ADPCM Tabanlı Ses Steganografi Uygulaması
The Application of Sound Steganography Based on ADPCM

*[1]Ahmet Karaca, [1]Özdemir Çetin ve [1]Halil İbrahim Eskikurt
*[1]Teknoloji Fakültesi, Elektrik-Elektronik Mühendisliği Bölümü, Sakarya Üniversitesi, Türkiye

Özet:

Günümüzde haberleşme teknolojileri hızla gelişmekte ve güvenli iletişim önemli bir kavram olarak ortaya çıkmaktadır. Güvenli iletişim için kullanılan çeşitli yöntemlerden biride steganografidir. Bu çalışmada ADPCM (Adaptive Differantial Pulse Code Modulation) ses kodlama algoritması kullanılarak kodlanmış ses sinyali üzerinde steganografi uygulaması yapılmaktadır. Gerçeklenen steganografi sistemi gerçek zamanlı olarak C8051F120 mikrodenetleyicisi üzerinde çalıştırılmış ve sonuçları bilgisayara aktarılarak performans incelemesi yapılmıştır. Bilgisayar ortamında tasarlanan arayüz ile orijinal sinyal ile veri gömülmüş sinyal incelenerek sinyaldeki bozulma oranları tespit edilmiştir.

Anahtar Kelimeler: Güvenli konuşma, Güvenli iletişim, Steganografi, ADPCM, SNR

Abstract:

At the present time, communication technologies are rapidly developing and secure communication arises as an important concern. One of the widespread methods used in the secure communication is steganography. In this study, a performance analysis application of the steganography using ADPCM (Adaptive Differential Pulse Code Modulation) on the voice signal is presented. Implemented steganography system is executed on C8051F120 microcontroller in real time and then the results are transferred to computer for performance analysis. Signal distortion ratios of data embedded signal and the original signal is determined via a graphical user interface which was developed for this purpose.

Key words: Secure speech, secure communication, steganography, ADPCM, SNR

1. Giriş

Bilişim teknolojilerinin hızla geliştiği günümüzde bireyler veya kurumlar arasında güvenli haberleşme araştırmacıların üzerinde durduğu önemli bir konu haline gelmiştir. Günümüzde ses, veri, görüntü şifreleme ve veri gömme ile bilgi güvenliği üzerine birçok çalışma yapılmıştır.[1-8] Geliştirilen bütün bu tekniklere bakıldığında en önemli amacın haberleşme mahremiyetinin sağlanması olduğu görülmektedir. Örneğin, günümüzde hayatın önemli bir parçası haline gelmiş olan sesli haberleşme imkânı sayesinde insanlar özel görüşmelerinden bankacılık işlemlerine kadar birçok önemli işlerini bu iletişim kaynaklarını kullanarak gerçekleştirmektedirler. Bu nedenle iletişim ortamlarının güvenirliliğinin sürekli sağlanması önemli bir konudur.

Bu çalışmada ses kodlama yöntemlerinden birisisi olan ADPCM algoritması kullanılarak kodlanmış ses sinyali üzerinde steganografi uygulaması yapılmıştır. Yapılan uygulamada C8051F120 mikrodenetleyicisi kullanılmıştır. Ses kodlama ve steganografi algoritmaları C8051F120 mikrodenetleyicisi üzerinde çalıştırılmıştır. Steganografi işleminin ses sinyali üzerinde oluşturduğu bozulmaları test etmek amacıyla bilgisayar ortamında bir arayüz kullanılmıştır.

*İletişim yazarı: Adres: Teknoloji Fakültesi, Elektrik-Elektronik Mühendisliği Bölümü, Sakarya Üniversitesi, 54187, Sakarya TÜRKİYE. E-posta adresi: akaraca@sakarya.edu.tr, Telefon: +902642956460 Fax: +902642956424

2. Materyal ve Yöntem

ADPCM algoritması yüksek işlem gücü gerektirmeyen bir algoritmadır. 16 kbps hızında çalışır ve kalite açısından da bakıldığında iyi bir ses kalitesi sağlamaktadır. ADPCM konuşma kodlama algoritmasında kodlama işlemi sırasında her bir ses örneği bağımsız olarak ele alınmaz. ADPCM kodlayıcının temel amacı giriş işaretinin ardışık iki örneği arasındaki farkı vermesidir. PCM deki gibi her bir ses örneğinin bağımsız olarak gösterilmesi yerine bir ADPCM kodlayıcı bir sonraki örnek değerinin tahmin edilmesini mümkün kılan ardışık konuşma örnekleri arasındaki yüksek benzerliğin avantajına sahiptir. Kodlama işleminde de ADPCM kodlayıcı her bir ses örneği için tahmin edilen örnek ile konuşma örneği arasındaki farkı kodlar. Bu metot konuşma sinyalinin genel kalitesini koruyarak örnek başına bitlerin sayısında azalma ile daha etkili bir sıkıştırma sağlar.

Kodlayıcı girişi X[n], ADC çıkışından alınan 16 bitlik konuşma verisidir. X[n] için izin verilen değerler aralığı 32,767 ile -32.768 dir. 16 bitlik bu değer sıkıştırma işlemi sonrasında 4 bitlik bir koda indirgenir ve 16 bitlik her bir giriş örneği için 4 bitlik bir kod elde edilmiş olur. Böylece giriş konuşma sinyali veri miktarı 4 kat azaltılmış olur. Elde edilen bu dört bitlik kod işaretli bir sayı şeklindedir. Bu kodun en yüksek değerlikli biti işaret biti olarak kullanılır ve iki ardışık konuşma örneği arasındaki farkın artı ya da eksi yönde olduğunu gösterir.

ADPCM kodlarının üzerine veri gömme işleminde kullanılması sırasında bütün kod değerlerinin kullanılması söz konusu değildir. Sıkıştırılmış kodlar ses sinyalindeki değişimleri ifade ettiği için bazı kodlar seste çok büyük değişimler meydana getirir bazı kodlar ise çok az değişim meydana getirirler. Veri gömme işlemini büyük değişimler meydana getiren kodlar üzerinde yapmak ses sinyalinin bozulmasına neden olacaktır. Bu nedenle veri gömme işlemi için ses sinyalinde en az değişim meydana getiren kodlar seçilerek veri gömme işlemi bu kodlar üzerinde yapılmalıdır. ADPCM kodlayıcıda ses sinyalindeki değişimler iki parametre ile belirlenir. Bunlardan birincisi ADPCM kodu, ikincisi ise algoritma içinde kullanılan adım büyüklüğü değeridir. Sesteki değişimin en az olduğu durumda adım büyüklüğü 7 değerini, kod değişkeni ise 0 yada 8 değerini alır. Tabii bu durum gürültüsüz ortamlarda söz konusudur gürültülü ortamlarda ise gürültüden dolayı bu değerlerin oluşması söz konusu değildir. Gürültülü bir ortam için bu işlem yapılacaksa belli bir eşik değeri belirlenmeli ve bunun altındaki değerlere veri gömme işlemi uygulanmalıdır. Naofumi Aoki tarafından yapılan çalışmada LSB tekniği ile veri gömme işlemi yapmak için aşağıdaki kod kullanılmıştır[1].

```
if (      s == 7  &&      (c & 0x7) == 0 )
          {
                    if (b == 0) c &= 0x7;
                    if (b == 1) c |= 0x8;
          }
```

Yukarıdaki verilen veri gömme kodunda ‘s’ değişkeni adım büyüklüğünü ‘c’ değişkeni ADPCM kodunu göstermektedir. Burada istenen şart adım büyüklüğü yani ‘s’ değişkeninin minimum olması, kod değişkeninin de yani ‘c’ nin en az değişime neden kod olmasıdır. Buda kod değişkenini 0 ya da 8 değerini aldığı durumlardır. Daha sonra tespit edilen bu değerlerin işaret değerini gösteren en yüksek değerlikli biti değiştirilerek veri gömme işlemi gerçekleştirilecektir. ‘b’ değişkeni yani gömülmek istenen veri bitleri eğer ‘0’ değerinde ise en yüksek değerlikli bit sıfıra kurulacak , ‘1’ değerinde ise en yüksek değerlikli bit bire kurulacaktır. Veri çıkartım işleminde ise tekrar kod değişkeninin 0 ya da 8 değerini aldığı durumlar tespit edilir ve en yüksek değerlikli biti olan işaret bitinin aldığı değerler toplanarak veri tekrar elde edilir.

Naofumi Aoki tarafından yapılan çalışma kayıpsız veri gömme işlemini yaparak sinyal üzerinde herhangi bir bozulma meydana getirmemektedir. Ama çalışmanın sonuçlarında gürültülü ortamlarda veri gömme işleminin gerçekleştirilemediği belirtilmiştir. Yaptığımız çalışmada ise adım büyüklüğü değiştirilerek sinyalde bozulma olsada veri gömme işlemi gerçekleştirilmiştir ve gömülen veri miktarına bağlı olarak ses sinyalindeki bozulmalar tespit edilmiştir.

$$SNR = 10log_{10}\left(\frac{\sum_{n=0}^{N} x[n]^2}{\sum_{n=0}^{N}(x[n]^2 - y[n]^2)}\right) \quad (1)$$

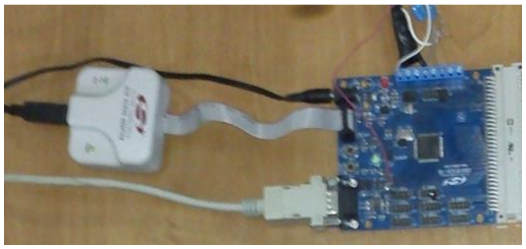
Ses sinyalindeki bozulmaları tespit edebilmek için veri gömme işleminden önceki ve sonrakı ses sinyalinin sinyal gürültü oranı (signal-to-noise ratio, SNR) Denklem 1 de verilen formül ile hesaplanmıştır. Sinyal gürültü oranı PCM ve ADPCM gibi dalga biçimi (waveform) kodlayıcı algoritmaların kalitesini değerlendirmek için sık tercih edilen bir yöntemdir[2]. Orijinal ses sinyali x[n] ile kod çözücü çıkışındaki ses sinyali de y[n] ile verilmiş olsun. SNR aşağıdaki formülle tanımlanır. Burada n ölçüm aralığını kapsayan zaman indeksidir. Hesaplanan SNR değeri desibel cinsinden bir sonuç verir. Bir müzik kasetinin SNR oranı 60 db, müzik CD’sinin ise 100 db’dir.

Ses sinyali üzerinde veri gömme işleminden dolayı oluşacak bozulmaları ve uygun veri gömme miktarını belirlemek amacıyla bir test düzeneği kurulmuştur. Test düzeneği Şekil 1 deki C8051F120DK geliştirme kartı ve Şekil 2 deki bilgisayar ortamındaki arayüzden oluşmaktadır.

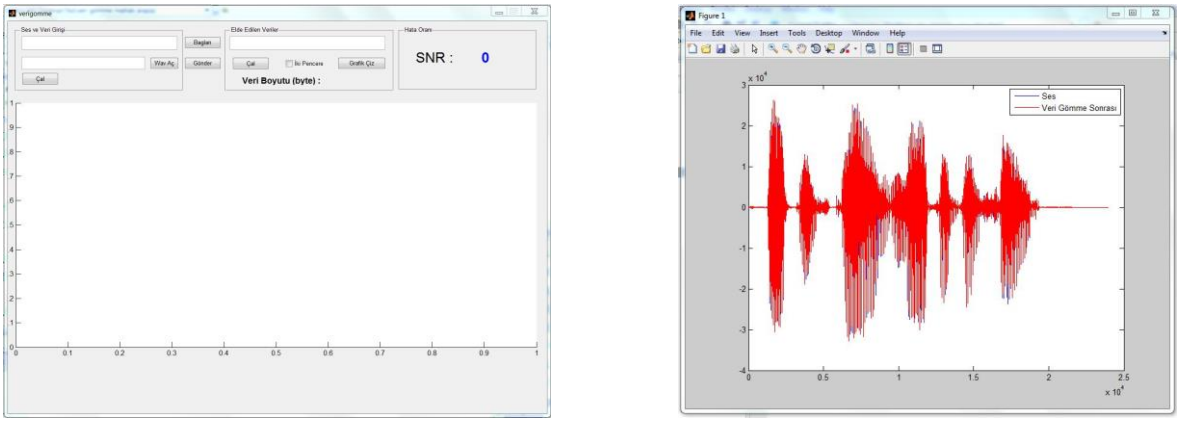
Bu test düzeneği geliştirme kartının RS232 portu aracılığıyla bilgisayara bağlanması ile oluşturulmuştur. Geliştirme kartı içerisinde ADPCM kodlayıcı ve kod çözücü, veri gömme ve veri çıkartma programları ile birlikte çalıştırılmaktadır. Bilgisayar ortamında oluşturulmuş bir arayüz sayesinde önce veri gömme işleminde kullanılacak metin RS232 bağlantısı üzerinden geliştirme kartına aktarılır ve bir dizide tutulur. Ardından ses dosyasının ilk örneği olan 16 bitlik sayı geliştirme kartına aktarılır ve bu sayı ADPCM kodlayıcı tarafından kodlanır. Elde edilen ADPCM kodunun veri gömme işlemi için uygun olup olmadığı araştırılır ve eğer uygun ise 1 bitlik veri gömme işlemi gerçekleştirilir. Sonrasında da işlemler tersine yapılarak önce veri çıkartma işlemi yapılır ve çıkartılan veriler bir dizide biriktirilir. Son olarak da ADPCM kod

çözücüye uygulanan bu kod tekrar ses sinyaline çevrilerek RS232 üzerinden bilgisayara gönderilir.

Ses dosyasının tamamı geliştirme kartında işlendikten sonra dizide saklanan ADPCM kodu içerisinden çıkartılan veriler ve gömülen veri miktarı yine bilgisayara aktarılır. Bilgisayardaki arayüzde giriş ses sinyali ve veri gömüldükten sonra elde edilen ses sinyallerinin grafikleri çizilir ve SNR oranı hesaplanarak hata oranı alanına yazılır. Yine çıkartılan veriler ve veri miktarı ilgili alanda gösterilir. Ayrıca her iki ses sinyali çal butonları yardımı ile dinlenerek bozulma miktarı kulaklada tespit edilebilir.



Şekil 1. C8051F120DK Geliştirme kartı

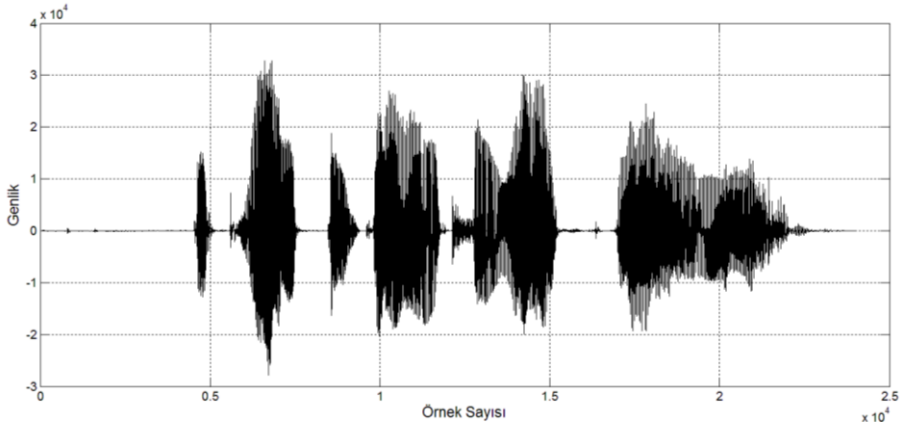


Şekil 2. Test işlemi için geliştirilen arayüz

Veri gömme sonuçlarının değerlendirilmesi amacıyla kullanılan ses dosyası Jerry D. Gibson ve arkadaşları tarafından yapılan PCM, DPCM ve ADPCM ses kodlayıcılarının performansının karşılaştırılması amacıyla yapılan çalışmada kullanılan ses dosyalarından biridir[3]. Bu dosyalar .vaw formatında kaydedilmiştir. 16 bit çözünürlüğe sahip olan bu dosyaların örnekleme frekansı 8 KHz'dir. 24000 örnekten oluşan bu dosyalar 3 sn uzunluğundadır. Veri gömme işlemi sırasında yapılan denemelerde mikrofondan alınan sinyaldeki gürültülerden dolayı veri gömme işlemi adım büyüklüğünün küçük değerlerinde mümkün olmamaktadır. Bu nedenle sistemin test edilmesi sırasında ses kayıt kalitesinden ve belirli bir uzunlukta olmasından dolayı bu dosyalar kullanılmıştır. Bu dosyalar da aşağıdaki cümle söylenmektedir.

s1.vaw dosyası: "The pipe began to rust while new." (kadın sesi)

Şekil 3 te s1.vaw dosyasına kaydedilmiş ses sinyali verilmiştir. Yatay eksen sinyalin örnek sayısını göstermektedir. 8 Khz ile örneklenen sinyal için örnek aralıkları 125µs'dir. 3 sn uzunluğundaki sinyal 24000 örnekten oluşmaktadır. Dikey eksen ise her bir ses örneğinin genliğini göstermektedir. 16 bit ile örneklenen bu sinyalde genlik değeri -32768 ile +32767 aralığındadır.

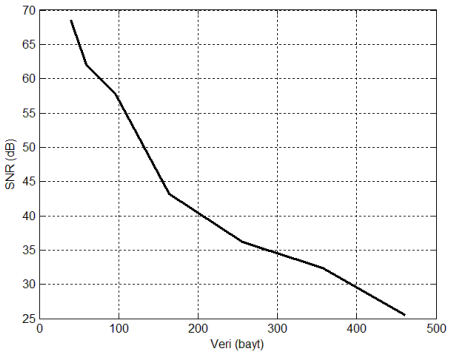


Şekil 3. s1.vaw ses dosyası

Tablo 1 de veri gömme işlemi için kullanılan adım büyüklüğünü, veri gömme miktarını ve veri gömme işlemi sonrası sinyalde meydana gelen bozulmayı göstermektedir. Adım büyüklüğü '8'den küçük olarak seçildiğinde kayıpsız veri gömme yapılmakta ve sinyal üzerinde herhangi bir bozulma meydana gelmemektedir. Bu tablodaki veriler kullanılarak Şekil 4 teki grafik elde edilir. Tablodaki değerler ve elde edilen grafik incelendiğinde gömülen veri miktarı arttığında SNR oranı belirgin bir şekilde düşmektedir. Ama 25 db de bile ses sinyalindeki bozulma kulakla anlaşılmayacak seviyededir.

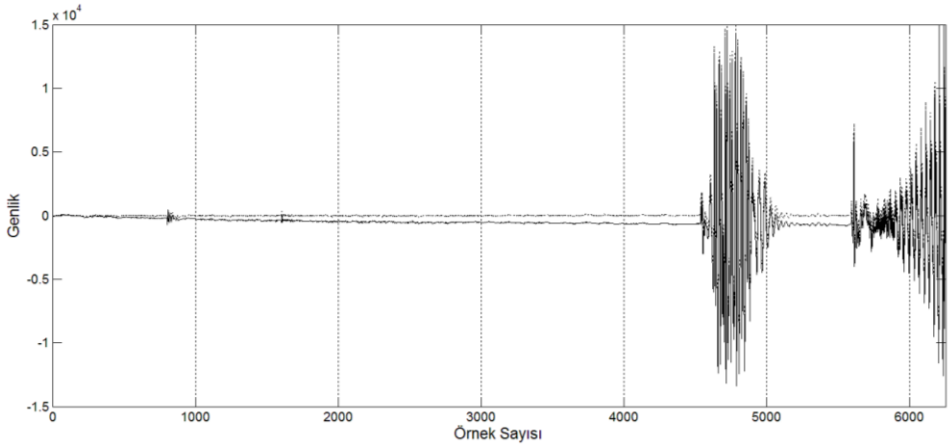
Tablo 1. s1.vaw dosyası için veri gömme işlemi sonrasında elde edilen sonuçlar

Adım büyüklüğü	Gömülen veri miktarı (byte)	SNR (dB)
8	34	Bozulma yok
10	40	68,5434
13	59	62,0479
16	97	57,6683
19	164	43,1478
25	256	36,2034
34	357	32,3691
50	461	25,4719

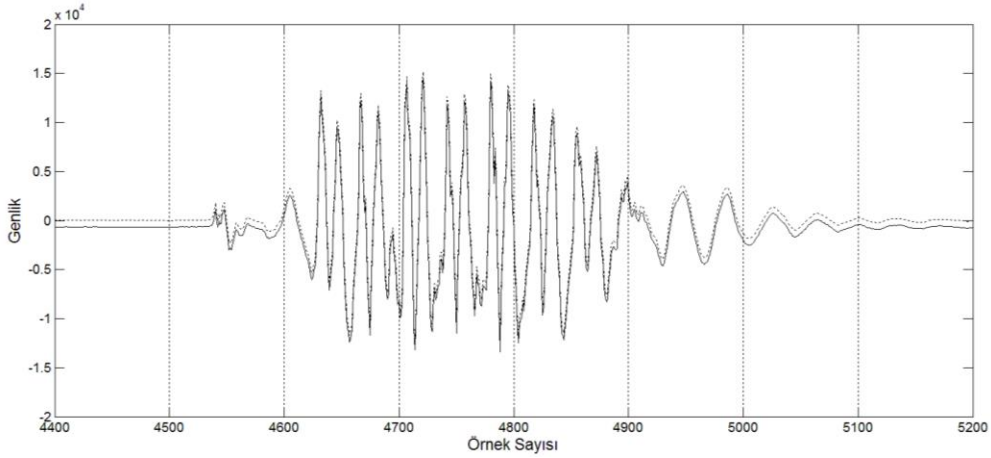


Şekil 4. s1.vaw dosyası için gömülen veri miktarına bağlı olarak sinyaldeki bozulma

Şekil 5 SNR oranının en düşük olduğu deneme için sinyal üzerinde meydana gelen bozulmanın en belirgin olduğu 0 ile 6250 aralığındaki örnekleri göstermektedir. Burada kesikli çizgi giriş sinyalini, düz çizgi ise veri gömüldükten sonraki sinyali göstermektedir. Bu aralık sinyaldeki değişimin en az olduğu dolayısıyla da veri gömme işleminin en yoğun olduğu aralıktır. Şekil incelendiğinde sinyalde meydana gelen bozulma şekil bozulması değil sinyalin üzerine bir ofset geriliminin eklenmesidir. Bu durum SNR oranını belirgin bir şekilde düşürse de insan kulağının bu tür değişimlere karşı hassas olmamasından dolayı sinyaldeki bozulma dinleyerek fark edilememektedir.



Şekil 5. s1.vaw dosyası üzerinde meydana gelen bozulma



Şekil 6. s1.vaw dosyası üzerinde meydana gelen bozulma

Şekil 6 incelendiğinde veri gömme sonucu sinyal üzerinde meydana gelen bozulma etkileri daha açık bir şekilde görülmektedir. Ses sinyalinin 4400 ile 5200 örnek aralığına bakıldığında sinyalde ki değişimlerin fazla ve az olduğu alanlar birlikte görülmektedir. Değişimin az olduğu anlarda veri gömme işleminden dolayı sinyalin genliğinde bir kayma gözlenmesine rağmen sinyal şekli ve frekansta herhangi bir bozulma olmamaktadır. Değişimin çok olduğu alanlarda ise zaten veri gömme işlemi uygulanmadığı için giriş sinyali aynen takip edilmektedir.

3. Sonuç

Yapılan çalışmada ADPCM ses kodlama algoritması kullanılarak veri gömme işlemi gerçekleştirilmiştir. Geliştirilen arayüz sayesinde orijinal ses sinyali ile veri gömme işlemi uygulanmış ses sinyali arasındaki bozulmalar incelenmiştir. Ses sinyalindeki bozulmalar gömülen veri miktarına bağlı olarak sinyal gürültü oranı şeklinde verilmiştir.

Kaynaklar

[1] Aoki N., Lossless Steganography Techniques for IP Telephony Speech Taking Account of the Redundancy of Folded Binary Code, in 2009 Fifth International Joint Conference on INC, IMS and IDC, 2009, pp. 1689–1692.

[2] Chu W. C., Algorithms Speech Coding Foundation and Evolution, in John Wiley & Sons, Inc., 2003.

[3] Gibson J. D., Jones S. K., Melsa J. L., Sequentially Adaptive Prediction and Coding of Speech Signals, IEEE Transactions On Communication, vol. COM-22, 1974, pp. 1789–1797.

[4] Gopalan K. G., Benincasa D. S., Wenndt S. J., Data embedding in audio signals, 2001 IEEE Aerospace Conference Proceedings (Cat. No.01TH8542), vol. 6, pp. 2713–2720.

[5] Chen Y., Gao T. Li, D., Hu X., Zhang X., Liu J., A secure mobile communication approach based on information hiding, IEE Mobility Conference 2005. The Second International Conference on Mobile Technology, Applications and Systems, vol. 2005, no. 1, pp. 129–129, 2005.

[6] Fakhr M. W., A Novel Data Hiding Technique for Speech Signals with High Robustness, 2007 IEEE International Symposium on Signal Processing and Information Technology, pp.

379–384, 2007.
[7] Geiser B., Peter V., High Rate Data Hiding In Acelp Speech Codecs, IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP 2008., pp. 4005–4008, 2008.
[8] Dipu Kabir H. M., Alam S. B., Hardware based realtime, fast and highly secured speech communication using FPGA, 2010 IEEE International Conference on Information Theory and Information Security, pp. 452–457, Dec. 2010.