسل وذلك لان قيمة الرقم السري سيكون مساوي لقيمه داله الاسترجاع. اما في حاله "d" لا تساوي f يتم حساب مؤشر الصورة التي تمثل الفرق ما بين قيمتين (f, d) باستخدام المعادلة (2) :-

$$S=d-f \bmod(2n+1) \quad (2)$$

يتم مقارنة قيمة s :-

اذا كانت قيمه s<=n فان $g_s=g_s+1$

اما اذا كانت القيمة s>n فان $g_{2n+1-s}=g_{2n+1-s}-1$

وتطبق هذه الخطوات حتى نهاية الارقام السرية المراد اخفاءها.

3. عمليه استرجاع الرسالة السرية من الصورة فتكون عبارة من مجموعة من الخطوات بالبدء سيتم تقسيم الصورة الى مجموعه من البيكسل وكل مجموعه متكونه من (n) من النقاط اما المعادلة المستخدمة لاسترجاع الرسالة السرية فتكون بالشكل الاتي:-

$$F=F(g_1,g_2,g_3,\ldots\ldots g_n)=[\sum_{i=1}^{n}(g_i * i)\bmod(2n+1)] \quad (1)$$

الارقام السرية المستخدمة من المجاميع سيتم تحويلها الى ارقام بالنظام الثنائي لتكوين سلسله من البتات واسترجاع الرسالة السرية .[6]

6. **الدمج بين طريقتي الابدال والتعويض** (Merge Substation Transform)

يتم استخدام طريقة الدمج (MST) وذلك لتشفير النص واعطاء درجة امنية عالية للبيانات التي سيتم اخفاؤها فيما بعد تبدا العملية بإدخال النص المراد تشفيره وليكن كمثال :

TAKE ME TO YOUR LEADER

حيث سيتم الاعتماد على جدول لأجراء عملية التشفير :-

جدول (1) المعتمد في التشفير وفك التشفير

	A	B	c	D	E
A	A	B	C	D	e
B	F	G	H	I	J
C	K	L	M	N	O
D	P	Q/Z	R	S	T
E	U	V	W	X	Y

نأخذ الحرف الاول من النص T ومقارنته مع القيمة المحددة بالجدول ويعوض عنه بالقيمة DE و اخذ الحرف الثاني A ومقارنته بالقيمة من الجدول ويعوض عنه بالقيمة AA وهكذا

سينتج لدينا النص التالي :

DE AA CA AE CC AE DE CE EE CE EA DC CB AE AA AD AE DC

يتم الان تقسيم النص الى جزئيين :

الجزء الاول DE AA CA AE CC AE DE CE EE

الجزء الثاني CE EA DC CB AE AA AD AE DC

بعدها يتم القيام بأخذ الحرف الاول من الجزء الاول مع الحرف الاول من الجزء الثاني وهكذا حتى نحصل على الناتج الاتي :

DC EE AE AA CD AC AC EB CACE AA EA DA ED CA EE ED EC

يتم الرجوع الى الجدول (1) مرة ثانية للتعويض عن قيمة كل حرفين لينتج النص الاتي:

RYEANCCVKOAUPXKYXW

الناتج يمثل النص المشفر وهو المرحلة الاولى من التشفير وتكون جاهزة للإخفاء داخل الصورة.

7. فك التشفير

بعد ان تم القيام بإخفاء النص داخل الصورة تبدء عملية فك تشفيره وذلك باستخدام الخطوات التالية:-

اولا :- البدء بأخذ الحرف الاول من النص R وتعويضه عن القيمة المحددة بالجدول (1) سينتج لدينا القيمة DC واخذ الحرف الثاني Y وتعويضه عن القيمة المحددة في الجدول سينتج لدينا القيمة EE وهكذا.

سينتج لدينا النص الاتي :

DC EE AE AA CD AC AC EB CA CE AA EA DA ED CA EE ED EC

ثانيا :- يتم القيام بتقسيم النص المشفر الى جزئين جزء مواقع فردية وجزء مواقع زوجية حسب تسلسل الحرف لينتج لدينا النص الاتي :

الجزء الاول DE AA CA AE CC AE DE CE EE

الجزء الثاني CE EA DC CB AE AA AD AE DC

ثالثا:- يتم العمل على دمج الجزئيين مع بعضهم البعض ويكون ترتيب النص بالشكل الاتي :

DE AA CA AE CC AE DE CE EE CE EA DC CB AE AA AD AE DC

الرجوع الى الجدول (1) للتعويض عن قيمة كل حرفين لينتج لدينا النص الاصلي

TAKE ME TO YOUR LEADER

8. الخطوات المتبعة ضمن النظام :

1. قراءة ملف صوري من نوع RGB

```
[a b] = uigetfile('*.jpg', 'pick an M-file');
q=imread([b a]);
```

شكل (2) :الصورة الاصلية cover

2. ادخال النص المراد اخفاءه .

```
text="ibrahem and ruaa.hghg";
```

3.استلام النص .

```
text2 =ibrahem and ruaa
```

4. تكوين الجدول المعتمد علية في عملية التشفير وقد تم اضافة سطر وعمود للجدول لكي يكون اكثر مرونة واعطاء امكانية استخدام الرموز التي يمكن ان يتم استخدامها بالنص .

5.تحديد طول النص المدخل ويتم اخذ الحرف الاول من النص الذي هو حرف الـ "i"وتعويضه بالجدول من كل سطر وعامود ينتج لدينا حرفين bd وتستمر العملية لجميع حروف النص المدخل.

جدول (2) : المحدث والمعتمد في التشفير وفك التشفير

	A	B	C	D	E	F
A	A	B	C	D	E	1
B	F	G	H	I	J	2
C	K	L	M	N	O	3

bdabdcaabcaeccdfaacdaddfdceaaaaa= partafter

6. يتم تقسيم النص الى جزئين بالتسلسل بشكل متساوي

bdabdcaabcaeccdf= partone

aacdaddfdceaaaaa= parttwo

7. يتم دمج الجزئيين بأخذ الحرف الاول من الجزء الاول مع الحرف الاول من الجزء ثاني وحتى نهاية الجزئيين.

badaacbddacdadafbdccaeeacacadafa

8. نأخذ كل حرفين ونعوضهم بالجدول لينتج حرف واحد عن كل حرفين والذي سيمثل النص المشفر ، وبالتالي يكون جاهز لعملية الاخفاء.

fpcipnd1imeukkp5= textencrapion

9. بعد اجراء عملية التشفير واختيار الصورة المراد الاخفاء فيها ،يتم تحديد عدد النقاط الكلي الصورة، حسب عدد الحروف المشفرة (uu) وحسب معادلة الاتية .

```
nopos=3*uu*n;
```

10. تحويل كل حرف بالنص المشفر الى نظام ثنائي من 8 بت وتقسيمه الى ثلاثة اجزاء وتحويل كل جزء الى نظام العشري حيث ان لكل جزء سيحتاج الى مجموعة واحدة من النقاط وحسب قيمة d!=f لكي تتم عملية الاخفاء.

d1= 011 010 01

3 2 1=d

11. حساب قيمة دالة الاسترجاع والذي يرمز لها بf من اجل اخفاء الجز الاول من الحرف حسب معادلة التالية

$F=F(g_1,g_2,g_3,\ldots\ldots g_n)=[\sum_{i=1}^{n}(g_i * i)\bmod(2n+1)]$

12. بعد حساب قيمة f يتم مقارنتها مع قيمه d .

```
d(xx)==f
```

فاذ كانت القيم متساوية فلا حاجه لتغيير قيم النقاط داخل المجموعة واما اذ كان هناك فرق فيتم حساب قيمه معامل القياسs وحسب المعادلة :-

$S=d-f \bmod(2n+1)$

13.اجراء عملية المقارنة بين [n,s] فاذ كان s اكبر من n يتم تطبيق المعادلة الاتية ونقصان قيمه البكسل المحدد بمقدار واحد.

$g_{2n+1-s}=g_{2n+1-s}-1$

واما اذ كان قيمه s اقل من n يتم حساب معادلة التالية وزيادة قيمة البكسل المحدد بمقدار واحد.

$g_s=g_s+1$

14. تستمر عمليه الاخفاء حتى نهاية النص المشفر في الصورة ينتج صورة التالية .

شكل (3):الصورة الغطاء -stego

15. حفظ الصورة .

```
imwrite( res,'C:\Users\3D\Documents\MATLAB\ibb.jpg')
```

9. الخطوات المتبعة في عملية الاسترجاع :

1. استلام الصورة ليتم قراءتها عند المستلم.

```
[u y] = uigetfile('*.jpg', 'pick an M-file');
qwe=imread([y u])
```

شكل (4):الصورة المستلمة

2. اجراء عملية فك الاخفاء بعد تحديد عدد النقاط التي تم الاخفاء بدخلها و تحديد قيمة n.

3. حساب داله الاسترجاع التي يرمز ها بالرمزر F من اجل استرجاع النص وذلك بتطبيق المعادلة على كل مجموعة من النقاط لاسترجاع جزء من الحرف وتستمر حتى استرجاع ثلاثة اجزاء والتي ستمثل الحرف الاول الذي تم اخفاءه.

$F=F(g_1,g_2,g_3,\ldots\ldots g_n)=[\sum_{i=1}^{n}(g_i * i)\bmod(2n+1)]$

3 2 1= text

4. تجميع كل ثلاثة ارقام عشرية وتحويل الى نظام الثنائي من 8 بت وبعدها تحويل نظام ثنائي الى حرف يمثل النص المشفر .
01101001= ans

5. تستمر العملية لحين ارجاع النص المشفر الذي تم اخفاءه داخل الصورة.

fpcipnd1imeukkp5= o

6. اخذ النص المشفر ناتج من عملية فك الاخفاء وتعويض عن كل حرف بقيمته المحدده بالجدول.

badaacbddacdadafbdccaeeacacadafa=Faktshfer

7. نقسم النص الناتج الى جزئين حسب المواقع الفردية والزوجية.

bdabdcaabcaeccdf= part4

part5 =aacdaddfdceaaaaa

8. دمج جزئي النص الى نص كامل .
bdabdcaabcaeccdfaacdaddfdceaaaaa= part4part5

9. تعويض عن كل حرفين بالجدول لينتج لدينا النص الاصلي.

ibrahem and ruaa= plantext

10. مقاييس الكفاءة :

تم اقتباس مقياس الكفاءة من مجالات معالجة الإشارات الرقمية و نظرية المعلومات حيث تم اعتماد الأسئلة التي يمكن أن تستخدم لأجل التمكن من قياس كميات الخطأ في الصورة المعاد تكوينها ويمكن تعريفها بان مستوى المعلومات المفقودة ومن الممكن أن يعبر عنه كدالة من الصورة الأصلية –المدخلة والصورة المسترجعة وتسمى بمقاييس المصداقية وبالرغم من انه استخدم بشكل واسع ، إلا انه ليس بالضرورة ارتباطه مع الإدراك (أو التمييز) لنوعية الصورة. فهنالك كثير من القياسات التي تعتمد على حساب مقدار التباين بين نسخ مختلفة لنفس الصورة ومن هذه المقاييس:

اولاً :نسبة الضوضاء بالصورة **(PSNR) :**

$$\mathbf{PSNR = 10LOG_{10}\left(\frac{R^2}{MSE}\right)} \qquad (3)$$

حيث ان:
R: تمثل عدد المستويات لتدرج الالوان
ثانياً : نسبة مربع الخطأ بالصورة **(MSE) :**

$$MSE = \sum [I_1(m,n) - I_2(m,n)]^2/(m*n) \qquad (4)$$

حيث ان:

I1(m,n): تمثل الصورة الاصلية قبل الاخفاء

I2(m,n): تمثل الصورة الغطاء.

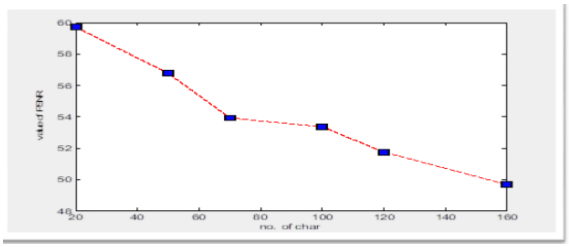
11. مناقشة النتائج :

تم تطبيق الخوارزمية المقترحة في هذا البحث وحساب مقاييس الكفاءة لعدد غير محدد من البيانات المدخلة من اجل بيان كفاءة الخوارزمية المقترحة والجدول (3) يوضح ذلك:

جدول(3):يوضح مقاييس الكفاءة لعدد غير محدد من الحروف لصورة معينة

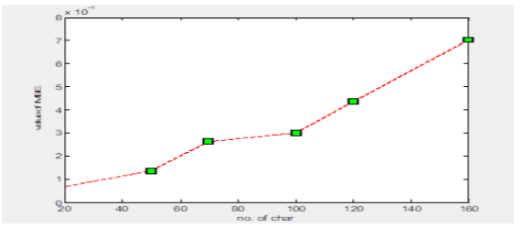
selected picture	No. of char	MSE	PSNR
	20 char	6.98332e-005	59.6902
	50 char	1.3750e-004	56.7479
	70 char	2.6374e-004	53.9191
	100 char	3.0114e-004	53.3431
	120 char	4.3623e-004	51.7336
	160 char	7.0408e-004	49.6564

نلاحظ من الجدول(3) ان قيمة معامل الضوضاء تقل كلما زادت كمية البيانات المدخلة وتزداد كلما قلت كمية البيانات الداخلة وقد كانت قيم معامل الضوضاء جيدة على الرغم من زيادة كمية البيانات الداخلة على النظام الا انه لم يوثر كثيرا على الصورة الغطاء التي هي اقرب للصورة الاصلية وقد تم رسم مخطط يبين العلاقة بين قيمة معامل الضوضاء (PSNR) وكمية البيانات المدخلة وكما موضح بالشكل (5).



شكل(5) يوضح العلاقة بين عدد الاحرف ومعامل الضوضاء PSNR

اما بالنسبة لمعامل الخطأ (MSE) فانه يزداد كلما زادت كمية البيانات المدخلة ويقل كلما قلت كمية البيانات المدخلة وعلى الرغم من زيادة كمية البيانات المدخلة في الصورة الا ان معامل نسبة الخطأ كان قليلا مقارنة مع كمية البيانات الداخلة مما يثبت كفاءة الخوارزمية المقترحة وان نسبة الخطأ بالصورة الغطاء قليلة وهذا يعني ان الصورة الغطاء هي اقرب للصورة الاصلية والشكل (6) يوضح العلاقة بين معامل نسبة الخطأ وكمية البيانات المدخلة.



شكل (6) يوضح العلاقة بين معامل نسبة الخطأ وكمية البيانات المدخلة

12. الاستنتاجات

بعد تطبيق الخوارزمية المقترحة على حالات متعددة من البيانات وعلى صور مختلفة تم التوصل الى ما يلي : استخدام طريقة ال MST كطريقة مقترحة بالتشفير اعطت امنية وكفاءة عالية للخوارزمية نظراً للمراحل المتعددة التي يمر بيها النص حتى نصل الى مرحلة تشفير النص النهائية . عملية اضافة السطر والعمود للجدول المقترح بطريقة ال MST اعطى مرونة بالنص الذي تم تشفيره والقضاء على حالات الضعف التي كانت موجودة بالجدول السابق. استخدام طريقة ال EMD في اخفاء البيانات المشفرة، اي نقاط الصورة التي يتم فيها طمر البيانات ستكون اقل عرضة للتشوه وذلك لان مقدار التغير الذي يحصل لنقاط الصورة سيكون اما بإضافة او نقصان واحد او تبقى القيمة كما هي وحسب حالات المستخدمة بالتضمين. دمج طريقة التشفير والاخفاء اعطى للخوارزمية المقترحة كفاءة وامنية عالية. بعد تطبيق الخوارزمية المقترحة تم استرجاع الملف النصي كاملاً وكانت نسبة التطابق 100%.

13. التوصيات

من اجل الاستفادة من النتائج التي تم الحصول عليها من الخوارزمية بالإمكان اتباع ما يلي:

1- من الممكن استخدام ملفات فيديوية كغطاء بدل من الصورة.
2- عملية اختيار المجاميع المستخدمة بطريقة ال EMD تكون بشكل عشوائي او حسب معادلات معينة وليس بشكل متسلسل.
3- من الممكن استخدام هذه الخوارزمية على ملفات الصوت والصورة بدلا من النص.

13. المصادر:-

1- Anasam A. Abdul Majeed, (2011), "A new way of writing covered in vector images of directional quantification", Master Thesis, Faculty of Computer Science, Mathematics, Computer Science Department, Mosul University.
2- Shahid Abdulrahman, Ilaf Osama, (2008), "Implementation of BMP color image coverage system", 1st Scientific Conference on Information Technology, University of Mosul, Iraq.
3- Mehdi Hussain, Ainuddin Wahid Abdul Wahab ,Noman Javed, Ki-Hyun Jung ,(2016), "Hybrid Data Hiding Scheme Using Right-Most Digit Replacement and Adaptive Least Significant Bit for Digital Images",Symmetry,MDPI.
4- Irfan Khan, Sudesh Gupta, Shivendra Singh ,**(2016),** "A New Data Hiding Approach in Images for Secret Data Communication with Steganography ",International journal of computer applications, vol135,No.13.
5- Ali Abdel-Baki Amin, (2001), "Encrypting Files Using Programming Techniques", Master Thesis, Faculty of Computer Science, Mathematics, Computer Science Department, Mosul University.
6- Ziad Safa Younis Safawi, (2016), "The concealment of information in images using EMD technique" (Al-Qadisiya Journal of Computer Science and Mathematics, vol. 8, no. 1).

New Approach for Data encrypted and hinding gy EMD method

Ghada Th. Younis , Ibraheem F. Alla, Ruaa Mahde

Department of Computer science, College of Computer science and Mathematics, University of Mosul, Mosul, Iraq

Abstract

The research aims to conduct an encryption process for the entered text using a proposed method of encryption called Merge Substitution Transposition MST based on a suggested table of letters in order to combine the two methods of compensation and substitution and using the method of Exploiting Modification Direction EMD which is considered one of the modern methods and adopted as an efficient method of masking methods in order to hide the text The encoder entered into the system and includes this data inside the image and sends it to the recipient, then the system acts as a receiver for the transmitted image in order to decode the embedding and get the cipher text and perform the decoding process and get the original text.

The RGB Image color system was worked on, and the proposed algorithm was applied using the MATLAB language, and the proposed algorithm was achieved, as the results were good by using efficiency measures represented by (PSNR, MSE) on color images, and the entire text was retrieved.

Keyword: encryption.