المجلة العراقية للعلوم الإحصائية (20) 2011
عدد خاص بوقائع المؤتمر العلمي الرابع لكلية علوم الحاسوب والرياضيات
ص ص [714-729]

تصميم نظام هجين وتنفيذه لتشفير الملف النصي وإخفاءه الملف النصي في بروتوكولات الصوت عبر الانترنت

د. منار يونس كشمولة* رشا عواد حسن**

الملخص

فتح التطور الهائل الذي تشهده شبكات الاتصال فضاءات جديدة تهدد أمن البيانات المنتقلة عبر شبكات الاتصال، ومن هنا ظهرت تقنيات الإخفاء والتشفير والدمج بينهما لزيادة أمنية البيانات المرسلة.

تم في هذا البحث اقتراح وتصميم نظام لإرسال البيانات بصورة سرية وذلك بدمج تقنيتي التشفير وإخفاء البيانات باستخدام تقنية نظام التغطية والقنوات المخفية، فقد تم تشفير البيانات السرية المراد إرسالها باستخدام خوارزمية تشفير البيانات القياسية (DES) أو خوارزمية التشفير المتكرر الثلاثي القياسي (TDES)، ومن ثم إخفاء البيانات المشفرة في صورة ملونة من نوع BMP باستخدام تقنية الخلية الثنائية الأقل أهمية واستخدمت القنوات المخفية لمجموعة من بروتوكولات نقل الصوت (بروتوكول بدء الجلسة Session Initial Protocol(SIP), بروتوكول وصف الجلسة Session Description Protocol(SDP), بروتوكول نقل الوقت الحقيقي Real-Time Transport Protocol (RTP), بروتوكول التحكم بالنقل في الوقت الحقيقي Real-Time Transport Control Protocol(RTCP) عبر بروتوكول الانترنت من نوع القناة المكانية المعتمدة على القيمة وذات السلوك الفعال لإرسال صورة الإخفاء أو ملف نصي،. وقد تم استرجاع المعلومات المخفية بصورة صحيحة ولجميع البروتوكولات.

أما الإخفاء في الصورة فقد تم باستخدام شريحة واحدة من شرائح الصورة أو ثلاث شرائح وفي خلية ثنائية واحدة أو خليتين ثنائيتين أو ثلاث خلايا ثنائية حيث يتم الانتقال من نقطة ضوئية Pixel إلى أخرى إما باستخدام مفتاح واحد أو مفتاحين أو ثلاثة مفاتيح. وتم الوصول إلى أن الإخفاء في خلية ثنائية واحدة يعطي قيمة خطأ اقل لكن مع وقت تنفيذ اكبر، أي أن مقدار قيمة MSE يعتمد على عدد الخلايا الثنائية التي يتم تغيرها، وأنه بالإمكان استخدام مفاتيح متعددة لزيادة سرية الإخفاء مع ضمان عدم فقدان البيانات. تم استخدام اللغة البرمجية Visual C# فضلا عن بيئة Matlab7.6 (R2008a) البرمجية

Design and implementation of the hybrid system for encryption and hiding the text file in the Voice over Internet Protocols.

ABSUTRACT

The immense development in the communication network has opened new spheres that threaten the data security transferred via the communication networks. As a consequence the techniques of encryption and information hiding and merging them to increase the security of data sent.

* استاذ مساعد/كلية علوم الحاسوب والرياضيات/جامعة الموصل
** طالبة ماجستير/ كلية علوم الحاسوب والرياضيات/جامعة الموصل

تاريخ التسلم :2011/10/1 ـــــــــــ تاريخ القبول : 21 /12 /2011

The paper presents suggestion and design for a system to send data secretly by merging encryption technique and information hiding using steganography technique and covert channels to hide the data. The secret data needed to be sent encoded by using Data Encryption Standard (DES) algorithm or by Triple Data Encryption Standard (TDES) algorithm. Then the encoded data were hidden in a form of colored image of BMP type using Least Significant Bit technique (LSB). The covert channels of Voice Over Internet Protocol used its type value based spatial channel and active behavior to send the stego-image or text file using (Session Initial Protocol(SIP) Session Description Protocol(SDP) Real-Time Transport Protocol (RTP) ,Real-Time Transport Control Protocol(RTCP)). The results have been retrieved hidden information properly for all the protocols.

The hiding in image was done by using one slide or three slides of image in one bit or two bits or three bits where the transfer taken place from one pixel to another either by using one key or two key or three key. It is concluded that the hiding in one bit given less error value but with longer execution time that is the value of MSE depends on the number of bits were changed and by using multiple keys to increase the secrecy with the guarantee of not losing the data. Visual C # and Matlab7.6 (R2008a)were used in the programming.

1- المقدمة:

غالبا ما يحتاج مستخدمو الانترنت إلى خزن معلومات سرية وإرسالها وتسلمها، والطريقة الأكثر استخداما لتنفيذ هذا الاحتياج هي بتحويل البيانات إلى شكل مختلف بحيث يمكن للأشخاص الذين يعرفون كيفية إرجاعها إلى شكلها الأصلي فهم البيانات الناتجة فقط ، وتعرف طريقة حماية المعلومات هذه بالتشفير Encryption. إن العائق الرئيس للتشفير هو وجود البيانات بصورة غير مخفية فعلى الرغم من إنها لا يمكن قراءتها لكنها لا تزال موجودة، فإذا كان هناك الوقت الكافي لشخص ما فإنه في النهاية يستطيع فتح شفرة البيانات، لذلك كان لابد من تطوير أمنية البيانات وإنشاء تقنيات جديدة، ومن هنا ظهر نظام التغطية Steganography. [2]

ونظام التغطية هو فن إخفاء البيانات بصورة مبهمة في بيانات أخرى، والهدف منه بصورة عامة هو إخفاء وجود البيانات بحيث إن المتطفل لا يشك بوجود بيانات مخفية أصلا، ويعتمد سر نجاح نظام التغطية على استخدام طرائق وتقنيات بعيدة عن التوقع، فضلاً عن كونه يمكن استخدامه في جميع الوسائط الحاسوبية من صور ونصوص و صوت و فيديو وحزم الشبكة، وبعكس التشفير الذي يعتمد على خوارزميات قياسية ومعروفة.

ومن أكثر تقنيات نظام التغطية شيوعا هي القنوات المخفية التي تعرف بأنها آلية يمكن استخدامها لنقل معلومات بشكل ينتهك السياسة الامنية للنظام، وكذلك يمكن تعريفها بأنها نتيجة سياسة توزيع المصادر وادارتها في نظام معين، أو أنها قناة اتصالات موجودة

ضد رغبة المصمم في نظام الحاسوب أو الشبكة، ومن الأمثلة على القنوات المخفية في الواقع أن نعطي لقارئ مستندا ليوصله الى زميل له في غرفة مجاورة من خلال استخدام شفرة مورس على أنابيب التدفئة الموجودة في غرفته، وتسمى هذهِ الأنابيب قناة مخفية لأن أنابيب التدفئة لم تصمم من قبل مصممي البناية كوسيلة اتصال.[2]

ومن التقنيات التي يمكن استخدامها في الإخفاء هي تقنية نقل الصوت عبر بروتوكول الانترنت Voice Over IP حيث يعرف الأخير أنه إمكانية نقل المحادثات الهاتفية عبر حزم بروتوكول الانترنت التي تعد من أكثر الخدمات شيوعا في شبكات بروتوكول الانترنت، كما أنها تستخدم بصورة واسعة في جميع انحاء العالم مما يعني أن حجم المرور traffic volume الذي يتولد دائما بازدياد، وهذا السبب جعل هذه التقنية مناسبة للاتصالات المخفية من خلال شبكة بروتوكول الانترنت. [11]

إن المحادثات الهاتفية التي تستخدم بروتوكولات نقل الصوت عبر الانترنت تقسم الى طورين: طور الأشارة Signaling Phase ، وطور المحادثة Conversation Phase، وفي كلا الطورين هناك عدد من المرور traffic الذي يتم تبادله بين طرفي الاتصال، حيث يتم استغلال الحقول غير المستخدمة والحقول الاختيارية الموجودة في بروتوكولات نقل الصوت عبر الانترنت لنقل المعلومات بصورة سرية بين طرفي الاتصال. [11]

في هذا البحث تم اقتراح و تصميم نظام يدمج بين تقنيتي التشفير ونظام التغطية، حيث يتم تشفير البيانات السرية باستخدام خوارزمية تشفير البيانات القياسية DES، أو خوارزمية التشفير المتكرر الثلاثي القياسي TDES، ومن ثم إخفاء البيانات المشفرة في صورة ملونة من نوع BMP باستخدام تقنية الإخفاء في الخلية الثنائية الأقل أهمية LSB وبعد ذلك إخفاء صورة الإخفاء في القنوات المخفية باستخدام بروتوكولات نقل الصوت عبر بروتوكول الانترنت VOIP.

2- الدراسات السابقة:

لا يزال العديد من الباحثين الذين يحاولون إيجاد تقنيات جديدة تواكب التطور السريع الذي يحدث في تقنيات أمنية المعلومات، فمنهم من أنجز بحوثا تتعلق بالتشفير ومنهم أنجز بحوثا أخرى تتعلق بإخفاء المعلومات، ومنهم من ربط بين التقنيتين، وآخرون أنجزوا الاتصال السري من خلال القنوات المخفية في بروتوكولات الشبكة، ومن هذه البحوث نسرد ما ياتي:

في عام 1996 قدم Sandfordr و Handel بحثا للإخفاء في بروتوكولات TCP/IP وذلك بالاستفادة من الخلايا الثنائية غير المستغلة في ترويسة البروتوكول IP في

الحقل TOS، والخلايا الثنائية المحجوزة في بروتوكول النقل TCP في حقل محجوز reversed، حيث تم إرسال حرف واحد في كل حزمة شبكة. [8]

وفي عام 2004 قدم Cauich، Gomez وWatanabe بحثا لإخفاء المعلومات في ترويسة البروتوكول الانترنت IP في حقل التعريف Identification وحقل انزياح الجزء Fragment Offset في حالة عدم تجزئة الحزمة من قبل الموجهات الموجودة في شبكة الاتصال. [7]

وفي العام نفسه قدم Cubuk ، Bordly و Shields بحثا اقترحوا فيه تصميم قناة مخفية وقتية باستخدام بروتوكول الانترنت IP. [5]

وفي العام نفسه قدم Llamas بحثا صمم فيه خادماً وكيلاً Server proxy لإخفاء معلومات باستخدام حقل التعريف Identification في ترويسة البروتوكول IP عند طلب خدمة معينة من الخادم. [10]

وفي عام 2005 قدم chauhan بحثا لتحليل التضمين الخزني والوقتي في القنوات المخفية، و يعتمد هذا التحليل على المعلومات المتضمنة في حقل المؤقت TimeStamp لبروتوكول TCP بالنسبة للتحليل الخزني ووصول الحزم لبروتوكول TCP بالنسبة للتحليل الوقتي. [6]

وفي العام نفسه قدم Murdoch وLwies بحثا لتصميم قنوات مخفية باستخدام حقل التعريف identification في ترويسة بروتوكول الانترنت IP، وحقل الرقم التسلسلي Sequence number في ترويسة بروتوكول النقل TCP في بيئة نظام التشغيل Linux. [13]

وفي عام 2006 قدم الباحثون Zander ، Armitage وBranch بحثا لإخفاء البيانات في حقل مدة الحياة Time To Live (TTL) في ترويسة بروتوكول الانترنت IP. [16]

وفي العام نفسه أيضا قدم Kwecka بحثا لإخفاء المعلومات في بروتوكول طبقة التطبيق، وهو بروتوكول نقل النص التشعبي HTTP. [9]

وفي عام 2008 قدم Mazurezyk و Szczypiorski بحثا نظري لإخفاء معلومات في بروتوكول نقل الوقت الحقيقي RTP وبروتوكول السيطرة على النقل في الوقت الحقيقي RTCP. [11]

وفي العام نفسه قدم الباحثان نفسهما بحثا آخر بصورة نظرية لإخفاء المعلومات في بروتوكول بدء الجلسة SIP وبروتوكول وصف الجلسة SDP.[12]

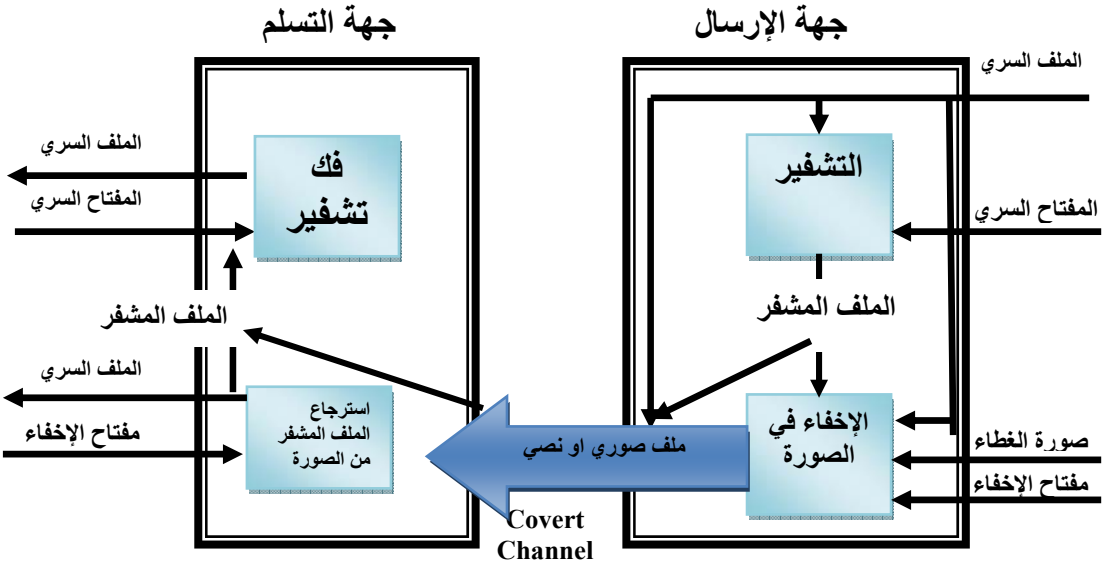
وفي عام 2009 قدم Anguraj و Balamurugand بحثا لإخفاء معلومات داخل ملف صوتي ومن ثم ارساله عبر بروتوكول RTP من دون تغيير خصائص RTP. [4]

وفي العام نفسه قدمت الباحثة أميرة بيبو بحثا لتشفير البيانات، ومن ثم اخفاؤها في صورة ملونة باستخدام الشبكات العصبية وإخفاء النص المشفر أو صورة الإخفاء في القنوات المخفية لبروتوكولات الشبكة TCP, UDP, IP و ICMP. [1]

وفي العام 2010 قدم الباحث احمد ياسين بحثا طبق فيه خوارزميات التشفير على إشارة الصوت المنقول عبر بروتوكول الانترنت، حيث تم تطبيق خوارزميتين من خوارزميات التشفير الكتلي هما: التشفير المتكرر الثلاثي القياسي (TDES)، والتشفير المتقدم القياسي(AES) ، ومن ثم اقترح خوارزمية تشفير جديدة تعتمد على نظام التشفير الكتلي في عملها، أُطلق عليها اسم خوارزمية المباشر والمعكوس (Direct and Reverse)، وتم تطبيقها في إشارة الصوت المنقول عبر بروتوكول الانترنت. [3]

3- تصميم النظام المقترح وتنفيذه

في هذا البحث تم اقتراح نظام لإخفاء معلومات سرية ونقلها بصورة مخفية عبر شبكة محلية، كما موضح في الشكل (1).



الشكل (1) الهيكلية العامة للنظام المقترح

حيث تمر المعلومات السرية في جهة الإرسال بثلاث خطوات هي:

- تشفير المعلومات باستخدام خوارزمية تشفير البيانات القياسية DES ذوات مفتاح سري متكون من 8 حروف ، أو خوارزمية التشفير المتكرر الثلاثي القياسي TDES والمفتاح السري المستخدم يتكون من 24 حرفاً .

- إخفاء النص المشفر باستخدام الخلية الثنائية الأقل أهمية لإخفاء المعلومات السرية، ويمكن استخدام خلية ثنائية واحدة 1-LSB أو خليتين 2-LSB أو ثلاث خلايا ثنائية 3-LSB، ويتم الانتقال من نقطة ضوئية Pixel إلى أخرى عن طريق مفتاح معين ويمكن استخدام مفتاح واحد أو مفتاحين أو ثلاثة مفاتيح.
- **ارسال** البيانات الواردة من اعلاه مخفية عبراحد بروتوكولات الصوت.

اما في جهة الاستقبال فيتم استرجاع المعلومات باستخدام نفس المفتاح الأول وبنفس الاسلوب المستخدم في جهة الارسال.

4- قياس مقدار الفرق بين الصورة الأصلية و صورة الإخفاء

هناك عدة مقاييس لمعرفة مقدار الفرق بين الصورة الأصلية وصورة الإخفاء منها: [2] [15]

- **متوسط مربع الخطأ :Mean Squared Error(MSE)**

لحساب متوسط الخطأ بين الصورة الأصلية وصورة الإخفاء يجب أن نعرف الفرق بين لون النقطة الضوئية pixel بين الصورتين، وذلك وفق المعادلة الآتية:

$$MSE = \frac{1}{mn}\sum_{x=0}^{m-1}\sum_{y=0}^{n-1} stego\_im(x,y) - \text{cover}\_im(x,y) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

حيث إن:

m,n: يمثل ارتفاع وعرضها الصورة

$stego\_im$: يمثل صورة الإخفاء.

cover_im: يمثل صورة الغطاء.

- **نسبة الإشارة إلى الضوضاء** Signal to Noise Ratio(SNR):

يتم استخدام المعادلة الآتية لحساب SNR بين الصورة الأصلية وصورة الإخفاء:

$$SNR = \frac{\sum_{x,y} \text{cover}\_im(x,y)^2}{\sum_{x,y} \left(\text{cover}\_im(x,y) - stego\_im(x,y)\right)^2}. \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2)$$

- **نسبة قمة الإشارة إلى الضوضاء Peak Signal to Noise Ratio(PSNR):**

يتم حساب PSNR بين الصورة الأصلية و صورة الإخفاء لمعرفة مقدار الفرق بينهما، وتسمى وحدة قياس PSNR بالديسبل dB. وتعبر هذه القيمة عن خاصية عدم الاكتشاف Undetectabililty. [14]

$$PSNR = 10.\log_{10}\left(\frac{(Max\,value \quad of\,Gray \quad level)^2}{MSE}\right) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(3)$$

5- نظام التغطية:

تم استخدام تقنية الإخفاء في الخلية الثنائية الأقل أهمية في صورة ملونة من نوع BMP ذات حجم480*640 إذ يبلغ حجم الملف الذي تم إخفاؤه 986 حرفا، وقد تم استخدام شريحة اللون الأحمر او باستخدام جميع شرائح الألوان: (شريحة اللون الأحمر، والأخضر، والأزرق) لإخفاء الملف في خلية ثنائية واحدة أوخليتين ثنائيتين أو ثلاث خلايا وكما مبين في الجدولين (1)، و (2) حيث تم حساب زمن تنفيذ عمليتي إخفاء البيانات المخفية واسترجاعها، وكذلك قيمة ***MSE*** وقيمة ***SNR*** فضلاً عن قيمة ***PSNR***. نلاحظ من الجدولين إن في حالة الإخفاء في خلية واحدة سوف يقل مقدار مربع الخطأ وتزداد قيمة PSNR وقيمة SNR لكن مع زيادة وقت الإخفاء والبيانات المخفية تكون قليلة، أما في حالة الإخفاء في خليتين ثنائيتين فسوف يزداد مقدار مربع الخطأ وتقل قيمة PSNR وقيمة SNR لكن مع وقت إخفاء أقل ومقدار البيانات المخفية تكون أكثر، وفي حالة الإخفاء في ثلاث خلايا سوف يزداد مقدار مربع الخطأ عن الإخفاء في خليتين ثنائيتين وتقل قيم كل من PSNR وSNR فضلا عن وقت إخفاء اقل وكمية البيانات المخفية تكون أكثر.

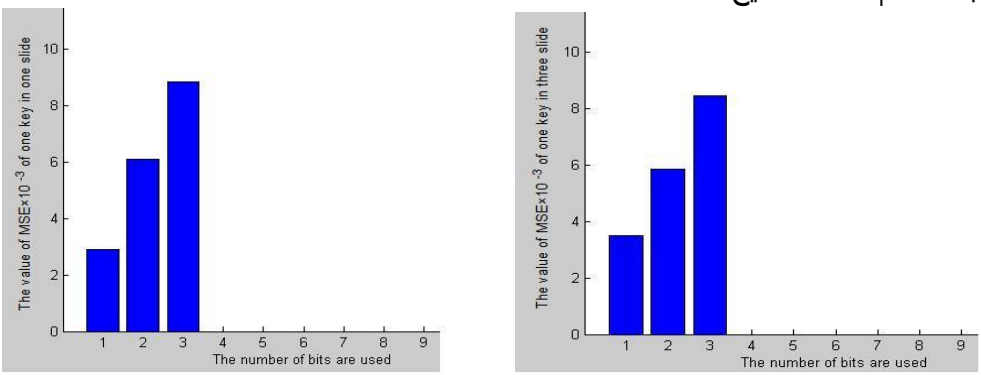
الجدول(1) نتائج نظام التغطية في شريحة اللون الأحمر

إخفاء في	نوع المفتاح	زمن عملية الإخفاء/ ثانية	زمن عملية الاسترجاع/ ثانية	*MSE*	*SNR*	*PSNR*
خلية ثنائية واحدة	مفتاح واحد	1.17677	0.64491	0.0028776	55.3722	73.5405
خليتين ثنائيتين	مفتاح واحد	0.836691	0.177365	0.00610352	54.9466	70.275
ثلاث خلايا ثنائية	مفتاح واحد	0.758126	0.286318	0.00881619	53.9747	68.678
خلية ثنائية واحدة	مفتاحان	1.17896	0.650008	0.0027908	55.3696	73.6735
خليتين ثنائيتين	مفتاحان	0.843698	0.18227	0.00564345	54.9409	70.6154
ثلاث خلايا ثنائية	مفتاحان	0.764406	0.293821	0.0089171	53.9772	68.6286
خلية ثنائية واحدة	ثلاثة مفاتيح	1.18654	0.293731	0.0028504	55.374	73.5816
خليتين ثنائيتين	ثلاثة مفاتيح	0.852421	0.186252	0.0057087	54.9488	70.5335
ثلاث خلايا ثنائية	**ثلاثة مفاتيح**	**0.766174**	**0.29624**	**0.00872396**	**53.9539**	**68.7237**

الجدول(2) نتائج نظام التغطية في جميع شرائح الصورة

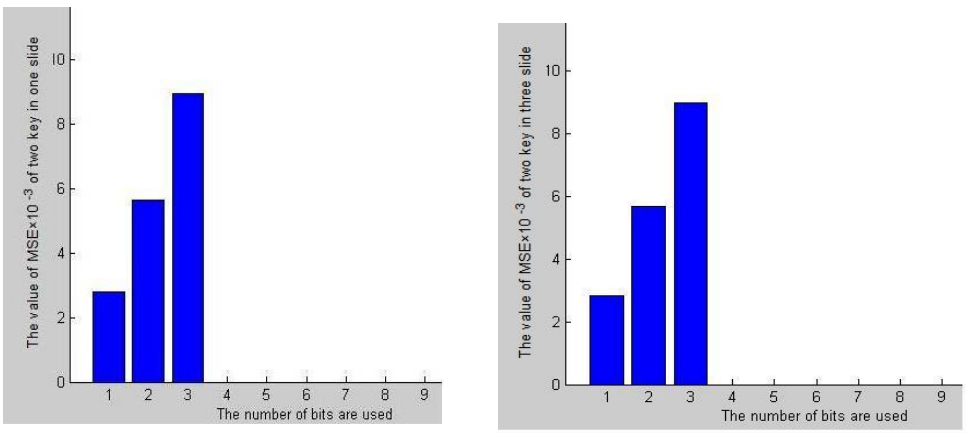
إخفاء في	نوع المفتاح	زمن عملية الإخفاء/ ثانية	زمن الاسترجاع / ثانية	MSE	SNR	PSNR
خلية ثنائية واحدة	مفتاح واحد	1.50358	0.370452	0.0034949501	55.1079	72.6963
خليتين ثنائيتين	مفتاح واحد	0.889348	0.220595	0.00584201	54.9548	70.4652
ثلاث خلايا ثنائية	مفتاح واحد	0.754967	0.152449	0.00843316	53.9217	68.8709
خلية ثنائية واحدة	مفتاحان	2.63662	0.30029	0.00283203	55.3718	73.6098
خليتين ثنائيتين	مفتاحان	0.890227	0.222423	0.00567925	54.9373	70.5879
ثلاث خلايا ثنائية	مفتاحان	0.76194	0.15148	0.00897786	53.824	68,5991
خلية ثنائية واحدة	ثلاثة مفاتيح	2.11802	0.300421	0,00279514	55.3746	73.6668
خليتين ثنائيتين	ثلاثة مفاتيح	0.900601	0.225981	0.00587023	54.9328	70.4443
ثلاث خلايا ثنائية	ثلاثة مفاتيح	0.766044	0.153938	0.00897786	53.824	68.5991

ويبين الشكل(2) نتائج نظام التغطية بشكل أعمدة بيانية في شريحة واحدة وثلاث شرائح باستخدام مفتاح واحد وفي خلية ثنائية واحدة، وخليتين ثنائيتين وثلاث خلايا لقيمة MSE، ويبين الشكل(3) نتيجة الإخفاء باستخدام مفتاحين ويبين الشكل(4) نتيجة الإخفاء باستخدام ثلاثة مفاتيح.

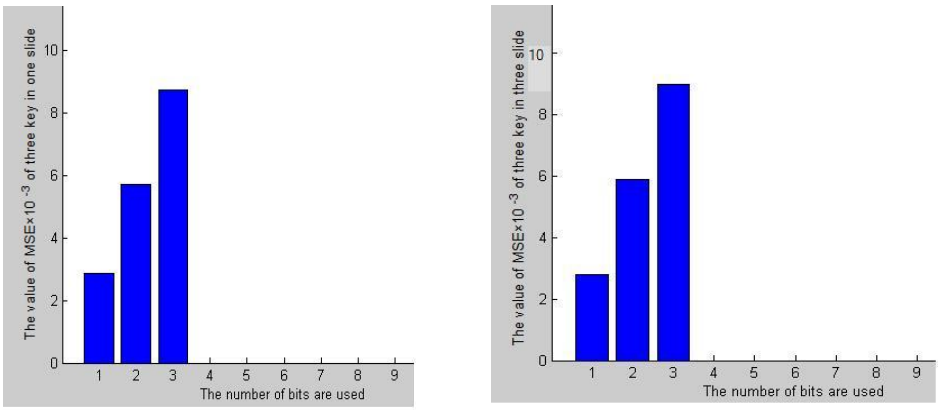


شريحة واحدة **ثلاث شرائح**

الشكل(2) نتيجة الإخفاء باستخدام مفتاح واحد في خلية ثنائية واحدة وخليتين ثنائيتين وثلاث خلايا ثنائية في شريحة واحدة وثلاث شرائح



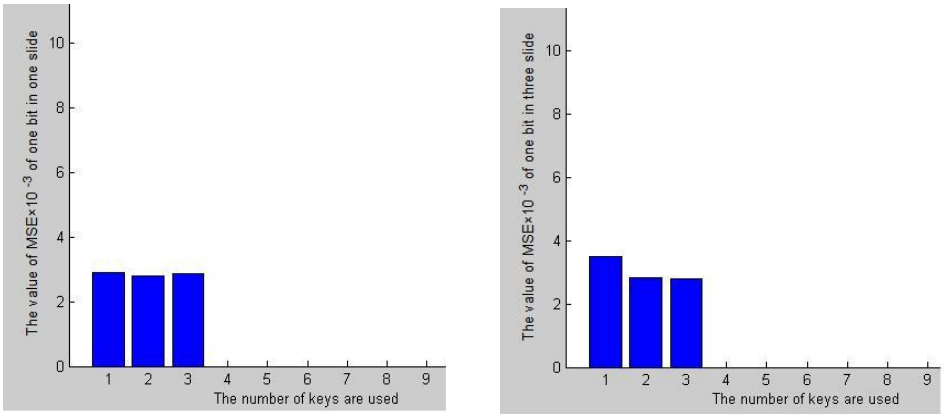
الشكل(3) نتيجة الإخفاء باستخدام مفتاحين في خلية ثنائية واحدة وخليتين ثنائيتين وثلاث خلايا ثنائية في شريحة واحدة وثلاث شرائح



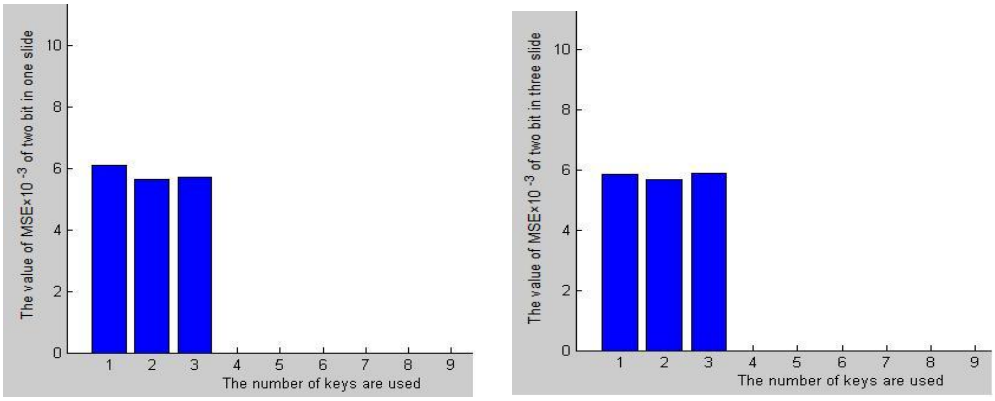
الشكل(4) نتيجة الإخفاء باستخدام ثلاثة مفاتيح في خلية ثنائية واحدة وخليتين ثنائيتين وثلاث خلايا ثنائية في شريحة واحدة وثلاث شرائح

نلاحظ من الإشكال السابقة أن هناك فرقاً في مقدار الخطأ في حالة الإخفاء في خلية ثنائية واحدة، والإخفاء في خليتين ثنائيتين، والإخفاء في ثلاث خلايا ثنائية فهذا يعني أن الإخفاء في خلية ثنائية واحدة يكون تأثيره قليلا في الصورة لأنه يسبب تغيير خلية ثنائية واحدة فقط من شريحة اللون الأحمر، أو الأخضر، أو الأزرق في حالة الإخفاء في شريحة واحدة، وتغيير خلية ثنائية من شريحة اللون الأحمر، والأخضر، والأزرق في حالة الإخفاء في جميع شرائح الصورة، أما في حالة الإخفاء في خليتين ثنائيتين فيحصل التغيير في خليتين ثنائيتين مما يكون الخطأ فيه أكبر من حالة الإخفاء في خلية ثنائية واحدة، وكذلك بالنسبة للإخفاء في ثلاث خلايا ثنائية فسوف يزداد مقدار الخطأ لأنه يسبب تغيير ثلاث خلايا ثنائية.

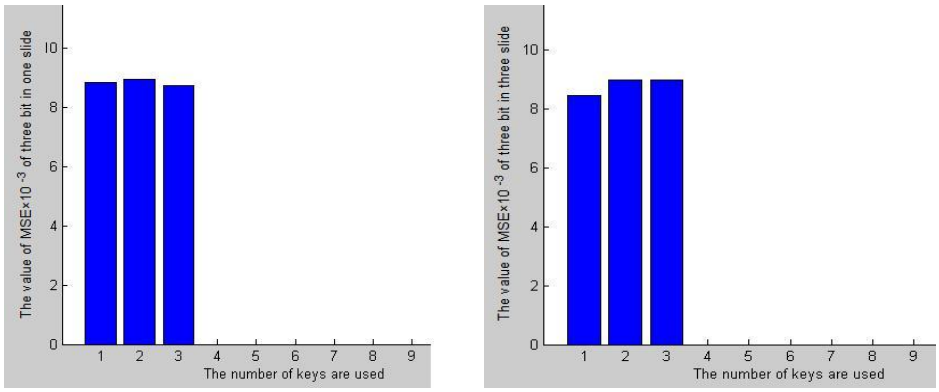
ويوضح الشكل(5) نتائج نظام التغطية في شريحة واحدة وثلاث شرائح وفي خلية ثنائية واحدة باستخدام مفتاح واحد، ومفتاحين، وثلاثة مفاتيح لقيمة MSE، ويوضح الشكل(6) نتيجة الإخفاء في خليتين ثنائيتين ويوضح الشكل(7) نتيجة الإخفاء في ثلاث خلايا ثنائية.



الشكل(5) نتيجة الإخفاء في خلية ثنائية واحدة باستخدام مفتاح واحد، ومفتاحين وثلاثة مفاتيح في شريحة واحدة وثلاث شرائح



الشكل(6) نتيجة الإخفاء في خليتين ثنائيتين باستخدام مفتاح واحد،و مفتاحين وثلاثة مفاتيح في شريحة واحدة وثلاث شرائح



الشكل(7) الإخفاء في ثلاث خلايا باستخدام مفتاح واحد، ومفتاحين وثلاثة مفاتيح في شريحة واحدة وثلاث شرائح

ومن الملاحظ من الإشكال السابقة أن هناك تقارباً في قيمة MSE، وباستخدام أعداد مختلفة من المفاتيح (مفتاح واحد، ومفتاحان، وثلاثة مفاتيح) لنفس عدد الخلايا الثنائية المستخدمة يعني أن تأثير المفتاح في مقدار الخطأ في الصورة يكون قليلاً لأنه يمثل مقدار الانتقال من نقطة ضوئية إلى أخرى فقط أي أن التأثير الحقيقي يحدث في عدد الخلايا الثنائية التي تم تغييرها لإخفاء البيانات، وهذا يعني أنه بالإمكان استخدام مفاتيح متعددة لزيادة الأمنية مع ضمان عدم فقدان في البيانات.

6- نقل المعلومات عبر القنوات المخفية:

يتم توليد حزم الشبكة في جهة الارسال حسب البروتوكول المستخدم كقناة مخفية. وتقرأ الحزم التي في حالة ارسال لغرض ادخال قيمة معينة في حقل منفذ المصدر source port لترويسة بروتوكول معطيات المستخدم UDP وذلك لكي يتم تمييز هذه الحزم عن الحزم الأخرى.

ثم تبدأ عملية إرسال بيانات الملف file عبر القناة المخفية باستخدام احد البروتوكولات الآتية:SIP، SDP ، RTP، RTCP SR و RTCP RR، وقد تم إرسال جملة voice over IP is one of most popular services in IP networks بصورة مخفية عبر البروتوكولات المذكورة. وتم تسجيل نتائج القنوات المخفية باستخدام برنامج Ethereal الذي يقوم بتحليل بروتوكولات الشبكة. وفي ما ياتي الخوارزمية العامة للإخفاء في القنوات المخفية:

1- بدأ الأتصال
2- تشغيل البرنامج الذي يولد حزم الشبكة حسب البروتوكول المستخدم كقناة مخفية
3- قراءة الملف السري المراد نقله
4- حساب حجم الملف المراد نقله
5- قراءة الحزم التي تكون في حالة ارسال
6- إدخال قيمة معينة في حقل source port لترويسة UDP
7- بدء عملية إرسال بيانات الملف file عبر القناة المخفية باستخدام SIP اوSDP اوRTP او RTCP
8- إنهاء الاتصال

6-1 الإخفاء في بروتوكول بدء الجلسة SIP:

أستخدمت خمس حزم لإرسال جملة voice over IP is one of popular services in IP networks عبر القنوات المخفية باستخدام جزء ***branch*** من حقل ***Via***، حقل ***Max-Forwards*** وجزء ***Tag*** من حقل ***From*** . وقد تم إرسال حجم الملف في حقل ***CSeq***، وفي مایاتي ترويسة بروتوكول بدء الجلسة SIP:

```
INVITE sip:john@192.190.132.31 SIP/2.0
Via: SIP/2.0/UDP 10.11.12.13;branch=z9hG4bK776asdhds
Max-Forwards: 70
To: ''John'' <sip:john@192.190.132.31>
From: :''Mark'' <sip:mark@10.11.12.13>;tag=1928301774
Call-ID: a84b4c76e66710@10.11.12.13
CSeq: 314159 INVITE
Content-Type: application/sdp
Content-Length: 228
```

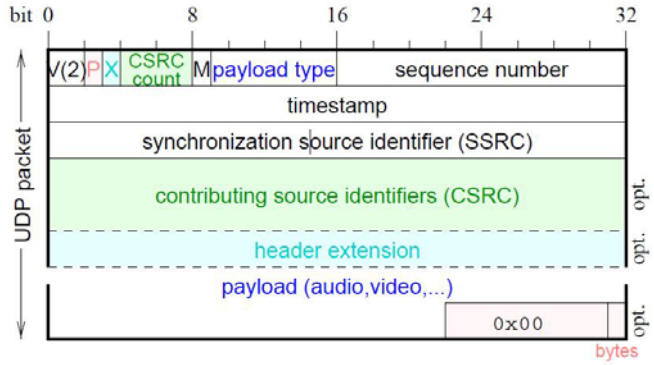
6-2 الإخفاء في بروتوكول وصف الجلسة SDP:

تم استخدام حزمتين لإرسال جملة voice over IP is one of popular services in IP networks عبر القنوات المخفية باستخدام حقل الإصدار وحقل المالك وارس حجم الملف في حقل ***CSeq*** في ترويسة بروتوكول بدء الجلسة، ومن ثم تم ارسال البيانات ضمن حقلي ***Ver*** و***Owner*** وترويسة بروتوكول وصف الجلسة SDP كالاتي:

```
v=0
o=alice 2890844526 2890844526 IN IP4 client.atlanta.example.com
s=-
c=IN IP4 192.0.2.101
t=0 0
k=clear:9123123kjnhdasdoq12e31021n2e4
m=audio 49172 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

3-6 الإخفاء في بروتوكول نقل الوقت الحقيقي RTP:

استخدمت سبع حزم لإرسال جملة voice over IP is one of popular services in IP networks في بيانات الحشوة ***padding data*** لترويسة بروتوكول ***RTP*** كما في الشكل(8). وارسل حجم الملف في حقل مؤقت الشبكة ***NTP TimeStamp*** وتم جعل حقل الحشوة ***Padding*** يساوي واحداً. ومن ثم تم حشر البيانات في نهاية بيانات الحشوة ***padding data***.

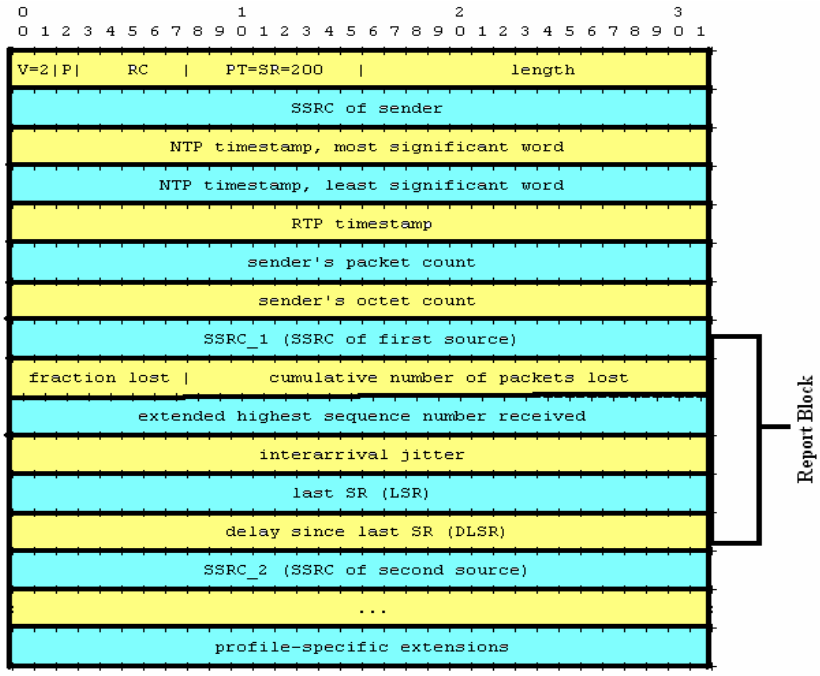


الشكل(8)
ترويسة بروتوكول نقل الوقت الحقيقي RTP

4-6 الإخفاء في بروتوكول السيطرة على نقل الوقت الحقيقي RTCP:

1- الإخفاء في حزم تقرير المرسل RTCP SR:

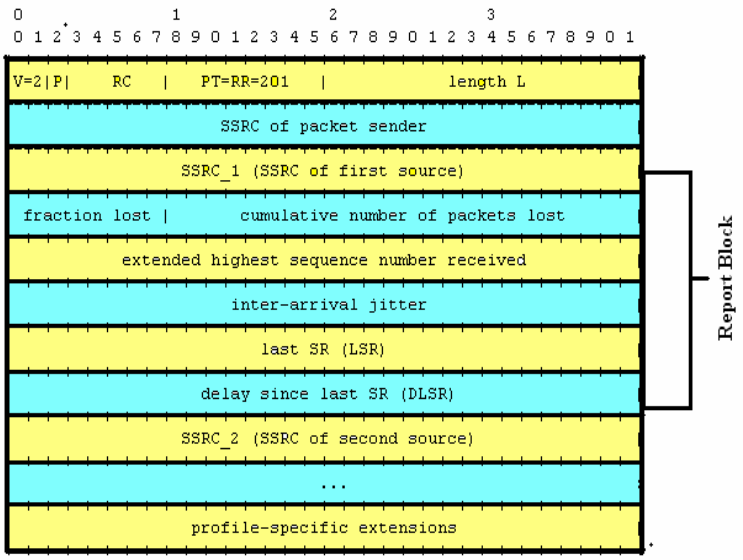
تم استخدام ثلاث حزم لإرسال جملة voice over IP is one of popular services in IP networks عبر القنوات المخفية باستخدام مجموعة حقول كتلة التقرير ***Report Block*** وإرسال حجم الملف في حقل مؤقت الشبكة ***NTP TimeStamp***. الشكل (9) ترويسة بروتوكول حزم تقرير المرسل.



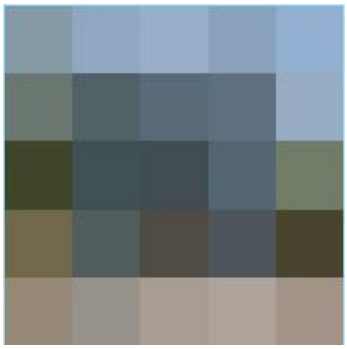
الشكل (9) ترويسة بروتوكول حزم تقرير المرسل RTCP Sender Report

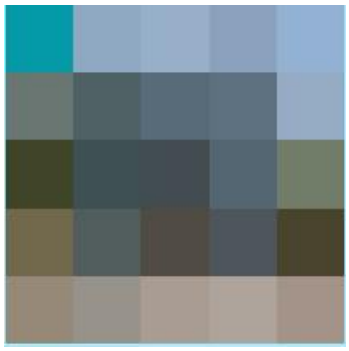
2- الإخفاء في حزم تقرير المستلم RTCP RR:

استخدمت ثلاث حزم لإرسال جملة voice over IP is one of popular services in IP networks عبر القنوات المخفية باستخدام مجموعة حقول كتلة التقرير ***Report Block*** وإرسال حجم الملف في الكتل الثمانية الأربع الأولى لمجموعة حقول كتلة التقرير ***Report Block*** . الشكل(10) يبين ترويسة بروتوكول حزم تقرير المستلم RTCP Receiver Report. ولإرسال صورة ملونة من نوع BMP حجمها 5*5 مخفي فيها كلمة help كما في الشكل(10-أ) والشكل (10-ب) تم استخدام 17 حزمة من بروتوكول نقل الوقت الحقيقي RTP.



الشكل(10)
ترويسة بروتوكول حزم تقرير المتسلم RTCP





10-أ 10-ب

الشكل(10-أ) يمثل صورة الغطاء والشكل (10-ب) يمثل صورة الإخفاء

7- استرجاع المعلومات المخفية:

يتم استرجاع البيانات من الحقول المذكورة ضمن الاخفاء عند الارسال وكل حسب البروتوكول المستخدم.

8- النتائج والاستنتاجات

تم انجاز هذا البحث ليضم قناة مخفية ناجحة من نوع القناة المكانية المعتمدة على القيمة وذات سلوك فعال وتحتوي على المواصفات الآتية: حزمة البيانات تبدو حزمة نظامية ومتناسقة، تم اختيار الحقول المناسبة لجعل مرور الشبكة طبيعياً وغير شاذ، اختيار بروتوكولات تقنية نقل الصوت عبر الانترنت زاد من السرية وقدرة الاختباء للمعلومات المخفية لأنها من البروتوكولات الشائعة في بيئة الشبكات، بعد القيام بتنفيذ النظام المقترح وذلك بتشفير البيانات وإخفائها بصورة ملونة، وإرسال الصورة عبر القنوات المخفية واسترجاع النص بصورة صحيحة، ومن خلال النتائج التي تم الحصول عليها تم التوصل إلى الاستنتاجات الآتية:

في مجال نظام التغطية:

يعتمد مقدار قيمة MSE على عدد الخلايا الثنائية التي يتم تغيرها لإخفاء البيانات فكلما كان عدد الخلايا الثنائية اقل كانت قيمة MSE اقل. إن استخدام مفاتيح متعددة لإخفاء البيانات يعطي سرية اكبر في الإخفاء مع تأثير قليل قد لا يذكر تقريبا في الصورة.

في مجال القنوات المخفية:

اختيار الحقول المناسبة في إخفاء البيانات لم يؤثر في مرور الحزمة عبر الشبكة. وبالامكان استخدام بروتوكول نقل الوقت الحقيقي RTP لإرسال عدد كبير من البيانات، لأنه بروتوكول يستخدم في طور المحادثة الذي يكون طويلاً نسبيا. وعدد البيانات التي يتم

إرسالها باستخدام كل من حزم تقرير المرسل RTCP SR وحزم تقرير المتسلم RTCP RR يعتمد على عدد حزم السيطرة التي يتم تبادلها بين الطرفين في طور المحادثة.

9- المصادر:

المصادر العربية:

1- البلاسيني ،أميرة بيبو سلو ، 2009، " تقنيات إخفاء المعلومات باستخدام الشبكات العصبية وبروتوكولات الشبكة"، "، رسالة ماجستير، قسم علوم الحاسبات، كلية علوم الحاسبات والرياضيات ، جامعة الموصل، العراق.

2- الحمامي، علاء حسين و الحمامي، محمد علاء، 2008، "إخفـاء المعلومـات: الكتابـة المخفية والعلامة المائية "، إثراء للنشر والتوزيع، الشارقة.

3- الراوي، أحمد ياسين كامل ،2010، " تطبيق خوارزمية تشفير مقترحة على الصوت عبر بروتوكول الانترنيت"، رسالة ماجستير، قسم علوم الحاسبات، كلية علوم الحاسبات والرياضيات ، جامعة الموصل، العراق.

المصادر الاجنبية:

4- Anguraj S. and Balamurugand D.,2009, "Implementation of Audio Steganography in Real-Time Protocol(RTP) and Hypothesis of RTP Features" National conference on Intelligent Electrical System(NCIES).

5- Cabuk, Serdar , Brodley, Carla and Shields, Clay (2004), "IP Covert Timing Channels: An Initial Exploration", Washington, USA.

6- Chauhan, Sweety, 2005, "Analysis and Detection of Network Covert Channels" Department of Computer Science and Electrical Engineering University of Maryland Baltimore County.

7- Cauich, Enrique, Gómez, Roberto and Watanabe, Ryouske (2004), "Data Hiding in Identification and Offset IP Fields", University of California, Irvine USA.

8- Handel, T. and Sandford ,M., 1996 “Hiding data in the OSI network model,” in *Proceedings of the First International Workshop on Information Hiding* pp. 23–38.

9- Kwecka, Zbigniew, (2006), "Application Layer Covert Channel Analysis and Detection", University for the degree of Bachelor of Science with Honours in Networked Computing, Napier University, Edinburgh.

10- Llamas, David, (2004), "Covert Channel Analysis and Data Hiding in TCP/IP", University for the degree of Bachelor of Science with Honours in Software Technology, Napier University, Edinburgh.

http://www.dcs.napier.ac.uk/~01009322

11- Mazurczyk, Wojciech and Szczypiorski, Krzysziof, 2008, "Steganography of VoIP Streams", Warsaw University of Technology, Faculty of Electronics and Information Technology Institute of Telecommunication.
12- Mazurczyk, Wojciech and Szczypiorski, Krzysziof, 2008, "Covert Channel in SIP for VoIP Signalling", Warsaw University of Technology, Faculty of Electronics and Information Technology Institute of Telecommunication.
13- Murdoch, Steven J. And Lewis, Stephen, (2005), "Embedding Covert Channels into TCP/IP", University of Cambridge, United Kingdom
14- Rana, Rita and Singh, Er.Dheerendra,2010, "Steganography-Cocealing Messages in Images using LSB Replacement Technique with Pre determined Random Pixel and Segmentation Image", International Journal of Computer Science & Communication, Vol.1, No.2, PP. 113-116.
15- Saffor, Amhamed and Ramli, Abdul Rahman, (2001), "A Comparative Study of Image Compression between JPEG and Wavelet", University Putra Malaysia, vol. 14, no. 1, 2001, pp. 39-45, Selangor, Malaysia.
16- Zander, Sebastian , Armitage, Grenville and Branch, Philip (2006), "Covert Channels in the IP Time To Live Field", Swinburne University of Technology Australia.