نظام محاكاة الاشارات المشفرة في منظومة الاتصالات الجوالة GSM باستخدام طريقة التشفير القياسي للبيانات (DES)

عهود قاسم عبدالمجيد باسل جهاد عبدالله

وزارة العلوم والتكنولوجيا / دائرة تكنولوجيا الفضاء والاتصالات

بغداد – العراق

الخلاصة

ان منظومة الـ (GSM) تمثل النظام العالمي للاتصالات الجوالة وهي تعتبر من التقنيات الخلوية الأكثر شيوعا في العالم، ومن أهم الاهداف التي تسعى اليها هذه المنظومة هي ايجاد امنية عالية للبيانات المتبادلة عبرها ولذلك فهي توظف العديد من خوارزميات التشفير لهذا الغرض مثل خوارزمية A5/1، A5/2 و A5/3.

ولكن هذه الخوارزميات ليست بمستوى كاف وعال من الأمنية لهذه المنظومة، لذا فمن المستحسن ان تتم زيادة الأمنية بإضافة طرق اخرى إضافية وفي هذا البحث تم استعراض طريقة الـ (DES) التشفير القياسي للبيانات الصوتية وتعتمد هذه الطريقة بالدرجة الأساسية على القلب والتبديل العشوائي في المواقع للقنوات الصوتية المستخدمة والتي تعالج القصور الحاصل في أمنية المعلومات وتحل مشكلة الاختراق الحاصل في المرمز الصوتي والذي يستخدم النبضات الرئيسية المستثارة والتنبوء البعيد الامد (RPE–LTP) Regular Pulse Excited – Long Term prediction ان الطريقة المقترحة تحقق تشفير اتصالات امن بين نهايتين في منظومة الـ (GSM) مؤكدة توافقية عالية بين شبكات الـ (GSM)وتطبيق سهل بدون الحاجة لاستخدام او تطوير أنظمة اخرى.

الكلمات المفتاحية: خوارزمية ، تشفير قياسي للبيانات ، القنوات الصوتية ، منظومة الاتصالات الجوالة ، ترميز وتشفير .

Simulation of GSM Signal Encryption Using DES Algorithm

Uhoud Kassem Abdulmajeed Bassil Jehad Abdullah

Ministry of Science and Technology/Space and Digital Communication Directorat

Baghdad- Iraq

E-mail: uhoud@hotmail.com basil.jehad@yahoo.com

Abstract

Global System for Mobile Communications (GSM) is one of the most commonly used cellular technologies in the world. One of the objectives in mobile communication systems is the security of the exchanged data. GSM employs many cryptographic algorithms for security like A5/1, A5/2 and A5/3.

Even so, these algorithms do not provide sufficient level of security for protecting the confidentiality of GSM. Therefore, it is desirable to increase security by additional encryption methods. This paper presents the use of DES encryption method for voice encryption with Random permutation and Inversion, based on current voice channel, which overcomes data channel's insufficiencies and solves the problem of penetrating the RPE-LTP vocoder (Voice Coder) by the encrypted voice. The proposed method fulfils an end-to-end secured communication in the GSM; insure a good compatibility to all GSM networks, and easy implementation without any modification in these systems.

Keywords: Algorithm ،DES، Voice Chanel, GSM، Coding and Encryption.

المقدمة

تمثل الأمنية محورا مهما في نظم الاتصالات اللاسلكية وهذا بسبب الانتشار اللاسلكي الواسع الاستخدام كوسط ناقل والذي يجعله عرضة للهجمات أكثر من باقي الوسائط أي ان المتنصت يمكنه الحصول على ما يشاء مما يجري ارساله عبر ومن خلال الشبكة اللاسلكية إضافة الى ذلك فان الاتصالات الحالية لا يمكنها ان تعرف من هو المرسل الاصلي من المتطفل وان أي تنصت او استراق لا يمكن اكتشافه في هذا الوسط اللاسلكي مما يجعله من اسوء وسائط النقل المستخدمة.

وبالتالي فالأمن يلعب الدور المهم والأساسي في نظام الاتصالات اللاسلكية الخلوية و لتوفير امنية للبيانات في نظام الاتصالات الجوالة العالمي (GSM) فأننا نحتاج الى ميكانيكية متطورة للتشفير حيث انه في هذه الدراسة تم اقتراح نهج جديد والذي يتضمن التشفير باستخدام القلب والتبديل العشوائي (DES) .

تستخدم منظومة الـ GSM التشفير بواسطة سلسلة متدفقة من الأصفار والواحدات (Stream Cipher) والتي يتطلبها التمثيل الثنائي (Binary) وفي تقنية التشفير تعالج الرموز مباشرة دون المرور على مستوى القضمة (البت). David, *et al.*, 1994)

وبالإضافة إلى ذلك، فان هذه التقنية لا تحتاج إلى أي أجهزة وتستند كليا على البرمجيات.

هذا الأسلوب هو أبسط بكثير من التقنيات الاخرى مثل الـ RSA ، RC4 ، AES والطريقة التي اتبعت بهذه الدراسة تسمى بالقلب والتبديل أي التشفير القياسي (DES).

تم التطرق في الدراسة الى:

تعداد المتطلبات الأمنية للشبكات المحمول وإعطاء لمحة سريعة عن قائمة خوارزميات التشفير في منظومة GSM ومجموعة متنوعة من اشكال الهجمات على هذه الخوارزميات و توضيح أسلوب التشفير بين نهايتين (End to end) و نتائج المحاكاة ، وأخيرا خلاصة النقاط الرئيسية.

الجانب النظري

المتطلبات الأمنية لشبكات الهاتف النقال

اصبح من الضروري وجود دراسات تتعلق بأمنية شبكات الهاتف المحمول حيث انه كلما تطورت تلك الشبكات فأن تقنيات اختراقها ستتطور ايضا تعتبر امنية الاتصالات اللاسلكية هي مقاييس وطرق تستخدم لحماية الاتصال بين مكونين ولحماية اي من هذه المكونات من مهاجمة طرف ثالث يروم كشف هوية او اختراق المعلومات او انتحال الصفة او التنصت اذن يجب توفر ميكانيكية حماية عالية لأجل منع ذلك.

الامنية في الشبكات المحمولة واللاسلكية لها عناوين متعددة والتي تبدأ من اعطاء التراخيص لمستخدم الشبكة و انتهاء بتكامل المعلومات وتشفيرها حيث ان منظومة الـ GSM وأسوة بباقي المنظومات تحتوي على مصادر بيانات ثمينة ومتعددة والتي تحتاج الى حماية ضد الاستخدام السيئ والهجوم المقصود المتعمد .

للعناوين المدرجة ادناه اهمية قصوى في توفير درجة جيدة من الامنية لمستخدمي الشبكات اللاسلكية (GSM) وبما انه التشفير هو جزء من أمنية منظومة الاتصالات لذا يجب مراعاة تلك العناوين لغرض اكتمال الأمنية. , (Noureddine, *et al.*, 2010), (Lmai, *et al.*, 2006)

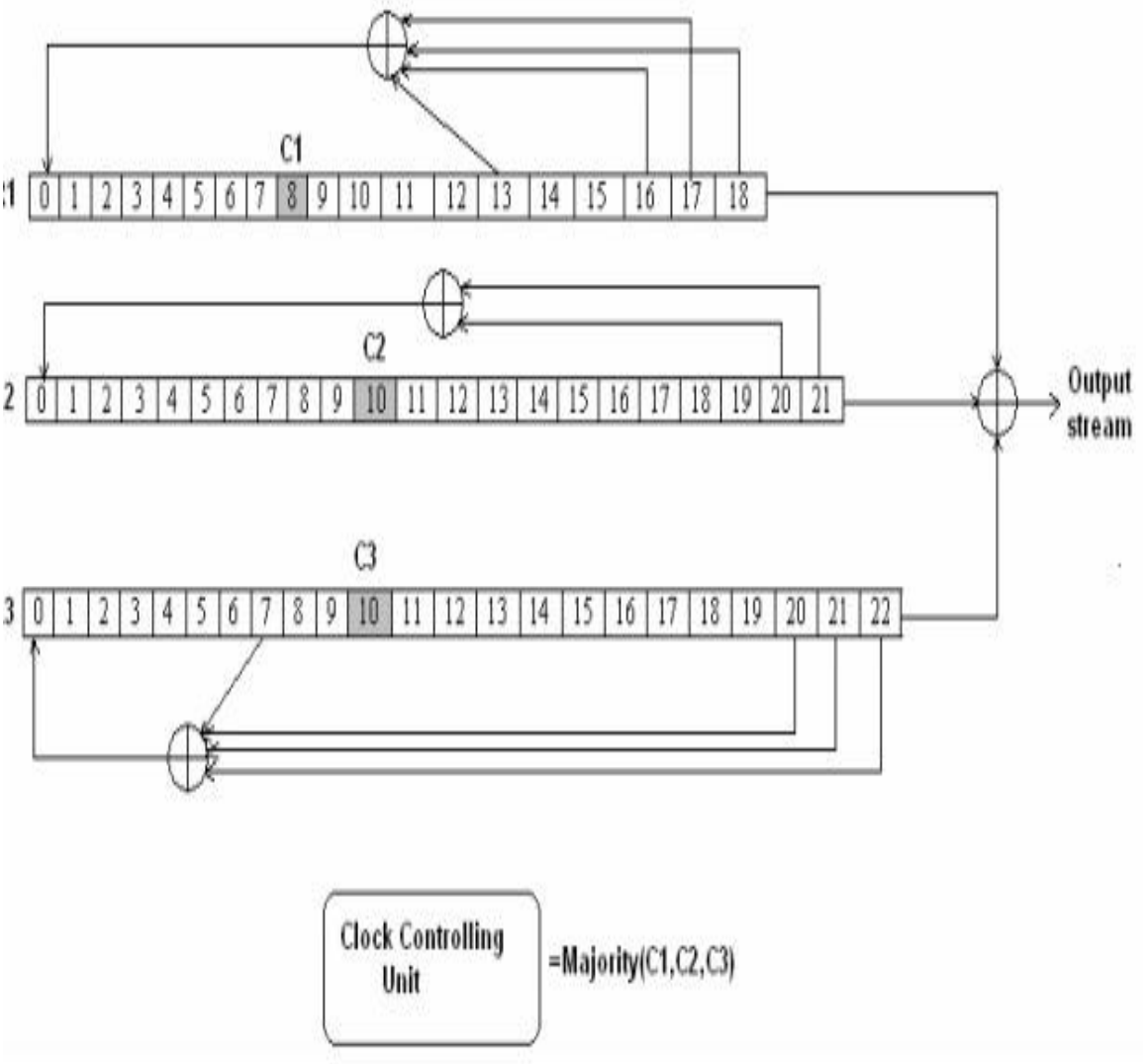
الخصوصية (Confidentiality) ، الترخيص (Authentication) ، عدم الانكار (Non repudiation) ، السيطرة على الدخول

(Access control) و الوجود المستمر للخدمة (Network Availability).

التشفير والهجمات في الـ GSM

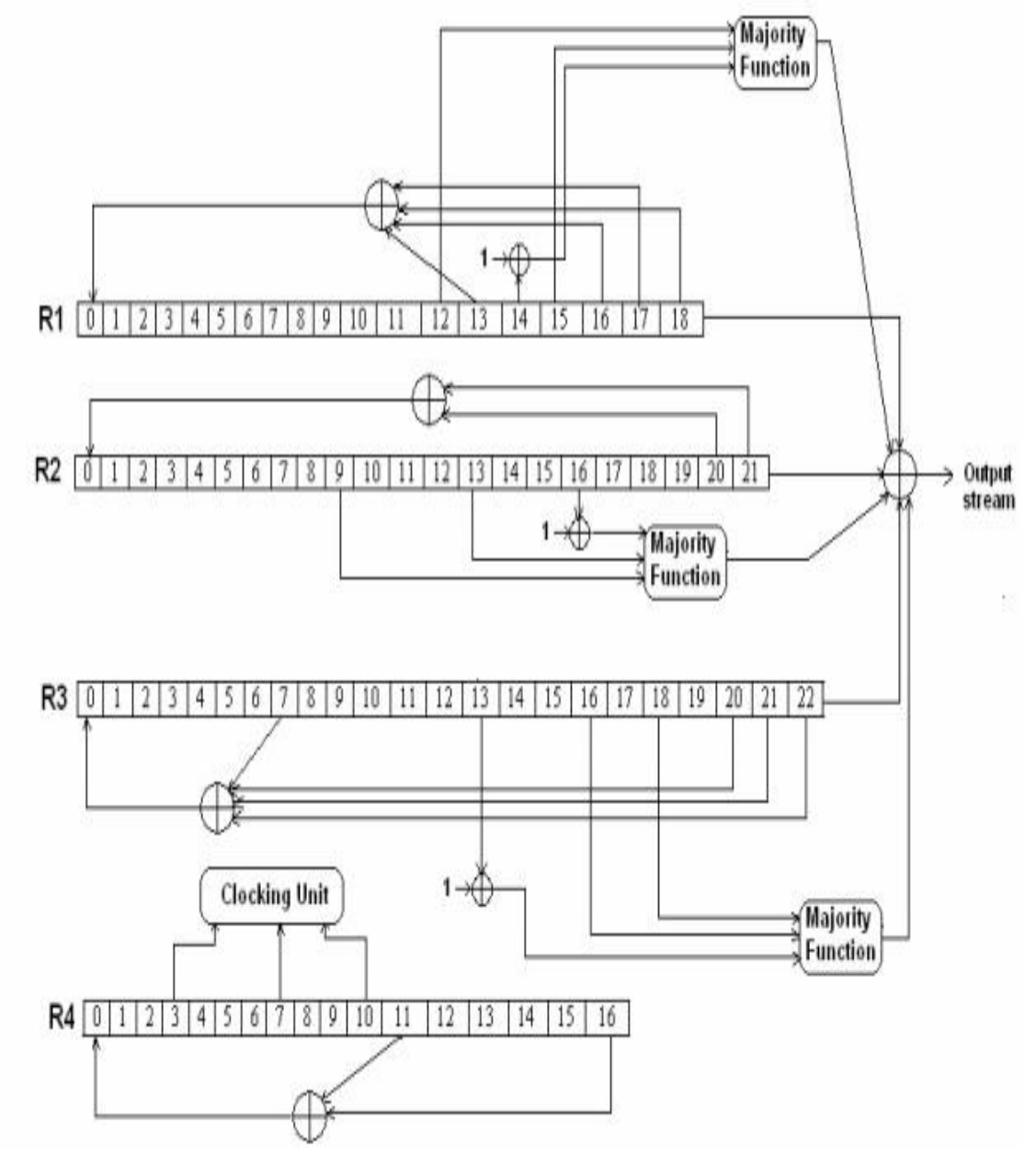
فـي منظومـة الـ GSM، تسـتخدم الخوارزميـة A5 بكل انواعها كما في الاشكال 1،2،3 أدناه.

Anderson and Mike, (1994)



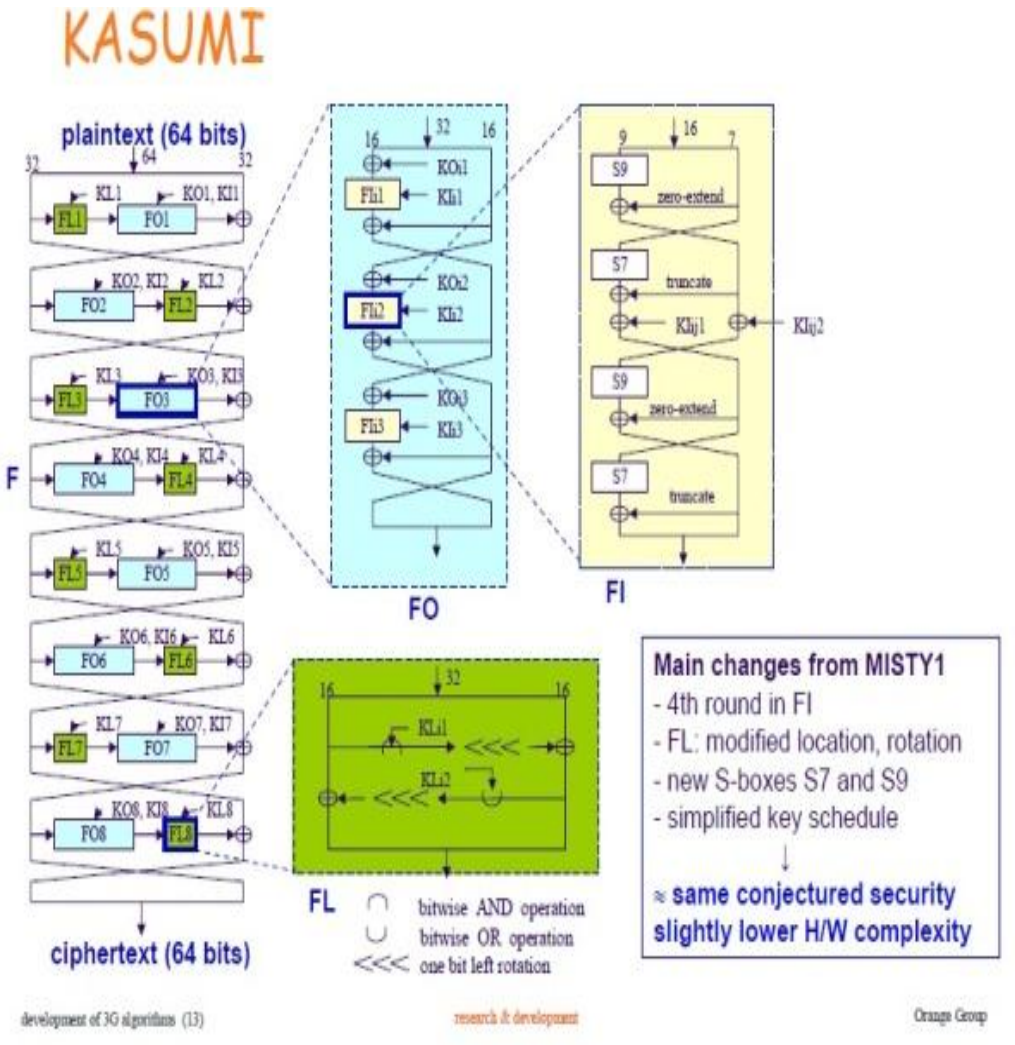
شكل(1) خوارزمية A5/1 للتشفير.

Imran and Emin, (2001)



شكل (2) خوارزمية 2/A5 للتشفير

Imran and Emin, (2001)



شكل (3) خوارزمية قاسمي 3/A5

Gandhi and Pasad, (1999)

وقد استطاع الباحث بريسينو وآخرون من كسر تلك الشفرة باستخدام الهندسة العكسية ومن ثم تم تعميمها. Siddique and Amir, (2006)

ان المشكلة الاساسية لتلك الخوارزمية هي قصر طول المفتاح و يبلغ طوله 64 بت. مع العلم ان 54 بت فقط هي الفعالة. ان المكونات المادية المتوفرة في الوقت الحاضر (HardWare) تمكن من تسجيل الرزم (Packets) بين الهاتف المتحرك ومحطة الارسال والاستقبال الرئيسية (BTS) وثم بعد ذلك فك التشفير لهذه الرزم.

Siddique and Amir, (2006)

بيريوكوف وآخرون تمكنوا من ايجاد مفتاح لمهاجمة الخوارزمية A5/1والموضحة بالشكل (1) والتي تحتاج إلى حوالي ثانيتين من وقت مفتاح السيل المتدفق من الاصفار والواحدات (Key stream) وبأمكانه ان يغطي مفتاح التشفير (Kc) بدقائق قليلة ، باركان وآخرون استطاعوا ايضا من ايجاد مفتاح جديد اخر لفك رموز النصوص المشفرة للخوارزمية A5/1 بإمكانه ان يغطي الـ (Kc) باستخدام اربعة اطارات (Frames) وكل اطار يتكون من 14 بت. اما الخوارزمية A5/2 الموضحة بالشكل (2) فأن اختراقها تم باستخدام 216 خطوة من الضربات العشوائية المزيفه.

Anderson and Mike, (1994) الخوارزمية الأمنية الجديدة، والمعروفة باسم A5/3 توفر لمستخدمي الهواتف النقالة (GSM) مستوى أعلى من الحماية ضد التنصت. ويستند A5/3على خوارزمية قاسمي (Kasumi)، التي اختصت بأنظمة الجيل الثالث من الهواتف المحمولة.

خوارزمية التشفير A5/3 خاصة بتوفر الحماية لمعلومات هامة مثل أرقام الهاتف وكذلك حماية البيانات المستخدمة لتأمين المكالمات الصوتية. وحتى الآن تعتبر هذه الخوارزمية أقوى من A5/1; و A5/2 ، ولكنها هوجمت من قبل بايهام و آخرون بدون عناء يذكر حيث تم خرق مفتاحها بسهوله.

Orr and.Nathan, (1999)

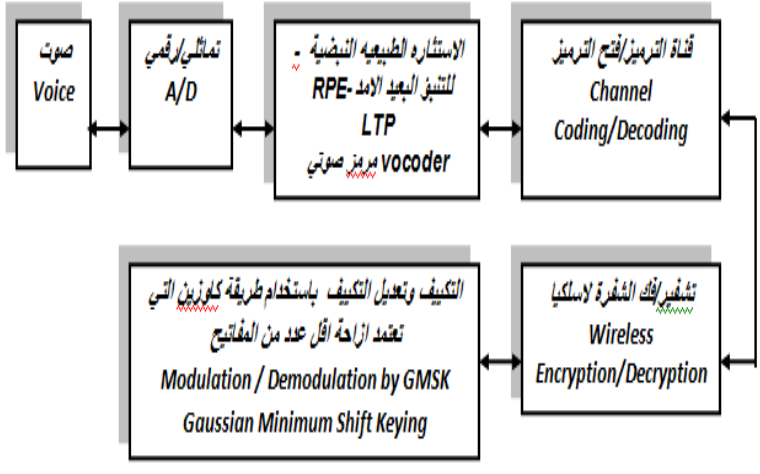
التشفير بين نهايتين End To End

نظرة سريعة على الارسال الصوتي في الـ GSM

ان عملية نقل الصوت في قنوات الـ (GSM) موضحة في الشكل (4)، و تشمل خمسة مراحل وهي:

المرحلة الأولى مرحلة التحويل التماثلي الى رقمي (Analog to Digital A/D)

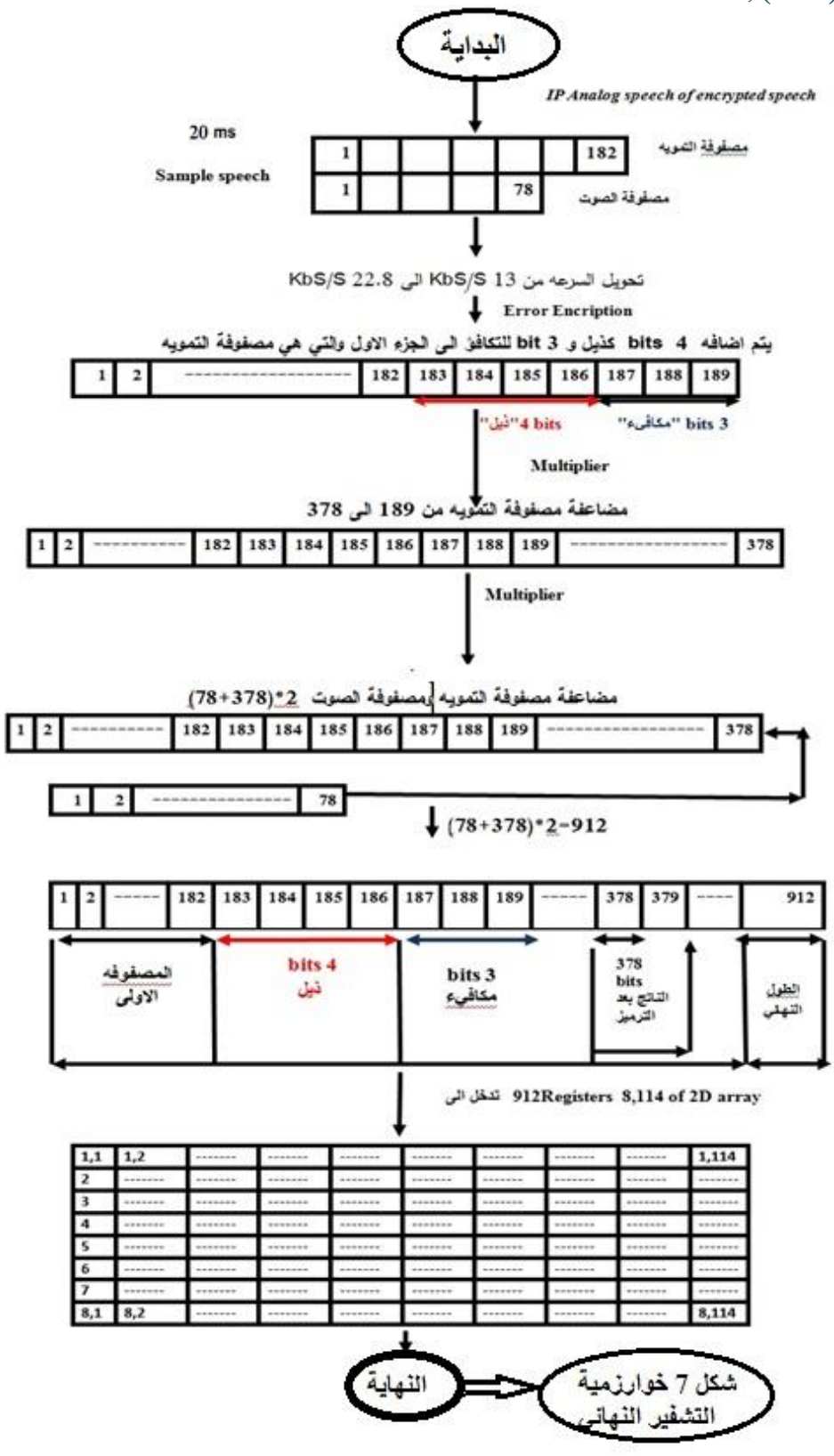
المرحلة الثانية المرمز الصوتي المسمى RPE– (Regular pulse excited–long term LTP prediction) الاستثاره الطبيعيه النبضية – للتنبؤ البعيد الامد.



شكل (4) عملية انتقال الصوت في منظومة الـ GSM

المرحلة الثالثة: ترميز / فك الترميز للقناة ، Channel Coding /Decoding موضحة بالشكل 5.

Khaled and Ouamri, (2012)



شكل (5) الترميز

المرحلة الرابعة: التشفير/ فك التشفير للاشارة اللاسلكية(Wireless Encryption/Decryption) المرحلة الخامسة: وحدة التكييف وتعديل التكييف باستخدام طريقة كاوزين (GMSK).

– التشفير/ فك التشفير يعمل فقط على وحدة قناة لاسلكية. لذلك فإنه لا يمكن توفير امنية بين نهايتين في نظام (GSM) . Khald and Ouamri, (2012)

- **نظره على طريقة ارسال الصوت في منظومة الـ GSM:**

ان المرمز الصوتي المستخدم للنبضات الاعتيادية المستثارة والتنبؤ البعيد الامد RPE–LTP) يعتبر خوارزمية هامة في مجال الترميز الصوتي، وهو لا يستخدم فقط في منظومة الأتصالات الجوالة (GSM)، ولكنه يستخدم أيضا في الإنترنت.

في مرحلة الإرسال فأن معالجة المرمز RPE–LTP) تتضمن اعادة المعالجة بشكل تحليل ترميز التنبؤ الخطي (LPC Linear Predictive Coding) ، ترشيح التحليل القصير الامد (Short Term Analysis Filtering) ، التنبوء البعيد الامد(LTP Long Term Prediction) و الترميز المرتب باستثارة النبضات الاعتيادية (Regular Pulse excitation sequence coding).هذه التفاصيل يمكن توضيحها كما يلي:

اولا: ترميز النماذج الرقمية الاصلية الاولى للاشارة الصوتية بمعدل ترميز 8 KHz، وإزاحة مركبة التيار المباشرة ثم استخدام مرشح نوعه (FIR Finite Impulse Response) مرشح وذلك لتأكيد استخدام الترددات العالية.

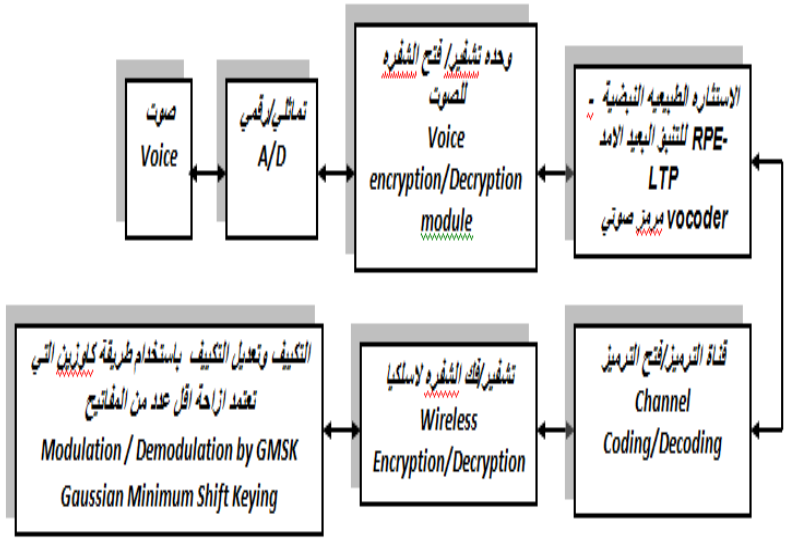
ثانيا تحليل ترميز التنبؤ الخطي (LPC Linear Predictive Coding) بحيث يأخذ 160 نموذج بوقت يعادل 20 ms ليمثل اطار(Frame) واحد

ان الترشيح باستخدام المحلل القصير الامد (Short Term Analysis) ينتج اشارة متبقية لترميز التنبؤ الخطي (LPC) Linear Predictive Coding ويزيل العشوائية عن (RPE–LTP)، ويخرج 260 بت ترميز لكل إطار في النهاية، اما في طرف الاستقبال فيتم اجراء عمليات معكوسة لإعادة استخراج الاشارة الكلامية الأصلية.

طريقة التشفير الصوتي

بشكل عام يتم وضع وحدة التشفير/ فك التشفير قبل المرمز الصوتي (RPE–LTP) ، لأنه يؤدي الى سهولة التنفيذ في النهايات الطرفية المحمولةMobile Terminal; MT . ولكن لا يمكن ان يؤمن اتصالات أمينة بين نهايتين ويحتاج الى عدة مراحل اخرى لغرض تطوير المحطة الرئيسية (Base Station (BS ، ولهذا فإننا نستخدم التشفير القياسي للبيانات (DES) في (التشفير / فك التشفير) اعتمادا على قناة الصوت وهذه الطريقه تؤمن اتصالات أمينة بين نهايتين وان المخطط المشار اليه في الشكل (6) يوضح ذلك ، يتم اضافة وحدة تشفير/فك التشفير بحيث يكون موقعها بين وحده التحويل التماثلي الى الرقمي (A/D)ووحدة المرمز (LTP – RPE).

الاشارة الصوتية القادمة من وحده A/D ستصل الى وحدة المجفر الصوتي الجديد والذي يقوم بدوره بعملية تشفيرها بعد ذلك ترسل الى المرمز (LTP–RPE) ثم يتم اختراق وحده (RPE– LTP) من قبل الاشارة المجفرة وتكون لها شدة



شكل (6) وحدة تشفير الصوت من نقطة الدخول (access point) حيث بداية تدفق البيانات في الطرف المحمول

تشفير مثاليه وفي نفس الوقت فان هذه الاشارة المشفرة يمكن ان تسترد لتعطي كلام مفهوم واضح بطرف المستقبل. هذه الطريقة من تشفير الصوت هي نوع من انواع التشفير لمصادر الاشارة التي مكن ان تؤمن اتصال امين ومضمون بين نهايتين.

الجانب العملي

خوارزمية التشفير

مبدأ خوارزمية التشفير موضح بالمخطط الانسيابي للتشفير النهائي والموضح بالشكل (7) ولتنفيذ خوارزمية التشفير، علينا متابعة الخطوات التالية:

تحلل الاشارة الكلامية الى اكثر من اطار (Frame)، وكل اطار يعطى رقم كمفتاح تسلسلي يشير له.

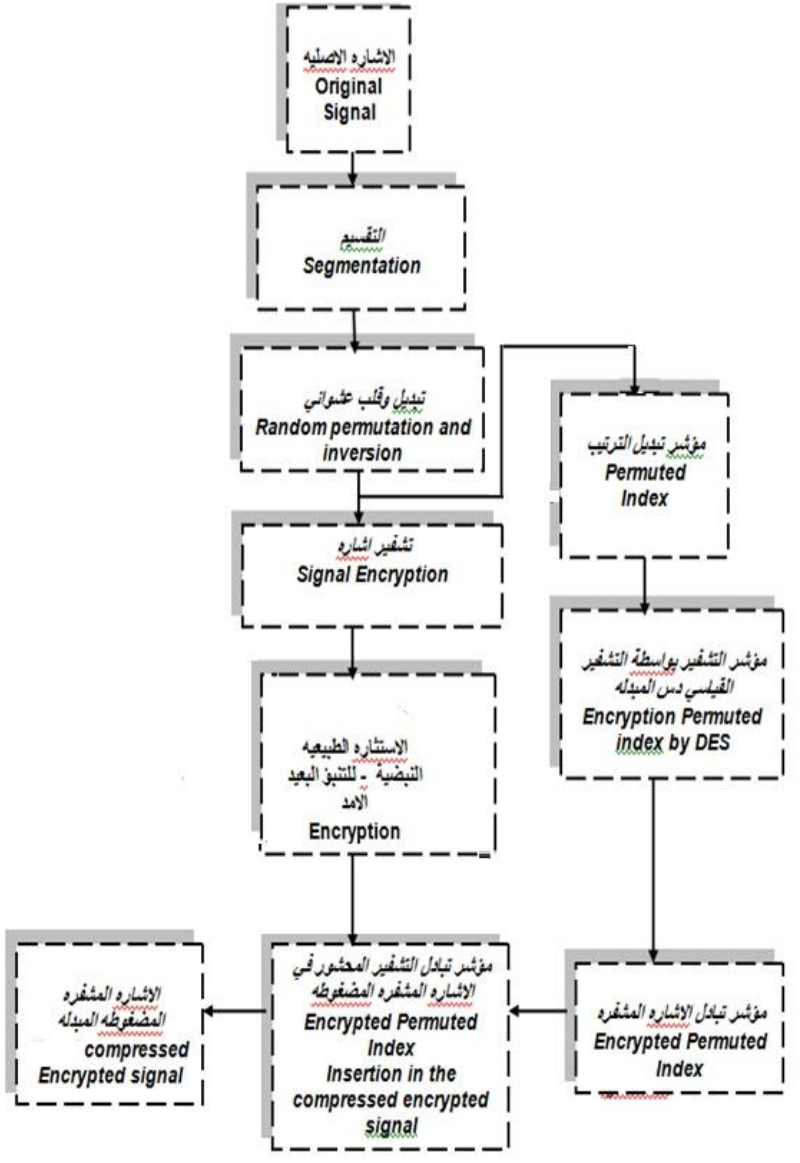
تشفير البيانات باجراء القلب والتبديل العشوائي باستخدام خوارزمية القلب والتبديل العشوائي والتي تشير الى تبديل المفتاح.

تشفير هذه الفهارس (المفاتيح المتسلسلة) باستخدام خوارزمية (DES).

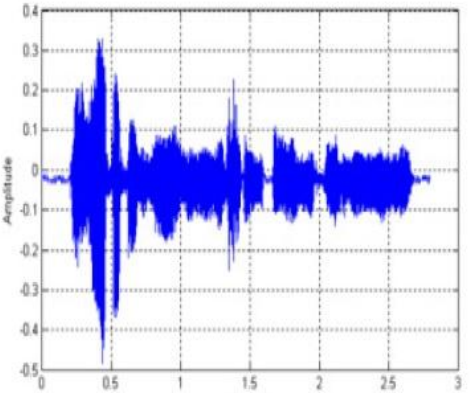
تستخدم هذه الفهارس لفك تشفير الاشارة.في هذه الدراسة، ثم اقتراح خوارزمية تقوم بعملية الجمع بين التبديل والقلب لنماذج الاشارة الصوتية معطية نتائج لها فهارس بشكل مفاتيح متسلسلة. هذه المفاتيح تمت معالجتها من قبل خوارزمية الـ (DES) وهذه المفاتيح المشفرة المبدلة تتم اضافتها الى نماذج الاشارة الكلامية المضغوطة والمشفرة بعد وحدة الـ (RPE–LTP) ولهذا فالاشارة الخارجة مشفرة بشكل جيد يغطي حاجة الطلب. الخوارزمية المستخدمة يجب ان تكون لها القابليه على جعل اشارة الصوت المشفر مشابهة لإشارة الصوت البشري الطبيعي، ويمكن لها ان تدخل المرمز الصوتي (RPE–LTP)، ومن ثم يمكن أن تنفذ عملية فك التشفير. (انظر الشكل 7).

نتائج المحاكاة

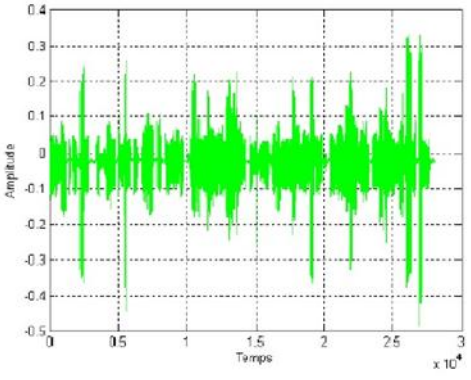
يعرض هذا القسم نتائج الطريقة المقترحة المعتمدة في قسم التشفير والهجمات في الـ GSM. هذا القسم أيضا يناقش النتائج التي تم الحصول عليها من تنفيذ النظام. ومن أجل تنفيذ مثل هذا النظام، يجب علينا أن نتبع عدة خطوات والتي وصفت بالتفصيل في الاقسام السابقة. ان نتائج المحاكاة تم الحصول عليها عن طريق الـ MATLAB وقد قسمت الى 3 مراحل هي (أ، ب، ج) و كما موضحة في الاشكال (8،9 و10)



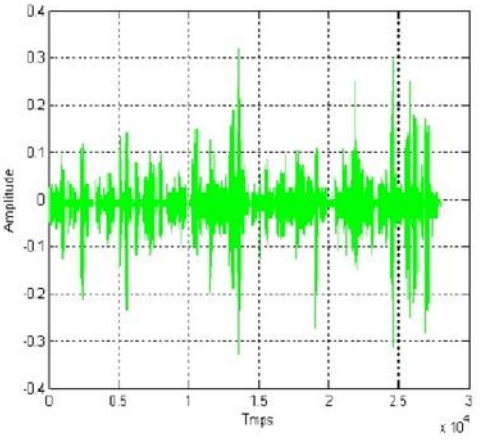
شكل (7) المخطط الانسيابي لعملية التشفير النهائي



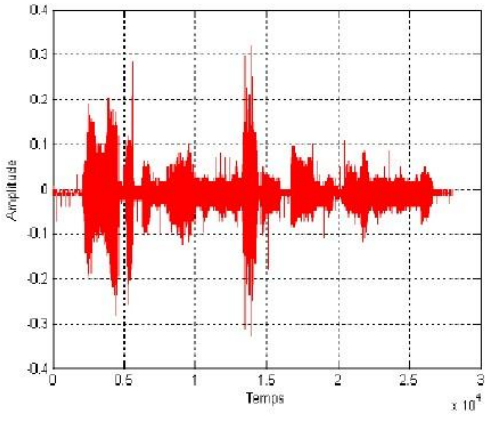
شكل (8) مخطط 1-أ) الاشارة الاصلية المؤقتة Original temporal signal



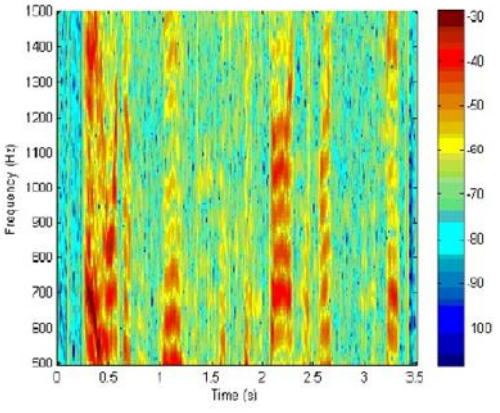
شكل (8) مخطط (2-أ) الاشارة المشفرة المؤقتة قبل الترميز Encrypted temporal signal before LPC



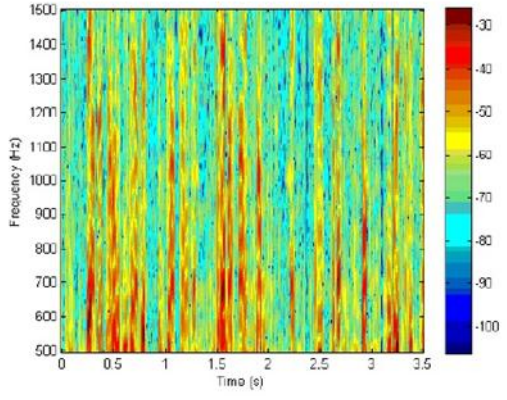
شكل (8) مخطط (3-أ) الاشارة المشفرة المؤقتة المركبة ترترديا Synthesized encrypted temporal



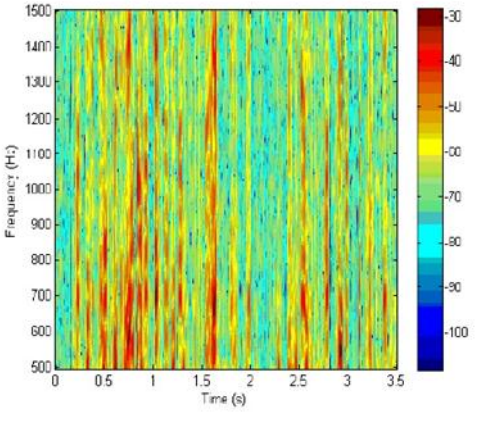
شكل (8) مخطط (4-أ) الاشارة المؤقتة المركبة ترترديا بعد فتح الشفرة Synthesized deciphered temporal



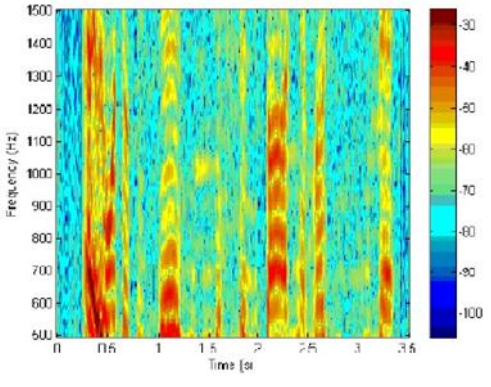
شكل (9) مخطط (1-ب) الشكل الطيفي للاشارة الأصلية Spectrogram of original Signal



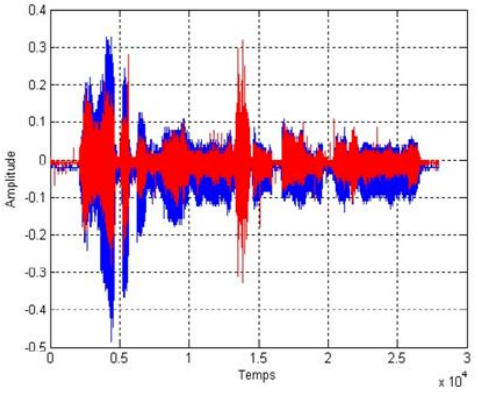
شكل (9) مخطط (2-ب) الشكل الطيفي للاشارة المشفرة قبل الترميز الخطي Spectrogram of encrypted signal before LPC



شكل (9) مخطط (3-ب) الشكل الطيفي للاشارة المشفرة المركبة ترديديا Spectrogram of Synthesized Encrypted Signal



شكل (9) مخطط (4-ب) الشكل الطيفي للاشارة المركبة ترديديا بعد فتح الشفرة Spectrogram of Synthesized Deciphered Signal



شكل (10) مخطط (ج) مقارنة بين الاشارة الاصلية والاشارة المركبة ترديديا Comparison between the Original Signal and the Synthesized Signal

في هذا الشكل يظهر لنا وجود فرق في معدل القضمة (Bit Rate) بين الاشارة الاصلية الزرقاء والاشارة المركبة الحمراء وهذا النقص سببه دخول الاشارة الى وحدة المرمز (RPE–LTP).

الأستنتاجات والتوصيات

ان هذه الطريقة الجديدة في التشفير تحل مشكلة عدم امكانية تشفير الاشارة مباشرة باستخدام خوارزميات التشفير التقليدية ، اضافة الى ذلك فأن هذه الطريقة قد جعلت من المرمز (RPE–LTP) يعطينا اشارة متوافقة مع اشارات شبكات الـ (GSM) كما تعطينا تنفيذ وتطبيق ملائم دون الحاجة الى اجراء ضبط نظام الاشارة في منظومة الـ GSM الحالية.

الخوارزمية المقدمة في هذه الدراسة استندت على خوارزمية الـ (DES) ولكن بالامكان اجرائها ايضا بواسطة طرق اخرى مثل الـ (RC4) و (AES) و (RSA) والتي تستخدم مفتاحين.

Refrences

Anderson,R. and Mike, Roe.(1994), A5 - The GSM Encryption Algorithm" http://academicpublishingplatforms.com/downloads/pdfs/gnujet/volume1/201107241658_6-45-1-PB.pdf

David,D. , G.; Birch, W. and Ian, J., (1994) Mobile Communications Security Private or Public, June IEEE,http://ceur-ws.org/Vol-867/ProcIcwit2012.pdf

Orr and Nathan, K. (1999) ,A paractical-Time Attack on the A5/3 Cryptosystem Used in Third Generation GSM Telephony, http://eprint.iacr.org/2010/013.pdf

ETSI, (1999) Speech Processing Functions General Description, Draft ETSI EN 300 961 (V8.0.1) (2000-07), European Standard (Telecommunications Series), Digital Cellular Telecommunications System (Phase 2+); Full Rate Speech; Trans Coding, (GSM 06.10 Version 8.0.1 Release), Version 8.0.1, (22-53), http://www.etsi.org/deliver/etsi_en/300900_300999/300961/08.00.01_40/en_300961v080001o.pdf

Gandhi, D. and Pasad, R.(1999) ,Kasumi Block Cipher,Data Encryptors, http://www.cs.rit.edu/~ark/spring2012/482/team/g1/presentation1.pdf

Hellwig,K.;Vary. and Massaloux, D., (1989), Speech Codec for the European Mobile Radio System.IEEE Global Commu Conf,25(3), l065-1069.

Imran, E. and Emin, A., (2001), **A** Modified Stream Genereator for The GSM Encryption Algorithms A5/1 and A5/2,http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.103.9435 and rep=rep1 and type=pdf

Imai, H.;Rahman,M. G. and Kobara, K., ,(2006) Wireless Communications Security" ARTECH HOUSE, 5 (6), 122-131.

Khaled, M. and Ouamri,A. , (2012) Securing Speech in GSM Net Work Using DES with Random Permutation and Inversion Algorithm, IJDPS International Journal of Distributed and Parallel System , 3 (4), 301-309,http://ijltet.org/wp-content/uploads/2013/04/40.pdf

Merite,K. and Ouamri,A.,(2012), Securing Speech in GSM Networks Using DES. International Journal of Distributed and Parallel Systems (IJDPS), 3 (4), 80-89.

Noureddine, B., (2010), "Wireless Communications", by Taylor and Francis Group, Security, CRC LLC, Siddique, S.M. and Amir, M., (2006) (SNPD'06), "GSM Security Issues and Challenges", Seventh IEEE International Conference on SW., AI Networking and Parallel/Distributed Computing (SNPD'06): (413 – 418).