Encrypt and Hide Data in True Color Image Classes

Maha A. Hasso **Shahad A. Hasso** **Ban Ghanem Maayouf**
College of Computer Science and Mathematics
University of Mosul, Mosul, Iraq

Received on: 12/02/2012 **Accepted on: 19/04/2012**

ABSTRACT

In a world that has evolved in which the information and means of transmission within the network of the whole world not to be a convenient way to keep that information to have some privacy or confidentiality had to be hide from some people who may resort to playing with them or use them brings harm to himself and to others and make them exclusive to the needed, and that was the motivation for the selection of research topic, it is aimed primarily to find a new technique to protect data.

In this research the application of triple data encryption standard (3DES) to encrypt a given text using multiple keys then hide the encrypted text in a true color image, after selecting their own identity by k-means algorithm for classification and a number of varieties.

Data has been hidden as bytes by putting it in the image (depending on the classification) and results showed high accuracy in the hiding did not appear to the human eye is no evidence on the existence of hidden data in the image in each color of the components of the (24 bit), any image that the unit used for the image store 3 bytes of the encrypted text so it is possible using the proposed algorithm to hide the size of any text, without the appearance of any effect on the resulting image.

The results showed that the size of the cover image after hiding the encrypted text is the same as it is before the process of hiding, and also found the application to increase or decrease the number of items does not represent a major factor in hiding, but whenever the size of the image is greater (Dimensions), the greater the proportion of hiding. Visual C # language have been used to implement the proposed method.

Keywords: Encryption, True Color Image.

تشفير البيانات وإخفائها في اصناف الصور حقيقية الالوان

مهى عبد الرحمن حسّو **شهد عبد الرحمن حسّو** **بان غانم معيوف**
كلية علوم الحاسوب والرياضيات
جامعة الموصل، الموصل، العراق

تاريخ استلام البحث: 2012/02/12 **تاريخ قبول البحث: 2012/04/19**

الملخص

في عالم تطورت فيه المعلومات ووسائل انتقالها ضمن شبكة تضم العالم بأسره لا بد من وجود طريقة مناسبة للحفاظ على تلك المعلومات لما يتمتع البعض منها بخصوصية او سرية توجب حجبها عن البعض الذي قد يلجأ الى العبث بها او استخدامها بشكل يجلب الضرر لنفسه وللآخرين وجعلها مقصورة على من يحتاجها ، فكان ذلك دافعا لاختيار موضوع البحث ، فهو يهدف بالدرجة الاولى الى ايجاد تقنية جديدة لحماية المعلومات.

تم في هذا البحث تطبيق خوارزمية تشفير البيانات القياسية الثلاثية (Triple Data Encryption Standard 3DES) لتشفير نص معين باستخدام عدة مفاتيح ثم إخفاء النص في اصناف صورة حقيقية الالوان (24بت) بعد تحديد اصنافها عن طريق خوارزمية k-means للتصنيف وبعدد من الاصناف.

تم اخفاء البيانات بوضعها بايتا كاملا عن طريق بعثرتها في الصورة (تبعا للتصنيف) واظهرت النتائج دقة عالية في الاخفاء ولم يظهر للعين البشرية أي دليل على وجود بيانات مخفية داخل الصورة وفي كل لون من مكونات ال(24 بت) أي ان الوحدة الصورية للصورة المستخدمة تخزن 3 بايت من النص المشفر لذا من الممكن باستخدام الخوارزمية المقترحة اخفاء أي حجم من النص وبدون ظهور أي تأثير على الصورة الناتجة.

وقد تبين من النتائج بان حجم الصورة الغطاء بعد اخفاء النص هو نفس حجمها قبل عملية الإخفاء وكذلك تبين من التطبيق ان زيادة او نقصان عدد الاصناف لا يمثل عاملا اساسيا في الاخفاء ولكن كلما كان حجم الصورة اكبر (ابعاد الصورة) زادت نسبة الاخفاء. تم تطبيق الخوارزمية المقترحة باستخدام لغة Visual C#.

الكلمات المفتاحية: التشفير، صورة حقيقية الألوان.

1. المقدمة

التشفير وإخفاء المعلومات هي تقنيات شائعة وواسعة الاستخدام لمعالجة المعلومات (رسائل) من أجل تشفيرها وإخفاء وجودها. هذه التقنيات لها تطبيقات واسعة جدا في مجال الحاسوب والمجالات الأخرى ذات الصلة لأنها تستخدم لحماية رسائل البريد الإلكتروني ومعلومات بطاقة الائتمان وأمنية بيانات الشركات والخ....**[1]**.

الاخفاء بحد ذاته فن وعلم للتواصل بطريقة تخفي وجود اتصال وبطريقة تضمن ارسال المعلومات عبر وسائل الاتصالات ويضمن بالتالي ارسال محتوى الرسائل عبر وسائل الاعلام في تغطية حتى لا تلفت الانتباه او تثير شك المتصنت غير المخول، مثال ذلك من الممكن تضمين نص داخل صورة او ملف صوتي **[2]**.

من ناحية أخرى ، التشفير هو دراسة التقنيات الرياضية المتعلقة بأمنية المعلومات لضمان سلامة البيانات السرية، فالتشفير يحمي المعلومات عن طريق تحويلها الى رموز وشفرات تكون غير مفهومة للمتصنت حتى ولو استطاع سرقتها اذ انها تظهر له بشكل غير قابل للقراءة.

تصنف نظم التشفير الى انواع حسب عدد مفاتيح التشفير المستخدمة ومدى سريتها، حيث هناك خوارزميات تشفير تعتمد على مفتاح واحد بين المرسل والمستلم ويكون سرياً (Symmetric key). واخرى تعتمد على مفتاحين الاول عام والثاني سري (asymmetric key) **[3]**.

لإخفاء المعلومات أهمية كبيرة وذلك لأن عدم ظهور المعلومات سواء مشفرة أو غير مشفرة للعيان عامل مساعد على إضفاء حمايةً وأمناً على المعلومات. يستخدم الاخفاء في العديد من المجالات، وخاصة في التجارة الإلكترونية التي تزداد تطبيقاتها، والاهتمام بها يومًا بعد آخر. وعلى افتراض أن المستخدم يتوقع وجود نص ما مخفي، فسيظهر أمامه تحدٍ آخر، وهو معرفة الطريقة المستخدمة في الإخفاء و كلمة السر ومفتاح التشفير، وكل من هذه الأشياء قد يستغرق اكتشافه وقتاً زمنياً طويلاً [4] [5].

عُني الإنسان منذ القدم بتصنيف المعرفة، وبذل الفلاسفة والمفكرون جهوداً لوضع نظم لهذا التصنيف، فالتصنيف في اللغة هو تمييز الأشياء بعضها عن بعض وهو أيضاً ترتيب الأشياء في أصناف أو أقسام، وإذا عرفت ورتبت نكون قد اعددنا نوعاً من أنظمة التصنيف [6].

ويمكن تعريف التصنيف بأنه عملية تقسيم مجموعة من البيانات إلى عدة مجموعات. اذ أن التشابه بين النقاط ضمن مجموعة معينة أكبر من التشابه بين نقطتين ضمن مجموعتين مختلفتين. فكرة تجمع البيانات هي فكرةٌ بسيطةٌ في طبيعتها وهي قريبة جدا من الإنسان في طريقه تفكيره حيث اننا كلما تعاملنا مع كمية كبيرة من البيانات نميل إلى تلخيص الكم الهائل من البيانات إلى عدد قليل من المجموعات اوالفئات، وذلك من اجل تسهيل عمليه التحليل. خوارزميات التجميع تستخدم على نطاق واسع ليس فقط لتنظيم وتصنيف البيانات وانما هي مفيده لضغط البيانات وبناء أنموذج ترتيب البيانات. اذ أنه إذا كان بإمكاننا أن نجد مجموعات من البيانات، فانه بالإمكان بناء نموذج للمشكلة على أساس تلك المجموعات [6] [7].

من الممكن تصنيف الصور الى عدة اصناف وتكون نقاط الصنف الواحد مبعثرة بصورة غير منتظمة داخل الصورة ، من هنا يمكن الاستفادة من مواقع هذه النقاط المبعثرة لاخفاء البيانات وهي طريقة تحافظ على امنية البيانات المرسلة [5].

يقوم البحث على اساس تطبيق خوارزمية k-means لتصنيف الصورة التي تمثل غطاء لاخفاء بيانات النص الذي تم تشفيره بخوارزمية 3DES وبواقع بايت كامل من النص لكل بايت من القيمة اللونية اي ان الوحدة الصورية الواحدة ستحتوي على ثلاثة بايتات من النص المراد اخفاؤه [2].

2. هدف البحث:

علم التشفير والإخفاء هما طريقتان لحماية المعلومات من عرضها والعبث بها من قبل الأشخاص الغير المخولين، لكن كلا من الطريقتين لو استخدمت لوحدها، قد لا تعد وسيلة حماية كافية وكاملة. بالنسبة لإخفاء المعلومات مثلا، حالما يكتشف أو يشك أحد المهاجمين بوجود معلومات مخفية في مكان ما، فإن الهدف من عملية الإخفاء يصبح بلا قيمة! لذا فإنه ولزيادة حماية المعلومات المخفية يجب علينا استخدام تقنيتي حماية المعلومات ، التشفير و الإخفاء.

يهدف البحث الى تطبيق خوارزمية امنية تحافظ على سرية النصوص المرسلة داخل صورة غطاء عن طريق تشفير النص وبعثرته داخل الصورة بطريقة التصنيف.

يتكون البحث من مجموعة من الفقرات الاساسية والتي تضم فقرة الدراسات السابقة وفقرات توضيح الخوارزميات الرئيسية التي اعتمدتها الخوارزمية المقترحة وهي (التصنيف بkmeans والتشفير ب Triple DES والاخفاء كبايت كامل)، ثم بعد ذلك تاتي فقرة توضح الخوارزمية المقترحة والنتائج والاستنتاجات ثم الاعمال المستقبلية والمصادر.

3. الدراسات السابقة:

التشفير وإخفاء المعلومات هما طريقتان امنيتان تكمل احداهما الاخرى حيث يقوم الاول بتغيير نص الرسالة الى شفرات ورموز غير واضحة وهذه الشفرات من الممكن ان تثير اهتمام المتصنت الى محاولة فتحها لذا ياتي الاخفاء مكملا للتشفير كي يخفيها داخل وسط ناقل بحيث لا يمكن للمتطفل معرفة وجود اتصال **[1]**.

قدم Kermani و Jamzad (2005) طريقة اخفاء بحيث لا يوحي الغطاء الى وجود معلومات اذ قاما بتقسيم الصورة السرية والصورة الغطاء الى مجموعة كتل بحجم (4×4) يؤخذ من كل كتلة النمط النسيجي لها ويتم البحث عن النمط المتشابه بين الصورة السرية والصورة الغطاء لاخفائه اي ان الاخفاء يعتمد على تشابه الانماط

النسيجية. عملية الاخفاء هنا سوف تتم عن استبدال الكتل الصغيرة في صورة سرية مع الكتل في صورة الغطاء مما يسبب تشويهاً. استخدم الباحثان مرشح جابور Gabor لقياس مدى التشابه بين أنماط الكتل. ويتم الاحتفاظ بعناوين مواقع الكتل في صورة الغطاء والتي حلت محلها كتل من صورة سرية. يتم تحويل البيانات إلى سلسلة من الارقام الثنائية وتعديلها باستخدام شفرة هامنك Hamming والتي تضمن في معاملات تحوير الجيب تمام المتقطع (Discrete Cosine Transform DCT) للصورة الغطاء باستخدام مفتاح يعتمد على مولد الارقام العشوائي [8].

الخوارزمية هنا لايمكن تطبيقها الا عندما تكون الصورة السرية مشابهة نسيجيا نوعا ما للصورة الغطاء لذا يتطلب البحث وجود قاعدة بيانات لصور متشابهة نسيجيا [8].

كما اقترح Socek واخرون (2007) طريقة جديدة لتشفير الفيديو الرقمية التي تمتاز بالعديد من المزايا، قدم تصنيف لخوارزميات التشفير الرقمي الفيديو من أجل توضيح هذه المزايا عن طريق تحليل الجوانب الأمنية والأداء للطريقة المقترحة. وبين الباحثون ان الطريقة المقترحة واعدة ومستقبل التحقيقات قد تكشف عن التطبيق على نطاق أوسع. من الممكن للخوارزمية المقترحة اخفاء شريط فيديو معين داخل فيديو آخر وهو مفهوم جديد في إخفاء المعلومات الفيديو الرقمية [9].

وقدم Arjun واخرون (2007) طريقة جديدة لإخفاء المعلومات وتطبيقها على عينة من الصور. تقوم الطريقة على اساس تضمين مصفوفة. هذه الطريقة تعطي قدرة وكفاءة عالية للتضمين. تم الاستفادة من قانون ويبر، فيشنر Weber-Fechner law لجعل الطريقة المقترحة غير واضحة بصريا (ذات كفاءة اخفاء عالية) مقارنة بالخوارزميات التقليدية [10].

قام Khashandarag و Ebrahimian (2009) بتطبيق خوارزمية لاخفاء البيانات السرية عن طريق تطبيق خوارزمية كبس البيانات Lempel-Ziv-Welch (LZW) و التشفير باستخدام خوارزمية تقسيم الأشجار الهرمية Set Partitioning In Hierarchical Trees (SPIHT) والتي تستخدم الترميز للحصول على معدل بت منخفض وصور بجودة ضغط عالية تستخدم في عملية الاخفاء، واعتمد الباحثان ايضا خوارزميتي تشكيل الطور التكييفي Adaptive Phase Modulation (APM) وتحويل فورييه المتقطع (DFT) Discrete Fourier Transform لاخفاء البيانات السرية [11].

واقترح Medeni و Souidi (2010) طريقة لبناء طريقة جديدة لإخفاء المعلومات، وهي امتداد لتصحيح الخطأ ورمز بناء إخفاء المعلومات. والطريقة المقترحة تتألف من استخدام منطق فك التشفير لتضمين الرسالة في صورة الغلاف، وتستند على استخلاص الترميز [12].

4. خوارزمية K_Means للتصنيف

التصنيف هو طريقة لتجميع البيانات المتشابهة في مجاميع أو اصناف مختلفة وكل مجموعة لابد أن تكون متشابهة والمجاميع المختلفة لابد أن تكون غير حاويةٍ على بيانات مشتركة.

تعد طريقة K-means من اهم تقنيات التصنيف وأكثرها فعالية اكتشفها سنة 1967 العالم J. Maqueen وهي تعد طريقة بدون اشراف، إذ تعطى مجموعة من القيم وتحاول تجزئتها إلى K من الاصناف، وتستعمل خوارزمية تكرارية لتقلل مجموع المسافات المربعة من الكيان إلى مركز الصنف. واكثر تطبيقات خوارزمية K-

means في معالجة الصورة image processing اذ تقوم بتقسيم الصورة الى مجموعة الاصناف المكونة لها ومشكلتها انها تحتوي على حسابات كثيرة. ولغرض تطبيق خوارزمية K-means على الصور يتم [6] :

1. تطبيق خوارزمية التصنيف على الصور تكون نتيجتها تجزئة القيم اللونية الى عدد من المجاميع أو الاصناف.
2. نفرض أن عدد الاصناف هو K , ولذلك فان كل نقطة من الصورة تعطى إلى واحدة من المناطق بالاعتماد على قربها من القيمة اللونية التي تمثل مركز الصنف.
3. الصورة الناتجة تكون على أساس K من القيم اللونية وهذا مشابه لتجزئة الصورة إلى 1,2,…,K من عتبة القيم اللونية.
4. يتم اختيار أحسن الاصناف لتقسيم الصور هو الذي يمتلك أقل مربع خطأ (Least Square Error) والمعرف بالشكل الأتي:

$$D = \sum_{k=1}^{K} \sum_{X_i \in C_k} | X_i - M_k | \quad \ldots(1)$$

حيث إن :

K : عدد الاصناف .

X : النقاط التابعة للصنف C_k.

M_k : مركز الصنف C_k.

إذاً فإن أقل D هي الاصناف الجيدة [7].

5. خوارزمية تشفير البيانات القياسية الثلاثية Triple Data Encryption Standard 3DES

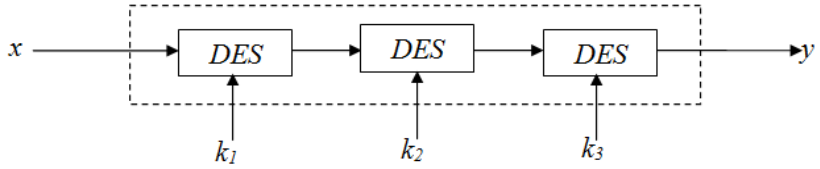
لقد وضعت طريقة تشفير البيانات القياسي (Data Encryption Standard DES) من قبل فريق من شركة آي بي إم حوالي عام 1974 والذي اعتمد على مفتاح بطول 56 بت، خوارزمية تشفير البيانات القياسية الثلاثية تكون ابطأ ثلاث مرات من خوارزمية تشفير البيانات القياسية العادية ولكنها اكثر بلايين المرات أمانا إذا ما استخدمت بالشكل الصحيح. استخدمت خوارزمية تشفير البيانات القياسية الثلاثية على نطاق أوسع بكثير من خوارزمية تشفير البيانات القياسية وذلك لسهولة كسر الاخيرة مع التقدم السريع للتكنلوجيا [1].

خوارزمية تشفير البيانات القياسية الثلاثية هي طريقة لتشفير البيانات تستخدم ثلاثة مفاتيح 64 بت اي ان طول المفتاح الكلي 192 بت، يقسم المفتاح المدخل الى ثلاثة مفاتيح كل منها مكون من 64 بت. طريقة التشفير في هذه الخوارزمية هي نفسها الطريقة المستخدمة في الخوارزمية العادية ولكنها تكرر ثلاث مرات حيث يتم تشفير البيانات بالمفتاح الاول ثم التشفير بالمفتاح الثاني ثم التشفير بالمفتاح الثالث وكالاتي [2]:

$$y=DES_{k3}(DES_{k2}(DES_{k1}(x))) \quad \ldots(2)$$

حيث x يمثل النص الصريح ، y النص المشفر ، k_1 وk_2 وk_3 مفاتيح التشفير الثلاثة

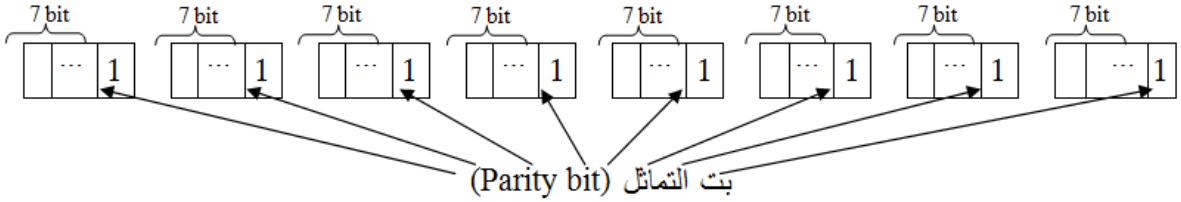
والشكل (1) يوضح كيفية تطبيق الخوارزمية.



الشكل (1) خوارزمية تشفير البيانات القياسية الثلاثية Triple Data Encryption Standard 3DES [2].

وبناء على ذلك، يعمل تشفير البيانات القياسية الثلاثي ثلاث مرات أبطأ من DES القياسية، ولكن هي أكثر أمنا إذا ما استخدمت بالشكل الصحيح. ان إجراءات فك الشفرة هي نفسها إجراءات التشفير، باستثناء انه يتم تنفيذها في الاتجاه المعاكس [1].

من المهم الاشارة الى انه بالرغم من أن مفتاح الإدخال لـDES هو بطول 64 بت، والمفتاح الفعلي المستخدم من قبل DES هو فقط 56 بت في الطول. حيث البت الاقل اهمية (أقصى اليمين) في كل بايت هو بت التماثل (Parity bit)، ويجب ان يكون واحداً للدلالة ان هناك دائما عدداً فردياً من 1 في كل بايت، يتم عادة تجاهل هذه البت في التشفير لهذا فقط 7 بت من البايت هي التي يتم استخدامها فعلا وعليه يكون طول المفتاح هو 56 بت فقط [1]. هذا يعني أن المفاتيح الفعالة الرئيسية لخوارزمية تشفير البيانات القياسية الثلاثية في الواقع 168 بت لأن كل واحد من المفاتيح الثلاثة يحتوي على 8 بت التكافؤ لا يتم استخدامها أثناء عملية التشفير، والشكل (2) يوضح مفتاح الادخال لخوارزمية التشفير القياسية الثلاثية.



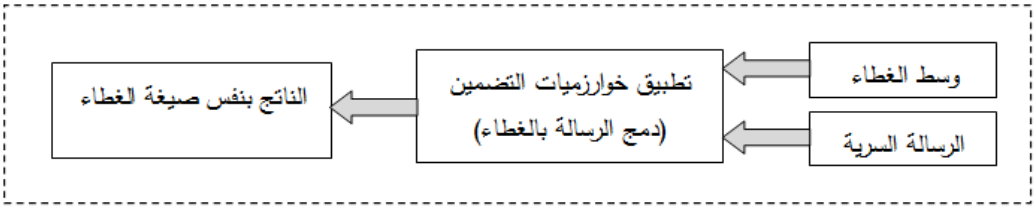
الشكل (2) مفتاح الادخال لخوارزمية 3DES

6. الاخفاء

الاخفاء هو علم يهتم باخفاء وجود اتصال بين طرفين ودمج الرسائل ضمن اوساط، بحيث تكون غير ظاهرة. يعمل إخفاء المعلومات من خلال استبدال بت من البيانات غير المهمة (غير المؤثرة) أو غير المستخدمة في ملفات الكمبيوتر العادية (مثل الرسومات، والصوت، والنص، أو الأقراص المرنة حتى) مع بت من المعلومات المراد اخفائها، بشكل غير مرئي ويمكن أن تكون المعلومات المخفية نصاً عادياً او نصاً مشفراً أو حتى صورة او فيديو [5].

يتم في بعض الأحيان استخدام إخفاء المعلومات عندما لا يسمح التشفير وهو الأكثر شيوعا، ويستخدم الاخفاء لتكملة التشفير فقد يخفى ملف مشفر باستخدام احدى طرق إخفاء المعلومات، لذلك حتى لو تم فك رموز الملف المشفر لا يتم الوصول إلى الرسالة المخفية [5].

يتم إخفاء الرسالة عن طريق إدخالها ضمن الغطاء والذي غالبا ما يكون ملفاً نصياً أو صورة أو ملفات صوت أو فيديو ثم إرسالها إلى الأطراف المعنية، والشكل (3) يوضح طريقة اخفاء المعلومات.



الشكل (3) طريقة إخفاء المعلومات

نتيجة التطور الحاصل في نظم الاخفاء سمح للمستخدم بإخفاء كميات كبيرة من المعلومات في صورة او ملف صوتي، هذه الأشكال من إخفاء المعلومات غالبا ما تستخدم بالاشتراك مع التشفير حيث يتم حماية المعلومات على نحو مضاعف، بحيث المتصنت اذا استطاع العثور على المعلومات اول مرة في ملف الغطاء وهي مهمة صعبة في كثير من الأحيان في حد ذاتها، يحتاج الى فك تشفيرها.

قبل التكلم عن كيفية إخفاء المعلومات في ملف صورة، يجب استعراض كيفية تخزين الصور اولا، ملف الصورة هو ملف ثنائي يحتوي على تمثيل ثنائي من لون أو شدة اضاءة من كل عنصر من العناصر التي تتألف منها الصورة. الصور عادة ما تستخدم إما 8 بت أو 24 بت لتمثيل اللون. عند تمثيل اللون بـ 8 بت، يصل عدد الالوان إلى 256 لونا، كل لون يرمز له قيمة 8 بت.

في نظام ألوان 24 بت، يستخدم 24 بت لكل وحدة صورية، وتوفر مجموعة أفضل بكثير من الألوان. في هذه الحالة، يتم تمثيل كل وحدة صورية ثلاثة بايتات، كل بايت يمثل دقة الألوان الثلاثة الأساسية الأحمر والأخضر والأزرق (RGB)، على التوالي [7].

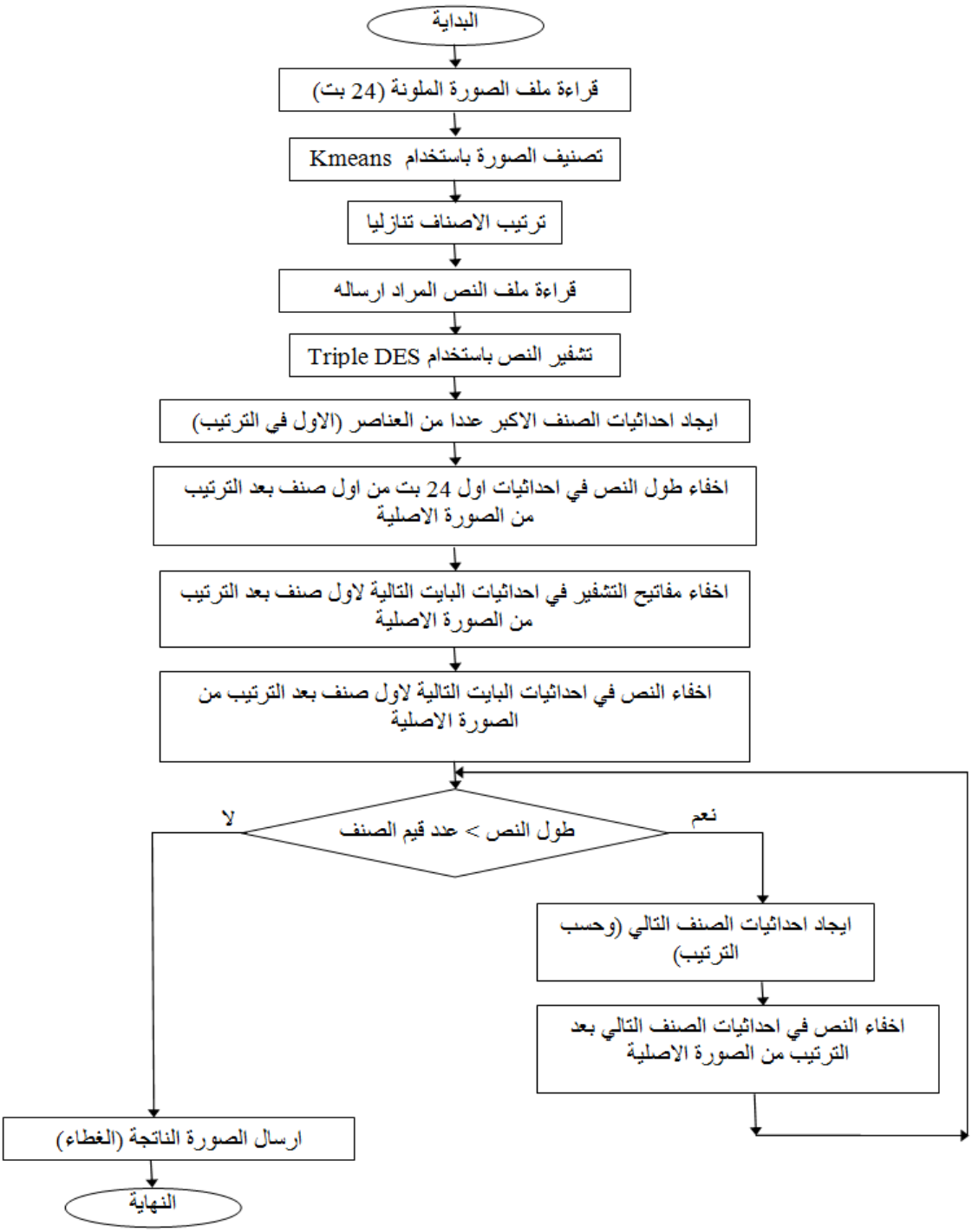
ابسط انواع الاخفاء هو إخفاء البيانات داخل ملف صورة باستخدام البت الأقل أهمية (Least Significant Bit LSB) لكل وحدة صورية. في هذه الطريقة، يمكن اتخاذ تمثيل ثنائي من البيانات المخفية والكتابة في LSB من كل بايت في الصورة الغطاء. إذا تم استخدام ألوان 24 بت، فإن مقدار التغير يكون ضئيلا جدا وغير مدرك للعين البشرية.

7. الخوارزمية المقترحة

تم في هذا البحث تصميم خوارزمية امنية تتكون من مرحلتين رئيسيتين مرحلة التشفير والاخفاء يطبقها المرسل وهي خوارزمية التشفير والتضمين والثانية يطبقها المستلم وهي خوارزمية الاسترجاع والحصول على النص الصريح.

7-1 مرحلة التشفير والتضمين

يتم في هذه المرحلة اجراء المعالجة الاولية لكل من النص والصورة (الغطاء) حيث يتم تطبيق خوارزمية تشفير البيانات القياسية الثلاثية 3DES على النص لغرض تشفيره وكذلك معالجة الصورة الاولية بتطبيق خوارزمية k-means للتصنيف عليها واختيار عدد اصناف عشوائي بعد اجراء دراسة على عدد كبير من الاصناف ثم يتم بعد ذلك اختيار الصنف الاكبر عددا من الوحدات الصورية والتي يستبدل كل بايت منها ببايت من النص المشفر اي ان عملية الاخفاء سوف تتم لكل القيمة اللونية (24 بت) من الصورة الاصلية قبل التصنيف وباحداثيات الاصناف الاكبر عددا من القيم وبترتيب تنازلي مع اخفاء مفاتيح التشفير وطول النص المشفر، وفي حالة كون طول النص اكبر من عدد قيم الصنف الاكبر يتم اختيار الصنف التالي (الاقل) فالاقل عددا من القيم وهكذا الى ان ينتهي النص، يتم بعد ذلك ارسال الصورة الناتجة، والشكل رقم (4) يوضح المخطط الانسيابي لمرحلة التشفير والتضمين في الخوارزمية المقترحة.



الشكل (4) المخطط الانسيابي لمرحلة التشفير والتضمين في الخوارزمية المقترحة.

2-7 مرحلة الاسترجاع (استرجاع النص وفك تشفيره)

يقوم المستلم للصورة المرسلة ايضا بالمعالجة الاولية للصورة ثم القيام باسترجاع النص المخفي حيث يبدا اولا بتطبيق خوارزمية k-means على الصورة الاصلية التي يجب توفرها لديه وايجاد احداثيات الاصناف وبصورة تنازلية وبنفس عدد الاصناف التي اعتمدها المرسل ثم يبدا المستلم باسترجاع طول النص والنص المشفر ومفاتيح التشفير ابتداءاً بالصنف الاكبر عدد من القيم فالاقل فالاقل وحسب طول النص المشفر المخفي.

في الخطوة التالية يتم فك شفرة النص باستخدام مفتاحي التشفير المسترجعين من الصورة وبنفس خوارزمية التشفير (فك تشفير البيانات القياسية الثلاثية) يتم بعدها الحصول على النص الصريح، والشكل رقم (5) يوضح مخطط مرحلة الاسترجاع في الخوارزمية المقترحة.

8. النتائج

تعد المقاييس الكمية من الطرق الأساسية المستخدمة لقياس أداء الخوارزميات المستخدمة في الاخفاء وتتضمن مقياس قمة نسبة الضوضاء الى الاشارة (PSNR) ونسبة الاشارة الى الضوضاء (SNR) ومقياس معدل مربع الخطا (MSE) ، يتم حساب هذه المقاييس وفقا للمعادلات [7]:

$$SNR_{std} = 10\log 10\left[\frac{\sum\sum(input\_image)^2}{\sum\sum(Output\_image - input\_image)^2}\right] \quad \ldots(4)$$

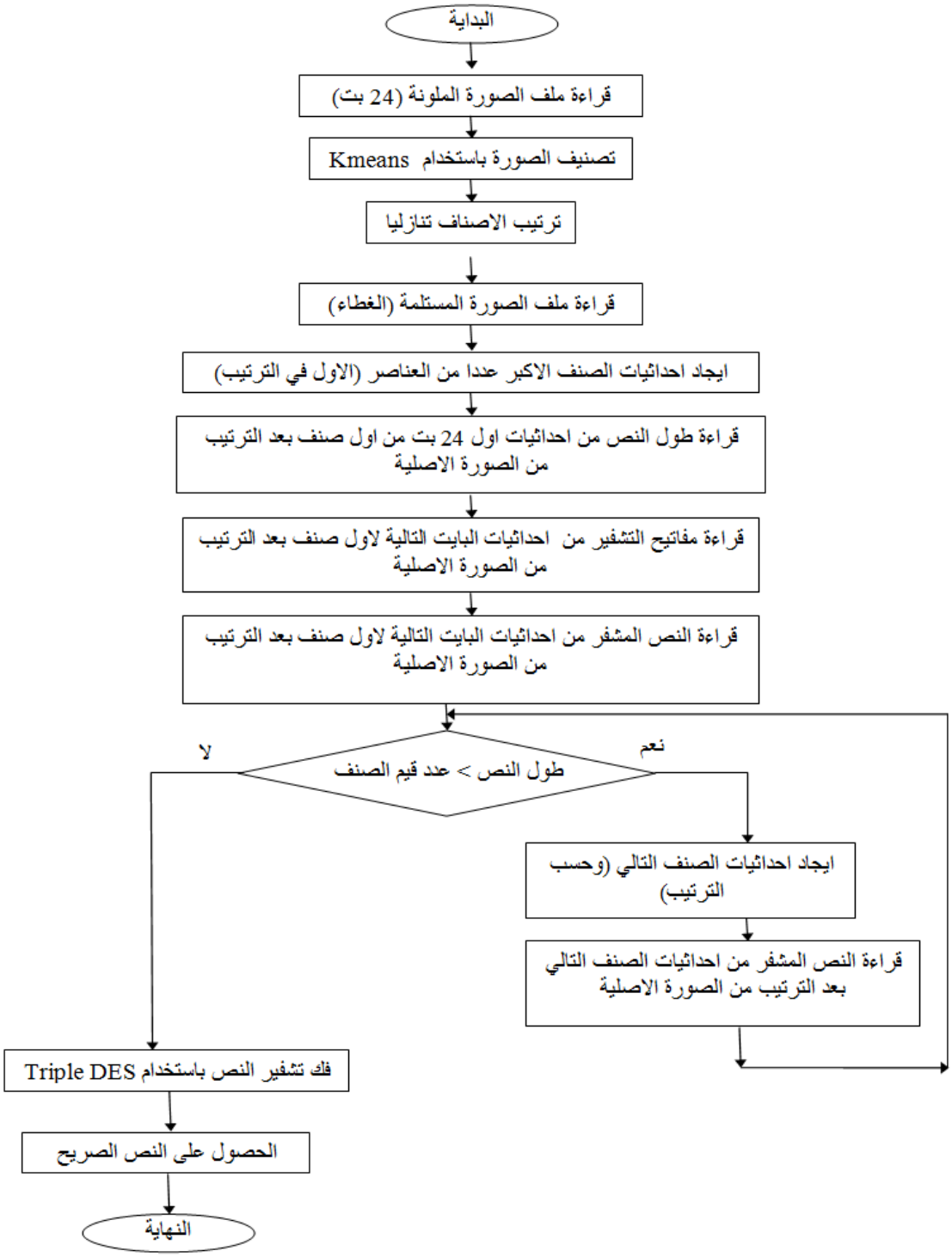
$$MSE = \frac{1}{MN}\sum\sum(Output\_image - input\_image)^2 \quad \ldots(5)$$

$$PSNR = 10\log 10\left[\frac{\max value}{\frac{1}{MN}\sum\sum(Output\_image - input\_image)^2}\right] \quad \ldots(6)$$

وكانت نتائج مقاييس الاداء بالنسبة للخوارزمية المقترحة كما موضح في الجدول (1) والذي يوضح بان الخوارزمية المقترحة كفوءة للتشفير والاخفاء مهما زاد طول الملف النصي وتزداد كفاءة الخوارزمية بزيادة حجم الصورة اما تاثير زيادة عدد الاصناف في الصورة فانه طفيف جدا ومن الملاحظ تقارب القيم الناتجة بالرغم من اختلاف عدد الاصناف (الضعف تقريبا).

تم في البحث اختبار الاصناف (5، 9، 17، 33، 55) وتبين بان تغيير عدد الاصناف ليس له تاثير سوى عند زيادة طول النص اي في تطبيق الخوارزمية، اذ كلما زاد عدد الاصناف سيقل عدد القيم في كل صنف وبالتالي يزداد عدد الاصناف المستخدمة في الاخفاء اذا كان النص طويلاً اي ان التاثير فقط سيكون في تطبيق الخوارزمية.

يمثل الشكل رقم (6) نتيجة اخفاء 2000 بايت من البيانات المشفرة ومن الواضح انه لا يمكن تمييز وجود بينات داخل الصورة الغطاء وكذلك فان حجم الصورة الغطاء لم يتغير بعد اخفاء البيانات داخله، اما الشكل رقم (7) فيمثل صورة غطاء ناتجة من خزن 1500 حرف تقريبا و الشكل رقم (8) يمثل صورة غطاء ل1000. بايت من البيانات.



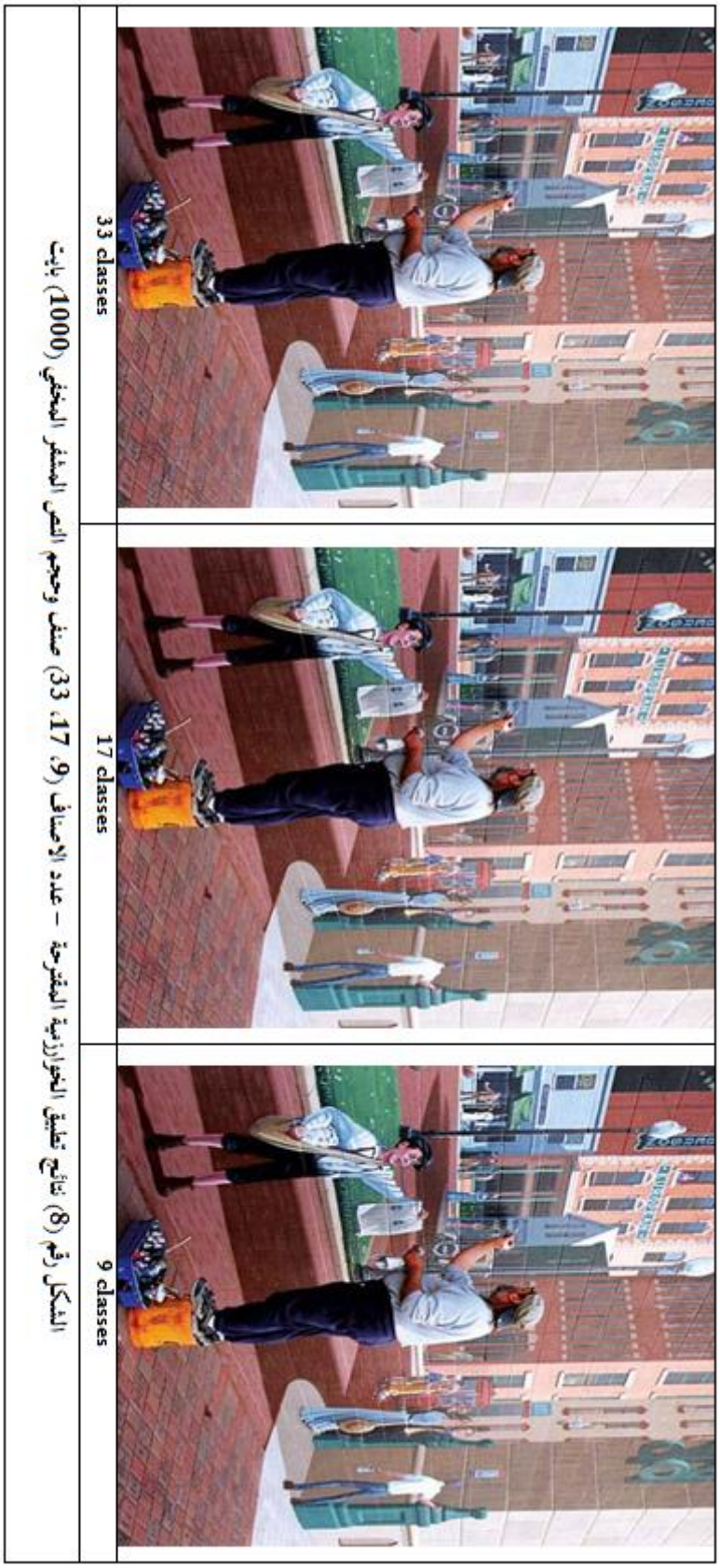
الشكل (5) المخطط الانسيابي لمرحلة الاسترجاع في الخوارزمية المقترحة.

الجدول رقم (١) نتائج تطبيق الخوارزمية المقترحة مع تغيير عدد الاصناف وحجم الصورة وحجم النص المشفر المخفي

Classes		9		17		33	
Text size (byte)	Image Resolution	MSE	PSNR	MSE	PSNR	MSE	PSNR
2000	1024X768	0.116633	57.462601	0.117915	57.415119	0.116242	57.477162
2000	660X461	0.157972	56.144993	0.158862	56.120605	0.155848	56.203789
2000	660X442	0.140934	56.640639	0.142068	56.605849	0.140813	56.644373
2000	660X495	0.172913	55. 752528	0.175032	55.699626	0.175025	55.699803
2000	660X440	0.166264	55.922827	0.161949	56.037020	0.160045	56.088389
2000	660X471	0.130754	56.966238	0.130732	56.966986	0.130872	56.962322
1500	660X660	0.146498	56.472477	0.145249	56.509658	0.142644	56.588273
1500	660X409	0.094725	58.366169	0.095541	58.328906	0.094627	58.370644
1500	480X640	0.086067	58.782456	0.075367	59.359006	0.082056	58.989689
1500	448X640	0.039316	62.185117	0.030575	63.277204	0.033481	62.882822
1500	410X511	0.238530	54.355381	0.227735	54.556514	0.234290	54.433275
1500	457X640	0.045428	61.557605	0.045204	61.579013	0.039629	62.150681
1500	469X640	0.027459	63.744006	0.029379	63.450467	0.024366	64.262980
1000	625X469	0.032665	62.989944	0.033187	62.921097	0.036811	62.470984
1000	258X376	0.381274	52.318427	0.394947	52.165418	0.383467	52.293528
1000	660X440	0.333563	52.899026	0.319555	53.085352	0.322133	53.050456
1000	590X585	0.052200	60.954138	0.051785	60.988746	0.045853	61.517079
1000	457X640	0.017304	65.749402	0.014751	66.442628	0.017143	65.789922
1000	441X640	0.034551	62.746201	0.038660	62.258211	0.036571	62.499491
1000	660X439	0.191155	55.316940	0.189264	55.360125	0.16664	55.302125

الشكل رقم (6) نتائج تطبيق الخوارزمية المقترحة – عدد الاصناف (9، 17، 33) صنف وحجم النص المشفر المخفي (2000) بايت

الشكل رقم (7) نتائج تطبيق الخوارزمية المقترحة – عدد الاصناف (9، 17، 33) صنف وحجم النص المشفر المخفي (1500) بايت



الشكل رقم (8) نتائج تطبيق الخوارزمية المقترحة – عدد الاصناف (9، 17، 33) صنف وحجم النص المشفر المخفي (1000) بايت

9. الاستنتاجات

من خلال تطبيق الخوارزمية المقترحة تبين مايلي:

- ان زيادة عدد الاصناف للصورة ليس له تاثير كبير على عملية الاخفاء اذ ان عملية البعثرة (توزيع النص داخل الصورة) لا يؤثر على تقييم الصورة الناتجة.
- تظهر كفاءة الخوارزمية كون النص يخفى بوصفه بايتاً كاملاً في الصورة وان كل وحدة صورية ممكن ان تخزن 3 بايت من النص وهذا ما يمكن المستخدم من اخفاء نص مهما كان حجمه (اكبر حجم للنص هو 2^{24} بايت) وهذا يعد حجماً كبيراً جدا بل وخيالياً للاخفاء.
- تزداد كفاءة الخوارزمية بزيادة ابعاد الصورة (حجم الصورة الغطاء) وكذلك بزيادة تشتت الالوان فيها وظهور اكبر عدد من الالوان فيها.

10. الاعمال المستقبلية:

- تطبيق الخوارزمية المقترحة على ملف فيديو بوصفه غطاء.
- استخدام خوارزميات التصنيف باستخدام الشبكات العصبية.

المصادر

[1] Stallings William; (2006), *"Cryptography and Network Security Principles and Practices"* , 4th Edition, Pearson Education, Inc., Prentice Hall.

[2] Denny Cherry; (2011) "Securing SQL Server: Protecting Your Database from Attackers", Elsevies. Inc. USA.

[3] Chen Kuanchin; (2005), "Information Hiding Digital Watermarking And Steganography", Western Michigan University, Idea Group Inc IGI , USA, pp 382-384.

[4] Mahmoud, H.; Alghathbar, K.; (2010), "Novel algorithmic countermeasures for Differential Power Analysis attacks on smart cards", Information Assurance and Security (IAS), 6th International Conference, pp: 52 – 55.

[5] Oday Jamal Fawzi, (2007), "Data hiding in Arabic texts", Ph. D thesis, Technical University, Baghdad

[6] Pratt William K., (2007), "Digital Image Processing", 4th Edition, John Wiley & Sons, Inc., California .

[7] González Rafael C. & Richard Eugene Woods, (2008), "Digital image processing", Pearson/Prentice Hall .

[8] Kermani Zahra Zahedi and Jamzad Mansour; (2005): "A Robust Steganography Algorithm Based On Texture Similarity Using Gabor Filter", IEEE International Symposium on Signal Processing and Information Technology.

[9] Socek Daniel , Hari Kalva, Spyros S. Magliveras, Oge Marques, Dubravko Culibrk, Borko Furht; (2007): "New Approaches To Encryption And Steganography For Digital Videos", Springer-Verlag.

[10] Arjun Santosh, Atul Negi, Chaithanya Kranthi, Divya Keerthi; (2007): "An Approach to Adaptive Steganography Based on Matrix Embedding", IEEE 1-4244-1272-2/07/2007.

[11] Khashandarag, A.S.; Ebrahimian, N.; (2009), "A New Method for Color Image Steganography Using SPIHT and DFT, Sending with JPEG Format", Computer Technology and Development,. ICCTD '09. International Conference on Volume: 1 , pp: 581 – 586

[12] Medeni, M.B.O.; Souidi, E.M.; (2010), "Steganographic Algorithm Based On Error-Correcting Codes For Gray Scale Images", I/V Communications and Mobile Network (ISVC), 5th International Symposium, pp: 1 – 4.