

ÜÇÜNCÜLÜK ÖDÜLÜ-1

GSM AĞI ÜZERİNDEN GÜVENLİ SES İLETİMİ

Mehmet Akif Özkan/ İTÜ Elektronik Mühendisliği

Proje Yöneticisi: Yrd. Doç. Dr. Sıddıka Berna Örs Yalçın

Mobil iletişim için küresel sistem (Global System for Mobile Communications, GSM) ile haberleşmenin yaygınlaşması hayatımızı kolaylaştırmıştır ancak çok ciddi güvenlik açıklarını da beraberinde getirmiştir. Bu çalışmada, cep telefonları ile haberleşerek GSM üzerinden yapılan görüşmelerin servis sağlayıcıları dahil üçüncü kişilere karşı korunmasını sağlayacak bir sistem geliştirilmiştir.

GSM hattı, daha verimli ve kaliteli bir iletim yapabilmesi için konuşmalara karşı duyarlıdır. Ayrıca GSM hattı üzerinden konuşmanın iletilmesi için, bir takım sıkıştırma algoritmaları kullanılır. Bu sebeplerden dolayı konuşma Şifrelendikten sonra doğrudan hatta verilemez. Bu çalışmada, sayısal olarak Şifrelenen ses, tasarlanan kodlayıcı sayesinde GSM hattı tarafından bastırılmayacak konuşmalara dönüştürüldükten sonra iletilir. Ayrıca bu tezde, yeni bir yöntem olarak eğitilebilir kodlayıcı yapıları önerilmektedir.

Çalışma boyunca sayısal verinin Şifrelenmesinin sağlanması için, 128 bit gelişmiş kodlama standardı (Advanced Encryption Standard, AES) algoritması sahada programlanabilir kapı dizisi (Field Programmable Gate Array, FPGA) üzerinde gerçekleştirildi. Sayısal verilerden, bozulmadan iletebilecek konuşmaların elde edilebilmesi için gerekli özelliklere karar verildi ve istenen özelliklere ait parametreler NTIMIT ses veritabanı taranarak elde edildikten sonra LBG (Linde–Buzo–Gray algorithm) algoritması kullanılarak kod kitapları tasarlandı. Sayısal verileri, kod kitaplarını kullanarak kodlayan ve doğrusal öngörü yöntemiyle (LPC) konuşmalar sentezleyebilen bir kodlayıcı tasarlandı. Matlab ortamında tasarlanan kodlayıcı ile Şifreleme donanımı, seri port kullanılarak haberleştirildi. Cep telefonunu ifade eden 13 kbps (kilo bit per second) GSM FR (Full Rate) kodlayıcısı bilgisayar ortamında modellendi. FPGA de gerçekleştirilen Şifreleme donanımına karakter LCD (Liquid Crystal Display) bağlandı. Sonu olarak sistemin çalışır olduğu gözlemlendi.