ISSN: 1991-8941

تطبيق خوارزمية تشفير مقترحة لتشفير الصوت عبر بروتوكول الانترنيت

أحمد ياسين كامل منار يونس كشمولة
مديرية تربية نينوى
جامعة الموصل - قسم علوم الحاسوب

الخلاصة

إن عملية نقل إشارة الكلام بسرية عالية وبأسرع وقت عبر شبكة الانترنيت يحتاج إلى تطوير تقنيات كبس وتشفير إشارة الكلام، وذلك لتقليل حجمها وجعلها غير مفهومة للأشخاص غير المخولين بالاستماع إليها. تم في هذا البحث تصميم نظام لتشفير الصوت عبر بروتوكول الانترنيت (VoIP) واستخدام تقنيات الكبس لغرض تقليل حجم البيانات وإرسالها عبر الشبكة، إذ تم استخدام خوارزمية (A_law PCM) في كبس بيانات الصوت. ومن ثم تم تطبيق خوارزميتي التشفير المتكرر الثلاثي القياسي (TDES)، ومقياس التشفير المتقدم (AES). تم اقتراح خوارزمية تشفير جديدة تعتمد في أساس عملها على نظام التشفير الكتلي، أُطلق عليها اسم خوارزمية المباشر والمعكوس، حيث تعتمد على ثلاث خطوات أساسية وهي توسيع المفتاح الأولي، وتوجيه التشفير لكل دورة باتجاه معين، وكذلك تبديل الـ (Bytes) حسب صندوق التعويض المستخدم في خوارزمية AES وذلك بجعله متحركاً. تم حساب نسبة الكبس بصورة عامة وكانت 50%، وتمت مقارنة نتائج معامل الارتباط للخوارزمية المقترحة مع نتائج خوارزميتي (AES, TDES).

مقدمة :

لا يخفى على احد أهمية الدور الذي تلعبه وسائل الاتصال الخاصة بالكلام في الحياة اليومية، ولاسيما بعد استحداث الهاتف الخلوي وخدمات الانترنيت التي أوجدت إمكانية نقل الصوت بصيغته الرقمية عبر شبكات الإتصال (الصوت عبر بروتوكول الانترنيت Voice over Internet Protocol / VoIP)،[4]. ومع نشوء وتطور أنظمة الاتصالات التي تستخدم الكلام أصبحت أمنية الكلام من الأهداف المهمة لمستخدمي هذه الأنظمة.

لغرض تحقيق عملية التناقل هذه ولضمان وصول إشارة الكلام إلى الجهات المطلوبة كان لا بد أن تكون في متناول الجميع عبر الشبكة المشتركة، وهنا تبرز الحاجة إلى تطوير تقنيات تشفير إشارة الكلام بحيث نحصل على مستوى عالٍ من السرية عن طريق جعل إشارة الكلام غير مفهومة بالنسبة للأشخاص غير المخولين بالاستماع إليها. وتحتوي إشارة الكلام على معلومات تتعلق بشخصية المتكلم, وهي تمثل الاختلافات القليلة في تردد طبقة الصوت حيث تُمكِنّ المستمع من تمييز الشخص المتكلم. ولهذا فانه يمكن أن نستخدم تردد حدة الصوت والزمن لأية إشارة كلام معطاة لتشكيل إشارة أخرى تحمل نفس الرسالة المرسلة، مع مراعاة أن إعادة التكوين هذه ربما تعطي صوتاً غير طبيعي، مما يُفقد الشخصية المتكلمة شيئاً من خصوصيتها، فضلاً عن أن كمية المعلومات المفقودة تعتمد على عدد من المتغيرات التي استخدمت لتشكيل الإشارة الجديدة؛ المبدأ لإعادة تكوين الكلام هو الفكرة الأساسية وراء تشفير إشارة الكلام.

مما سبق يتضح أن الرسالة الصوتية تحتوي على نوعين من المعلومات هما محتويات الرسالة وشخصية المتكلم. وفعلياً فإن الإشارة المشفرة يجب أن تحجب كلاً من محتويات الرسالة وخصائص المتكلم عن الشخص غير المخوَّل، ومن ثم المقدرة على إعادة تكوين كلام واضح مطابق للأصل[2]. ولزيادة حماية الرسائل وتقليل المساحة اللازمة لخزنها في ملف أو إرسالها على الشبكة استخدمت تقنية الكبس. وقد ظهر الكبس في الاتصالات قبل حوالي 25–30 سنة، ومن الأسباب التي جعلت استخدام كبس البيانات ضرورياً في الاتصالات، أن كبس النصوص يكون باستخدام رموز قصيرة للنصوص المتشابهة وطويلة للأخرى، وهو عملية تحويل بيانات نص إلى بيانات أخرى بحجم اقل من الأولى. ويوجد العديد من خوارزميات الكبس التي تعتمد على أفكار مختلفة، وتعطي نتائج مختلفة، ولكن لها المبدأ نفسه وهو كبس البيانات[1].

دراسات سابقة

في عام 2002 قام الباحثان (G.Manjunath and G.V.Anand) باستخدام تقنية تشفير متناظرة جديدة باستعمال التحويل المركزي الوحدوي لنموذج من عينة الإشارة

المتناظرة وهي أقل عرضة للمهاجمة من الطرق التي تعتمد على نظام بعثرة الإشارة في مجال الوقت والتردد [11].

في عام 2003 قامت الباحثة علياء موفق بتشفير إشارة الكلام بطريقتين: الأولى بعثرة الكلام في حيز الزمن (بعثرة وحدات الوقت)، والثانية تعتمد على تبديل معاملات تحويل فورير السريع والتي تسمى بعثرة مجال التحويل، والاثنان يعطيان نفس الدرجة من السرية. ولكن جودة الإشارة المسترجعة في طريقة بعثرة مجال التحول تكون أفضل[2].

في عام 2004 قامت الباحثة سجى جاسم باقتراح خوارزمية جديدة لعملية كبس الملفات الصوتية عن طريق اكتساب الكلام من لاقط الصوت والعمل على إزالة فترات الصمت واقتباس بعض العينات للإشارة الناتجة وتقطيعها وتطبيق إحدى طرائق موائمة منحني الإشارة وخزن النتائج في ملف ذي صيغة جديدة أُطلق عليه الامتداد (ssc.) وكانت نسبة الكبس(26.283%) [4].

في عام 2005 قام الباحثون (Yoshifumi Chisaki, et.al.) باقتراح نظام لتشفير الكلام بمعدل (Bit Rate) منخفض لخوارزمية ترميز لخط النقل التناظري. استخدم ستة مفاتيح لتشفير ثلاثة أجزاء مختلفة لحماية معلومات الكلام. فضلاً عن إمكانية إيصال الإشارة المشفرة عبر خط ناقل للموجة الطورية واستخدام الشريط المغناطيسي لخزن الموجة الطورية. وكذلك فان نظامهم المقترح مفيدٌ لخط الإرسال الرقمي دون صعوبة[10].

كذلك في نفس العام قدم الباحثون (Wei-Gang Fu, et.al.) خوارزمية متدرجة لعمل جولات متداخلة من البعثرة لملفات MP3 السمعية. إذ تم إعادة تكوين إخراجات ملفات الMP3 السمعية بنوعيات مختلفة بالاعتماد على عدد المفاتيح المعطاة وعدد جولات البعثرة المُنجزة. و تعتمد كل جولة من إعادة الترتيب على نتائج الخطوة السابقة[19].

كذلك في نفس العام قام الباحثون (Xinyuan, et.al.) بتضمين علامة مائية أُحادية في حزمة الـ(VOIP) المتدفقة بتعديل طفيف في توقيت اختيار الحزمة[18].

في عام 2008 قام الباحث (Markus Albert) بتصميم نظام تشفير الصوت عند الزمن الحقيقي، إن الفكرة الأساسية للنظام هي استخدام تقنية بعثرة التردد على إشارة الصوت المأخوذة من لاقط الصوت، ثم إعادة تشغيلها بشكل مبعثر حيث يقوم باستخدام تحليل قناة التردد خلال مرشح الإشارة الرقمية ثم يعيد ترتيب أجزاء الحزمة بتسلسل مختلف وبذلك تنتج إشارة صوت مبعثرة[8].

كذلك في نفس العام قام الباحثان (Tin and Nant) بتشفير الصوت المنقول عبر بروتوكول الانترنيت باستخدام خوارزمية (Linear Feedback Shift Register/LFSR) التي هي إحدى خوارزميات المفتاح المتماثل، إذ يتم تشفير إشارة الصوت وتحويله إلى نص مشفر، وفي الطرف الآخر يتم تحويل النص المشفر إلى إشارة صوت، وكانت نتائج الصوت المسموع جيدة[17].

تم في هذا البحث تصميم نظام نقل الصوت عبر بروتوكول الانترنيت (VoIP) والذي ضم خوارزمية لكبس بيانات الصوت. وتم تطبيق خوارزميتين من خوارزميات التشفير الكتلي هما: التشفير المتكرر الثلاثي القياسي (TDES) ومقياس التشفير المتقدم (AES)، وتم اقتراح خوارزمية تشفير جديدة تعتمد على نظام التشفير الكتلي في عملها، أُطلق عليها اسم خوارزمية المباشر والمعكوس (Direct and Reverse) وتم المقارنة بين نتائج التطبيق للخوارزميات على إشارة الصوت باستخدام معامل الارتباط بين الإشارة الأصلية والإشارة المشفرة.

بروتوكولات الوسائط

تتطلب عمليات نقل ملفات الوسائط بروتوكولات، وهذه البروتوكولات تعمل بمواصفات تخدم تطبيقات الوقت الحقيقي منها:-

بروتوكول نقل الوقت الحقيقي Real Time Transport Protocol RTP

يدعم هذا البروتوكول وظائف نقل الشبكة نهاية إلى نهاية (end-to-end) التي تكون مناسبة لتطبيقات نقل بيانات الوقت الحقيقي مثل الصوت أو الفيديو عبر شبكة الخدمات المفردة أو المتعددة. من مساوئه انه لا يدعم أية تقنية لضمان وقت الوصول ولا يدعم ضمان نوعية الخدمة (Quality of Service / QoS) [6,21].

بروتوكول السيطرة والنقل للوقت الحقيقي Real Time Transport Control Protocol RTCP

هو بروتوكول متمّم ويستخدم لنقل معلومات السيطرة مثل عدد الحزم المرسلة والمفقودة والتأخير والهيجان [13]. ترسل النقاط النهائية بشكل دوري (حزم) من (RTCP) لينشر معلومات مفيدة عن نوعية الخدمة، فالنقاط النهائية ممكن أن تختار القيم المناسبة الصحيحة لتنقل بشكل فعال الوسائط عبر (RTP)، ومن الوظائف التي يوفرها هذا البروتوكول ,إرجاع نوعية الخدمة(QoS Feedback), والسيطرة على الجلسة (Session Control), وتداخل الوسائل المتزامنة(Inter Media Synchronization) لاحداث تزامن بين سيل من الصوت والفيديو[2].

كيف يعمل الـ VOIP

عند نقل الصوت عبر بروتوكولات الأنترنيت يجب أولاً تحويل الإشارات التناظرية الخارجة من المصدر إلى إشارات رقمية, ثم تبدأ بعد ذلك عملية كبس الكلام باستخدام خوارزميات كبس الكلام مثل (PCM,ADPCM...الخ)، وبعد تحويل حزم الصوت إلى حزم بيانات يتم استخدام بروتوكولات (UDP,RTP) لنقل حزم البيانات عبر بروتوكول الانترنيت، وبعد ذلك يقوم نظام تأشير (Signaling system) بمحاولة استكشاف ومن ثم العثور على عنوان الهدف لإقامة اتصال معه. وعند المستلم لابد من فك الكبس للحزم وتحويلها إلى إشارة صوت تناظري [7,15].

ترميز الكلام:

هناك عدة تقنيات تستخدم لترميز الكلام ومن بينها ترميز الموجة, حيث يتم كبس إشارة الكلام دون الأخذ بنظر الإعتبار كيفية توليد الموجة. وتستند طرائقهِ إلى مجال الزمن ومجال التردد. اما التي تعمل في مجال الزمن:-

1- Pulse Code Modulation /PCM
2- Differential Pulse Code Modulation / DPCM
3- Adaptive Differential Pulse Code Modulation / ADPCM

بينما الطرائق التي تعمل في مجال التردد هي:-

1- Subband Coder
2- Transform Coder

وقد تم في هذا البحث استخدام طريقة الـ(PCM) ،حيث أنها معروفة ببساطة تمثيلها وقلة تأخيرها. ويتم تمثيل كل عينة بكلمة مرمزة، وتستخدم تكميم منتظم بفواصل متدرجة. وعند تطبيق التحويل يكون التكميم المنتظم بفواصل متدرجة قد تُغير إلى تدرج لوغارتمي، لكي يسمح بتغطية القيم العالية بنفس عدد الـ(Bits). وباستخدام اسلوب التحويل (A-Law). وتعتمد على قيمة دقيقة هي المعامل الرياضي A، فإذا فرضنا أن العينات المتوفرة هي S، فإن العينات المكبوسة باستخدام طريقة A-Law هي SA:

$$SA = \begin{cases} \left(\frac{A}{1+\ln A}\right)(S) & 0 \le |S| \le 1/A \\ \frac{1+\ln(AS)}{1+\ln A} & \frac{1}{A} \le |S| \le 1 \end{cases}$$

حيث أن (A=87.56) [20,9].

تم اعتماد طريقة A-Law PCM في عملية كبس عينات إشارة الكلام حيث تقوم بكبس (12 or 16 Bit/Sample) وتحويلها إلى (8 Bit/Sample) أما في عملية فتح الكبس فيتم تحويل (8 Bit/Sample) إلى (12 or 16 Bit/Sample) مع فقدان بعض البيانات كما هو موضح في الجدول (1) [9,20].

الجدول (1) جدول الكبس A-Law PCM

Input Code	*Compressed Code*	*Output Code*
s0000000wxyza...	s000wxyz	s0000000wxyz1…
s0000001wxyza...	s001wxyz	s0000001wxyz1…
s000001wxyzab...	s010wxyz	s000001wxyz10…
s00001wxyzabc...	s011wxyz	s00001wxyz100…
s0001wxyzabcd...	s100wxyz	s0001wxyz1000…
s001wxyzabcde...	s101wxyz	s001wxyz10000…
s01wxyzabcdef...	s110wxyz	s01wxyz100000…
s1wxyzabcdefg...	s111wxyz	s1wxyz1000000…

حيث تمثل s (sign bit)

خوارزمية المباشر والمعكوس المقترحة للتشفير

في هذا البحث تم اقتراح خوارزمية لتشفير الصوت استناداً إلى خصائص **شانون** وتتلخص هذه الخوارزمية بثلاث خطوات أساسية، كما يلي:

1- يتم توسيع المفتاح الأولي لكي يصبح بطول (عدد الدورات × حجم البيانات × نصف طول المفتاح الأولي).
2- تتم عملية التشفير أو فك التشفير باتجاهين متعاكسين للبيانات (أي من بداية كتلة البيانات إلى نهايتها أو بالعكس) وذلك بجعل كل دورة تتجه باتجاه معين (أي إذا كان لدينا ثلاث دورات فالأولى تتجه بالاتجاه المباشر والثانية تتجه بالاتجاه المعاكس أما الثالثة فتتجه بالاتجاه المباشر). فضلاً عن ذلك يكون في الدورة الواحدة لكل حرف نصف طول المفتاح الأولي من المفاتيح لتشفيره أو لفك تشفيره. وبذلك يكون عدد العمليات الحسابية التي تجري على كتلة من البيانات هي بطول المفتاح الموسع.
3- يتم استخدام صندوق التعويض المستخدم في خوارزمية الـ AES لتبديل الـ Bytes ثم التحديث عليه، وذلك بجعله متحركاً على عكس خوارزمية AES (أي كان ثابتاً).

تطبيق خوارزميات التشفير على الصوت عبر بروتوكول الانترنيت

تم تصميم نظام تشفير إشارة الكلام وإرسالها عبر بروتوكول الانترنيت، جهة المرسل تمر بأربع خطوات :-

1- تهيئة الاتصال بين طرفي المرسل والمستقبل وتبادل المفتاح السري.

2- تسجيل الصوت الداخل من لاقط الصوت المربوط ببطاقة الصوت.
3- كبس بيانات الصوت التي تم تسجيلها في الخطوة الثانية.
4- يتم تشفير بيانات الصوت باستخدام (الخوارزميات المقترحة، TDES، AES).

أما جهة المستقبل فتمر بأربع خطوات أيضا:

1- تهيئة الاتصال بين طرفي المستقبل والمرسل وتبادل المفتاح السري.
2- فك تشفير بيانات الصوت المستلمة حسب الخوارزمية المتبعة.
3- فك كبس بيانات الصوت.
4- عرض بيانات الصوت الناتجة من الخطوة الثالثة على السماعة (Speaker).

1. كبس الصوت

في هذا البحث تم استخدام خوارزمية (A-law PCM) في كبس بيانات الصوت تم تحويل (16 Bits) للعينة الواحدة إلى (8 Bits)، متكونة من ثلاثة أجزاء (S Exponent Mantissa)، حيث أن S تتكون من (1 Bit) أما الـ Exponent تتكون من (3 Bits) والـ Mantissa تتكون من (4 Bits)، ويتم التحويل من خلال استخدام الجدول (1)، وتتم عملية كبس الصوت ببناء جدول الكبس (A-law PCM) لجميع احتمالات العينات المسجلة.ومن ثم تبديل قيمة كل عينة مسجلة مع القيمة التي تقابلها في جدول الكبس (A-law PCM).

2. فك كبس الصوت

في عملية فك الكبس يتم تحويل العينة المستلمة المتكونة من (8 Bits) إلى (16 Bits) وذلك من خلال جدول (1) لعملية فك الكبس (A-law PCM) وهذه العملية تتم ببناء جدول فك الكبس (A-law PCM) لجميع احتمالات العينات المستلمة. وتبديل قيمة تلك العينة مع القيمة التي تقابلها في جدول فك الكبس (A-law PCM).

3. تشفير وفك تشفير الصوت

استخدم في هذا البحث ثلاث خوارزميات للتشفير وفك التشفير وهي (الخوارزمية المقترحة، AES، TDES).

4. الاختبارات الشخصية والموضوعية لقياس جودة الكلام

لغرض تقييم ومقارنة جودة الكلام المُسترجع بعد إجراء المعالجة المطلوبة تم إيجاد بعض أنواع المقاييس، التي استخدمت نوعين من الاختبارات الشخصية والموضوعية (Subjective and Objective Test)[8].

الاختبارات الشخصية

تستخدم الاختبارات الشخصية الإذن البشرية في عملية التقييم، إذ تُسَهِل هذه الاختبارات التقييم المباشر لدرجة الضوضاء الموجودة في الكلام من خلال استماع عدد من الأشخاص إلى الإشارة الأصلية والإشارة المُسترجعة ومقارنتهما معاً، وإعطاء نتائج مباشرة، ومن أشهر المقاييس التي تعمل على هذا المبدأ مقياس متوسط الآراء الشخصية (MOS: Mean Opinion Score)، الذي يحوي على خمس درجات، والمبينة في الجدول (2) [12,4].

الجدول (2) مقياس MOS لقياس جودة الكلام

النسبة	جودة الكلام	مستوى التشويه
1	ممتاز	جودة الكلام ممتازة تماثل حديث شخص مع آخر
2	جيد	الكلام يشبه الحديث في الهاتف
3	متوسط	الكلام مفهوم لكنه ليس بالجودة الممتازة
4	مقبول	يمكن فهم الكلام لكن لا يمكن معرفة المتحدث
5	رديء	لا يمكن فهم الكلام ولا معرفة المتحدث

الاختبارات الموضوعية

نظراً لطبيعة الإذن البشرية التي تجعل من عملية التمييز بين الإشارة الأصلية والمسترجعة عملية صعبة وغير موثوق بها، ولأنها لا تعطي تقييماً دقيقاً، لذلك يتم تقييم إشارة الكلام المُسترجع من الكبس بالاعتماد على طريقة موثوق بها وهي الاختبارات الموضوعية [2]. وهي طرائق رياضية تستخدم لتقييم جودة الإشارة المسترجعة، ومن أهم وأشهر طرائق الاختبارات الموضوعية هو اختبار نسبة مقطع الإشارة إلى الضوضاء
(Segmental Signal to Noise Ratio/SEGSNR) [4].

$$SEGSNR = \frac{1}{M}\sum_{m=1}^{M} 10\log_{10}\frac{\sum_{n=1}^{N}|S_{in}(n)|^2}{\sum_{n=1}^{N}|S_{out}(n)-S_{in}(n)|^2}$$

إذ أن : S_{in}: تحويل فورير للإشارة الداخلة
S_{out}: تحويل فورير للإشارة الخارجة
N:عدد عينات الكلام داخل المقطع
M: عدد المقاطع

ومن الطرائق الأخرى المستخدمة, معامل الارتباط (Correlation) هو مقياس لقوّةِ العلاقةِ بين المتغيرات العشوائية، إن معامل الارتباط بين اثنين من المتغيرات (X) و (Y) معرف كما يلي:

$$\rho (X, Y) = \text{Covariance } (X, Y) / \{\text{Variance } (X) \times \text{Variance } (Y)\}^{1/2} \quad \ldots.(3)$$

حيث إن (ρ) هو معاملُ الارتباط، وهو العدد الذي يُلخّصُ الاتجاه وقربَ العلاقاتِ الخطيّةِ بين متغيّرين. ومعامل الارتباط يُمْكِنُ أَنْ يَأْخذَ القِيَمَ بين (−1 و+1). والإشارة (+ أو −) لمعامل الارتباط تمثل اتجاه العلاقة [15,17].

النتائج

بعد تصميم النظام وإدخاله حيز التنفيذ أُستخدِم نموذج صوتي للدراسة متمثل بصوت رجل تكلم جملة تحوي على جميع أحرف اللغة العربية وهي **(خرجت مع الأُستاذ عبد الغفور في ظلمة الليل، لزيارة مصطفى حيث أن شيء من الضنك قد حل به)**، وقد تم كبس الصوت لهذه الجملة ومن ثم تشفيرها ونقلها عبر النظام المصمم وعند استلامها من الطرف الآخر تم فتح التشفير ومن ثم فتح الكبس وتمت مقارنة النتائج على ضوء ذلك.

نسبة الكبس

عملية حساب نسبة الكبس يمكن الحصول عليها كما يأتي:

نسبة الكبس = (حجم الملف بعد الكبس \ حجم الملف قبل الكبس) × 100%

وكانت نسبة الكبس الناتجة من تطبيق خوارزمية الكبس A− law PCM على نموذج الكلام السابق هي:−

$$(100\times 136) \text{ KB} \setminus 68 \text{ KB} = \%50 = 0.5 \times 100 =$$

اختبار جودة الكلام المسترجع

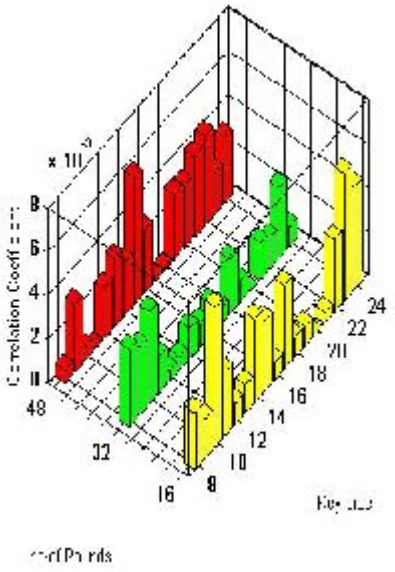
يمكن معرفة جودة الكلام الناتج من تطبيق خوارزمية الكبس A−law PCM بالاعتماد على المقاييس الشخصية والموضوعية لقياس جودة الكلام المسترجع، وقد تم أولاً تطبيق مقياس (MOS) للاختبارات الشخصية والشكل (1)يبين النتائج التي تم الحصول عليها من هذا الاختبار.

الشكل (1) قياس درجة جودة الإشارة المسترجعة باستخدام مقياس MOS

أما عند استخدام طريقة الاختبار الموضوعي لقياس جودة الكلام المسترجع فقد تم حساب قيمة SEGSNR حسب المعادلة (2) لنموذج الكلام وكانت قيمته (26.0184) وهي جيدة وكذلك تم حساب معامل الارتباط بين الإشارة الأصلية والمسترجعة حسب المعادلة (3) فان نتيجة الحساب تكون مساوية لـ(0.9074).

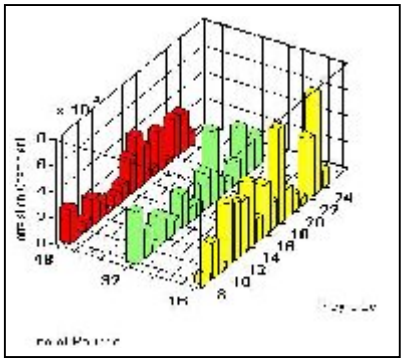
نتائج التشفير

تم تنفيذ النظام وكما تم ذكره سابقاً باستخدام ثلاث خوارزميات للتشفير فعند تطبيق خوارزمية التشفير المقترحة (المباشر والمعكوس) كانت النتائج كما في الجدول (3), حيث يوضح معامل الارتباط لنموذج الكلام الذي تم تشفيره باستخدام حجم كتلة ثابت مقداره (8,16,32 Bytes) وعدد دورات متغير ذو قيم (48،32،16) ولكل عدد دورة حجم مفتاح أولي ذو طول متغير من (8 Bytes) إلى (24 Bytes)، ويلاحظ أن معامل الارتباط يكون أقل ما يمكن عندما تكون عدد الدورات (32) لحجم كتلة (8 Bytes) ولمعظم أطوال المفتاح كما في الشكل (2). أما الشكل (3) يوضح معامل الارتباط لنموذج الكلام الذي تم تشفيره مطابقاً للنموذج السابق؛ ولكن باستخدام حجم كتلة ثابت مقداره (16 Bytes)، فقد لوحظ أن معامل الارتباط يكون أقل ما يمكن عندما يكون عدد الدورات (48) ولأكثر أطوال المفاتيح إذ أنها تصل إلى الصفر عندما يكون طول المفتاح (13) وتقترب جميع النتائج عند قيمة قليلة من معامل الارتباط عندما يكون طول المفتاح (10).



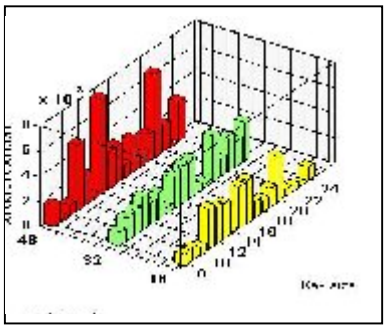
الشكل (2) قيم معامل الارتباط لخوارزمية المباشر والمعكوس لحجم كتلة (8 Bytes)

جدول(3) قيم معامل الارتباط لخوارزمية المباشروالمعكوس					
ت	عدد الدورات	حجم المفتاح الأولي	معامل الارتباط لحجم كتلة (8 (Bytes	معامل الارتباط لحجم كتلة (16 (Bytes	معامل الارتباط لحجم كتلة (32 (Bytes
1	16	8	0.0026	0.0005	0.0009
2	16	9	0.0018	0.0027	0.0010
3	16	10	0.0064	0.0005	0.0006
4	16	11	0.0029	0.0048	0.0033
5	16	12	0.0010	0.0044	0.0030
6	16	13	0.0013	0.0041	0.0028
7	16	14	0.0038	0.0050	0.0001
8	16	15	0.0032	0.0018	0.0033
9	16	16	0.0008	0.0039	0.0034
10	16	17	0.0038	0.0021	0.0013
11	16	18	0.0009	0.0073	0.0010
12	16	19	0.0009	0.0022	0.0015
13	16	20	0.0000	0.0013	0.0036
14	16	21	0.0005	0.0006	0.0006
15	16	22	0.0033	0.0047	0.0004
16	16	23	0.0058	0.0076	0.0001
17	16	24	0.0047	0.0013	0.0011
18	32	8	0.0035	0.0040	0.0011
19	32	9	0.0031	0.0022	0.0018
20	32	10	0.0042	0.0006	0.0020
21	32	11	0.0017	0.0023	0.0026
22	32	12	0.0005	0.0017	0.0017
23	32	13	0.0006	0.0010	0.0021
24	32	14	0.0014	0.0026	0.0005
25	32	15	0.0011	0.0011	0.0025
26	32	16	0.0015	0.0008	0.0030
27	32	17	0.0008	0.0028	0.0031
28	32	18	0.0025	0.0055	0.0002
29	32	19	0.0010	0.0013	0.0003
30	32	20	0.0000	0.0008	0.0037
31	32	21	0.0017	0.0017	0.0014
32	32	22	0.0014	0.0039	0.0027
33	32	23	0.0032	0.0023	0.0020
34	32	24	0.0009	0.0025	0.0031
35	48	8	0.0006	0.0026	0.0017
36	48	9	0.0031	0.0001	0.0002
37	48	10	0.0006	0.0007	0.0009
38	48	11	0.0001	0.0020	0.0052
39	48	12	0.0023	0.0015	0.0024
40	48	13	0.0031	0.0000	0.0003
41	48	14	0.0024	0.0008	0.0076
42	48	15	0.0058	0.0012	0.0030
43	48	16	0.0029	0.0028	0.0030
44	48	17	0.0002	0.0040	0.0011
45	48	18	0.0001	0.0028	0.0027
46	48	19	0.0030	0.0006	0.0010
47	48	20	0.0029	0.0030	0.0022
48	48	21	0.0037	0.0003	0.0066
49	48	22	0.0041	0.0030	0.0022
50	48	23	0.0019	0.0029	0.0000
51	48	24	0.0030	0.0010	0.0032



الشكل (3) قيم معامل الارتباط لخوارزمية المباشر والمعكوس لحجم كتلة (16 Bytes)

أما الشكل (4) يوضح معامل الارتباط لنموذج الكلام الذي تم تشفيره مطابقاً للنموذج السابق ولكن باستخدام حجم كتلة ثابت مقداره (32 Bytes)، ويبين تقارب النتائج لمعامل الارتباط بين الأشكال لعدد الدورات الثلاثة(48،32،16) واقترابها من الصفر عند نقاط عديدة، هذا مما يجعلها أفضل من سابقتيها.



الشكل (4) قيم معامل الارتباط لخوارزمية المباشر والمعكوس لحجم كتلة (32 Bytes)

مناقشة نتائج التشفير

عند تطبيق النظام باستخدام خوارزمية AES وبحجم كتلة (16 Bytes) ومفتاح طوله (32 Bytes) كانت قيمة معامل الارتباط بين الإشارة الأصلية والمشفرة هو (0.0042)، وبمقارنة هذه القيمة مع قيم معامل الارتباط المحسوبة للخوارزمية المقترحة لنفس حجم كتلة البيانات الموضحة في الجدول (3)، نجد أن هذه القيمة مقاربة لبعض قيم معامل الارتباط لعدة قيم من أحجام المفتاح الأولي، في حين نجد أن قيم معامل الارتباط للخوارزمية المقترحة اقل من هذه القيمة ومقاربة للصفر لمعظم أحجام المفتاح الأولي، وهناك قيمة لمعامل الارتباط مساوية للصفر عندما تكون عدد الدورات (48) وحجم المفتاح الأولي(13 Bytes).

أما عند تطبيق النظام باستخدام خوارزمية TDES فقد كان حجم الكتلة مساوياً (8 Bytes) وطول المفتاح (24

Bytes) ويُلاحظ أن معامل الارتباط يساوي (0.0006)، وبمقارنة هذه القيمة مع قيم معامل الارتباط المحسوبة للخوارزمية المقترحة لنفس حجم كتلة البيانات والموضحة في الجدول (3)، نجد أن هذه القيمة مقاربة لبعض قيم معامل الارتباط لعدة قيم من أحجام المفتاح الأولي، في حين نجد أن هناك قيم لمعامل الارتباط للخوارزمية المقترحة أقل من هذه القيمة ومقاربة للصفر لبعض أحجام المفتاح الأولي، وهناك قيمتين لمعامل الارتباط مساوية للصفر عندما حجم المفتاح الأولي (20 Bytes) لعدد دورات (16 و 32).

الاستنتاجات

بعد القيام بتنفيذ النظام في هذا البحث وبعد الحصول على النتائج, تم تنفيذ عملية الكبس والتشفير (On–Line). وكانت نسبة الكبس 50% وهي نسبة جيدة. وكان الكلام المُسترجع بعد عملية فك الكبس والتشفير واضح ومفهوم. اما معامل الارتباط المحسوب بين الإشارة الأصلية والإشارة المسترجعة يساوي (0.9074) وهي علاقة خطية قوية جداً، وقيمة (SEGSNR) بين الإشارة الأصلية والإشارة المسترجعة تساوي (26.0184) وهي قيمة جيدة. والتأخير عند عملية الكبس ضئيل جداً وغير مؤثر. ومعامل الارتباط لخوارزمية AES و TDES ذو قيمة جيدة. وكانت معظم قيم معامل الارتباط للخوارزمية المقترحة مُقارِبة للصفر. اما عند تنفيذ الخوارزمية المقترحة لحجم كتلة (32 Bytes) فقيم معامل الارتباط أفضل من القيم الأخرى لحجم كتلة (16 Bytes, 8Bytes). ويمكن تطبيق الخوارزمية المقترحة لأي حجم من كتل البيانات، وذلك لجعل اكبر عدد من الـ(Bytes) المتشابهة والمتتالية تملك مفاتيح مختلفة. ويمكن زيادة مقاومتها ضد محلل الشفرة بزيادة (عدد الدورات، وحجم كتلة البيانات، وحجم المفتاح الأولي)، وجعل هذه المعلومات مجهولة يؤدي إلى صعوبة حل الشفرة من قِبَل محلل الشفرة. وأي تغيير في قيمة أي Byte ضمن كتلة البيانات المشفرة لا يؤثر على باقي بيانات الكتلة.وأخيرا فإنَّ استخدام صندوق التعويض المتحرك يجعل لكل (Byte) من البيانات (16) قيمة تعويضية، وبذلك إذا تتالت كتلتان من البيانات متشابهتان فان ناتج تشفيرهما مختلف.

المصادر

[1].الغريري، شهد عبد الرحمن حسّو، 2003، "تصميم نظام حماية هجين وتطبيقه على النصوص"، رسالة ماجستير، كلية علوم الحاسبات والرياضيات، جامعة الموصل.

[2]. حليم، علياء موفق عبد المجيد، 2003، "تشفير إشارة الكلام بطريقة البعثرة"، رسالة ماجستير، كلية علوم الحاسبات والرياضيات، جامعة الموصل.

3]. قدو، سجى جاسم محمد، 2004، "كبس إشارة الكلام بواسطة استخلاص الخواص" ، رسالة ماجستير، كلية علوم الحاسبات والرياضيات، جامعة الموصل.

[4]. Ali. Dia Mohamad, 2007, "Analysis and Design of Voice over Internet Protocol (VoIP) Accelerato", PH.D. Thesis, College of Engineering, University of Mosul.

[5]. AL-SHARIF. ZIAD. A, 2005, "A High Level Audio Communications API for the Unicon Language", M.Sc. Thesis, New Mexico State University.

[6]. Arcomano. R, 2002, "VoIP Howto", General Public License, v1.7.

[7]. Brandau. Markus Albert, 2008, "Implementation of a real-time voice encryption system", M.Sc. Thesis, University of Applied Sciences Cologne.

[8]. Brokish. C. W and Lewis. M, 1997, " A-Law and mu-Law Companding Implementations Using the TMS320C54x ", Texas Instruments Incorporated.

[9]. Chisaki. Y, Morinaga. H, Kitajima. K, Koba. M and Usagawa T, 2005, "Speech encryption system with a low bit rate coding algorithm for analogue transmission line".

[10]. G. Manjunath and G. V.Anand, 2002, "Speech Encryption using Circulant Transformations", IEEE.

[11]. Gibson. J, 2005, "Speech Coding Methods, Standards, and Application", University of California, Santa Barbara, CA 93106-6065.

[12]. Katz.D, Lukasiak.T, Gentile.R and Meyer.W, 2006, "Want to know how VoIP works? Protocols, codecs, and more", www.eetindia.com.

[13]. Ken W. Li, "Correlation Analysis: Concepts & Graphical Representation",www.ictlab.tyict.vtc.edu.hk/~kenli/BDM1/Lecture/L1/ES_CO_1.pdf .

[14]. Latif. T and Malkajgiri.K, 2007, "Adoption of VoIP", M.Sc. Thesis, Luleå University of Technology.

[15]. Shen. D, Lu. Z & Pharmaceuticals. A, "Computation of Correlation Coefficient and Its Confidence Interval in SAS", Paper 170-31, www.sas.comproceedingssugi31170-31.pdf.

[16]. Tin Lai Win and Nant Christina Kyaw, 2008, "Speech Encryption and Decryption Using Linear Feedback Shift Register (LFSR)", Proceedings of World Academy of Science, Engineering and Technology, VOL.36, ISSN 2070-3740.

Scrambling for MP3 Audio",National University of Singapore.
[19] www. Wikipedia.G.711 - Wikipedia, the free encyclopedia.htm.
[20]. Yan.K, 2005, "Network Protocols Handbook", 2nd Edition, Javvin Technologies Inc, USA.
[17]. Wang. X, Chen. S and Jajodia. S, 2005, "Tracking Anonymous PeertoPeer VoIP Calls on the Internet", Alexandra, Virginia, USA.
[18]. Wei-Gang Fu, Wei-Qi Yan, Mohan S. Kankanhalli, 2005, "Progressive

Implementation of a Proposal Encryption Algorithm for Voice over Internet Protocol (VoIP)

Ahmed Yassin Kamil **Manar Y. Kashmola**

E.mail: mortadha61@yahoo.com

Abstract: The process of transfer a speech signal by high confidentially and as quickly as possible through the Internet needs to develop compression and encryption technology for a speech signal, so as, to reduce its size and make it understandable to persons not authorized to listen to. A system was designed to encrypt the voice over Internet Protocol (VoIP) and use compression technique for the purpose of reducing the size of data and send it over the network, (A_law PCM) algorithm was used the to compress audio data. Then algorithms of Triple Data Encryption Standard (TDES) and Advanced.Encryption Standard (AES) were applied. A new encryption algorithm was proposed based in its work on the block cipher encryption system called the Direct and Reverse algorithm, which based on three basic steps, firstly expand the initial key, secondly direct the encryption of each round in one direction, and finally substitute (Bytes) as used in the Compensation Box in AES algorithm by making it moving. In general compression ratio was calculated and it was (50%) and the results of the correlation coefficient for the proposed algorithm was compared with the results of (AES, TDES) algorithms.