İSTANBUL TEKNİK ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ

FPGA TABANLI ŞİFRELİ KABLOSUZ HABERLEŞME SİSTEMİ

YÜKSEK LİSANS TEZİ

Ilgaz AZ

Disiplinler Arası Programlar Anabilim Dalı

Savunma Teknolojileri Programı

OCAK 2014

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ

FPGA TABANLI ŞİFRELİ KABLOSUZ HABERLEŞME SİSTEMİ

YÜKSEK LİSANS TEZİ

Ilgaz AZ
514091033

Disiplinler Arası Programlar Anabilim Dalı

Savunma Teknolojileri Programı

Tez Danışmanı: Doç. Dr. Gökhan İNALHAN

OCAK 2014

İTÜ, Fen Bilimleri Enstitüsü'nün 514091033 numaralı Yüksek Lisans Öğrencisi **Ilgaz AZ**, ilgili yönetmeliklerin belirlediği gerekli tüm şartları yerine getirdikten sonra hazırladığı **"FPGA TABANLI ŞİFRELİ KABLOSUZ HABERLEŞME SİSTEMİ"** başlıklı tezini aşağıda imzaları olan jüri önünde başarı ile sunmuştur.

Tez Danışmanı :	**Doç. Dr. Gökhan İNALHAN** İstanbul Teknik Üniversitesi	.....
Jüri Üyeleri :	**Prof. Dr. Cingiz Hacıyev** İstanbul Teknik Üniversitesi	.....
	Doç. Dr. M. Turan SÖYLEMEZ İstanbul Teknik Üniversitesi	.....

Teslim Tarihi : **13 Aralık 2013**
Savunma Tarihi : **17 Ocak 2014**

Eşime ve aileme,

ÖNSÖZ

Tez çalışmam boyunca bana yol gösteren ve yardımlarını esirgemeyen başta değerli hocam Doç. Dr. Gökhan İNALHAN'a, Romanya'da yapılan yarışmada çalışmanın sunumunda bana katkıda bulunan sevgili arkadaşım Ali Himmet YÜCE'ye ve C# ile programlama konusundaki katkılarından dolayı sevgili arkadaşım Altan TOKSÖZ'e teşekkürlerimi borç bilirim.

Bu çalışmam esnasında bana her yönden destek olan kıymetli eşim Hatice SAR AZ'a teşekkür ederim.

Aralık 2013

Ilgaz AZ
Elektronik ve Haberleşme
Mühendisi

İÇİNDEKİLER

Sayfa

KISALTMALAR

ASIC : Application Specific Integrated Circuit
AES : Advanced Encryption Standard
COTS : Commercial Off The Shelf
DES : Data Encryption Standard
FPGA : Field Programmable Gate Array
FIPS : Federal Information Processing Standards
Flops : Floating point operation per second
Gbps : Gigabit per second
I2S : Integrated Interchip Sound
IEEE : Institute of Electrical and Electronics Engineers
Kbps : Kilobit per second
LED : Light Emitting Diode
LUT : Look-up Table
MAC : Media Access Control
MHz : Megahertz
NIST : National Institute of Standards and Technology
PC : Personel Computer
RF : Radio Ferquency
RFID : Radio Frequency Identification
SPI : Serial Peripheral Interface
UART : Universal Asynchronous Receiver and Transmitter
USB : Universal Serial Bus
VGA : Visual Graphics Array
VHDL : Very High Speed Integrated Circuit Hardware Description Language
WPAN : Wireless Personal Area Network
WLAN : Wireless Local Area Network

ÇİZELGE LİSTESİ

Sayfa

ŞEKİL LİSTESİ

Sayfa

FPGA TABANLI ŞİFRELİ KABLOSUZ HABERLEŞME SİSTEMİ

ÖZET

Önerilen sistemde, iki farklı noktada bulunan kullanıcılar arasında şifreli mesaj, resim ve ses verisi gönderip alabilen düşük güçlü ve maliyet-etkin FPGA tabanlı kablosuz haberleşme sistemi tasarımı yapılmıştır. Kullanıcılar, donanım tabanlı sistemleri sayesinde birbirleri arasında ister şifreli ister şifresiz haberleşme kanalı üzerinden veri alış-verişi yapabilmektedir. Şifreli kanal seçimi kullanıcı tarafından arayüz programı yardımıyla yapılabilmektedir.

Donanım tabanlı olan sistem, FPGA geliştirme kartı üzerine kurulmuştur. FPGA geliştirme kartı, sistemin ana kontrolcüsü olarak çalışmaktadır. Sistemde kullanılan geliştirme kartı Digilent firmasına ait Nexys-2 modelindeki karttır.

Sistemde kablosuz haberleşme, ses örnekleme ve ses çıktısı üretme işlemleri çevresel birim kartlarıyla gerçekleştirilmektedir. FPGA geliştirme kartına bağlanabilen çevresel birim kartları, IEEE 802.15.4 kablosuz haberleşme standardını gerçekleme, ses girdisi alma ve ses çıktısı üretme işlevlerini yerine getirmektedir. Mesaj ve resim verileri bilgisayar ortamında C# programlama dili kullanarak oluşturulan arayüz üzerinden girilebilmektedir. Kullanıcı arayüz programı ile FPGA kartı UART seri arayüz protokolü ile haberleşmektedir.

Sistemde kullanılan şifreleme algoritması AES-128 simetrik blok şifreleme algoritmasıdır. Algoritmanın hem şifreleme hem de şifre çözme adımları FPGA üzerinde gerçeklenmiştir.

Sistemin yazılımsal altyapısı FPGA üzerinde VHDL kullanarak oluşturulmuştur. Şifre ve şifre çözme algoritmaları, kablosuz haberleşme, UART arayüzü, ses örnekleme ve ses çıkış ana kontrol ve alt birim yazılım modülleri VHDL kullanarak oluşturulmuştur.

Sistemin yazılımsal tasarımında, sistemi kontrol eden yapılar en küçük işlevsel bloklara kadar ayrılmış ve tasarımlarında alttan-üste (bottom-up) yaklaşımı kullanılmıştır. Alt birimleri kontrol eden yazılım modülleri tasarlandıktan sonra bu modülleri üst seviyede kontrol edecek yazılım modülleri tasarlanmıştır. Bu sayede, hata ayıklama işlemleri kolaylaştırılmıştır.

Sistem testlerinde, standardın verdiği mesafelerde konumlanan iki kullanıcıya donanım birimleri kurulmuş ve donanımlar UART arayüzü üzerinden kullanıcı arayüz programına bağlanmıştır. Bilgisayarda bulunan kullanıcı arayüz programı üzerinden şifreli haberleşme işlevi aktif edilmiş ve mesaj ve resim verileri gönderilip alınmıştır. Aynı zamanda, ses giriş biriminden alınan sayısal ses verisi, karşı kullanıcıya gönderilip ses çıkışı alınmıştır. Bu özelliklerinden ötürü, tüm sistem yakın konumlanan güvenli arayüze sahip haberleşme cihazı şeklinde çalıştığı düşünülebilir.

Sistem, iki kullanıcı arasında yarı-zamanlı (half-duplex) yapıda haberleşme arayüzü sağlamaktadır ancak yazılım altyapısında kurulan mimari sayesinde kullanıcılar birbirlerine veri gönderimi yaparken herhangi bir zamansal kısıtları bulunmamaktadır. Kullanıcılar aynı anda veri gönderimi yapsalar dahi, sistem bu verileri kaydedip haberleşme kanalının boş olduğu zamanda verilerin iletimini gerçekleştirmektedir.

Sistem, yazılım teknikleri ve mimarisi sayesinde (saat darbesini gerekli zamanlarda aktif etme, aktif olmayan modülleri kapatma vb.) literatürde önerilen diğer sistem tasarımlarına göre görece düşük güç tüketimi değerlerine sahiptir. Kullanılan yazılım teknikleri sayesinde (en küçük işlevsel modüllere ayırma vb.) FPGA üzerinde az sayıda kaynak harcanarak tasarlanmaya çalışılmış ve daha ucuz FPGA yongalarıyla da bu tasarımın gerçeklenmesine çalışılmıştır.

FPGA-BASED ENCRYPTED WIRELESS COMMUNICATION SYSTEM

SUMMARY

Wireless communication is transmission method that uses electromagnetic waves, which has no physical connection between users. Most widespread used wireless communication systems are television, cellular mobile phones, radios, wireless modems, walkie-talkie and satellites. Given systems transmit or receive electromagnetic waves and render meaningful data.

Cryptography is ciphering science. It is used to prevent of using, monitoring and changing data and information. It is practice and study techniques for secure communication in the presence of third parties. More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects information security such as data confidentially, data integrity, authentication and non-repudiation. Modern cryptography intersects the disciplines of mathematics, computer science and electrical engineering. Applications of cryptography include ATM cards, computer passwords and electronic commerce.

Modern cryptography is heavily based on mathematical theory and computer science practice; cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary. It is theoretically possible to break such a system but it is infeasible to do so by any known practical means. These schemes are therefore termed computationally secure; theoretical advances, e.g., improvements in integer factorization algorithms, and faster computing technology require these solutions to be continually adapted. There exist information-theoretically secure schemes that provably cannot be broken even with unlimited computing power—an example is the one-time pad—but these schemes are more difficult to implement than the best theoretically breakable but computationally secure mechanisms.

For practical applications, implementation complexity and security level of algorithms has become increasingly important. Thus, hardware base of implementation becomes crucial. Today, cryptographic algorithms are generally implemented on Field Programmable Gate Arrays (FPGA) and Application-Specific Integrated Circuits for speed, area and power specific application fields.

One of the application fields of cryptographic algorithms are wireless communication systems. For wireless communication systems such as cellular phones, sensor networks, low-power consumption will arise as a main concern. So, it becomes important to choose right cryptographic algorithm for low power and low complexity required wireless communication applications. AES-Rijndael algorithm is good choice in terms of simplicity and high security level.

In thesis, wireless communication and cryptography topics are integrated in hardware basis. FPGA-based encrypted wireless communication system is designed for establishing secure communication link between distinctly located users. Each user is capable to transmit and receive message, image and audio data. For

communication, wireless personal area network (IEEE 802.15.4, WPAN) is preferred which is especially customized for low power applications. AES-128 algorithm is chosen for establishing data security between users.

Low power consumption, low cost design and high processing power are main concerns of implementation. To fulfill power consumption issue, WPAN protocol is chosen which designed for low power applications. In addition, software is designed by following power reduction schemes such as clock enabling, module enabling/disabling, sleeping and waking integrated circuits at relevant time. To fulfill low cost design issue, total resource usage of FPGA tries to be reduced with iterative implementations. To fulfill high processing power issue, it is followed recommended ways of software implementation in terms of parallelism of FPGA.

Hardware based system is implemented on FPGA development board. FPGA development board, which is the main controller of the system, is Nexys-2 that is produced and manufacturer by Digilent Inc.

Main functions that are implemented on Nexys-2 FPGA board is transmitting and receiving data over UART interface, controlling audio sampling module, buffering digitized audio, controlling audio reconstruction unit, sending digitized audio to reconstruction unit, encrypting and decrypting buffered data and initializing wireless communication module and handling transceiving function of communication module.

Proposed system is able to transmit and receive message, image and audio. For given purposes, peripheral boards are plugged to FPGA development board. These boards are PmodRF2, PmodMIC and PmodI2S that are designed and manufactured as COTS products by Digilent Inc. PmodRF2 is IEEE 802.15.4 WPAN Protocol board that is used for transmission and reception of data. PmodMIC is audio sampling board. It has microphone unit and digitizing IC for sampling. PmodI2S is audio reconstruction board used for creating analog audio from digital audio data.

Proposed system has two software bases, one is FPGA software and other is graphical user interface.

VHDL is hardware description language to describe logic and logical interconnection of high speed integrated circuits such as FPGA and ASIC. VHDL can also be used as a general purpose programming language.

FPGA software module designs are written with VHDL. Encryption/decryption module, UART interface module, audio controller module, wireless communication controller modules are all implemented with VHDL on FPGA. While designing given controller modules, low cost design and high processing power requirements of system are considered.

In software module design, functionality and requirements of whole system is deeply examined. After functionality of system becomes clear, it is divided into functional elementary submodules. Such submodules are responsible to implement minor functions. It is such as wireless, audio peripheral board controlling, UART communication with PC and encryption/decryption process controlling. These submodules are getting together with bottom-up design approach. By bottom-up approach and minor functionality submodule design, high processing power requirement is achieved. Given approaches makes simple and straightforward to describe desired functionality in terms of VHDL statements. Additionally, debugging processes becomes simpler when design has minor submodules.

System has graphical user interface to transmit and receive message and image from user's computer. There are message box that is used to write any type of message and history box that is used to monitor received message. There is selection box for image data. Any type of image can be selected from computer. User can also select to enable/disable encryption process and microphone module from GUI. GUI establishes communication link over UART interface between computer and FPGA. It is written with C# language.

System is able to transmit and receive different data types such as message, image and audio. To classify such data, data packaging protocol is implemented. Every data package has header, length of data, data and footer bytes. Thus, data types can be separated and related channeling can be provided. Message and image data can be routed to UART interface and audio data can be routed to peripheral board.

Encryption algorithm of system is symmetric-key block cipher AES-128 algorithm. Mathematical complexity of AES is suitable to implement it in hardware basis. Additionally, security level of AES is high because of consisting non-linear transformations and using long key length. AES is based on a design principle known as a substitution-permutation network, and is fast in both software and hardware. AES operates on a 4×4 column-major order matrix of bytes, termed the state, although some versions of Rijndael have a larger block size and have additional columns in the state. Most AES calculations are done in a special finite field. Algorithmic flow of AES includes; key addition, substitution of bytes, shifting rows of bytes, mixing columns of bytes. Given operations are iteratively applied on input data for several turns according to key length.

The communication link style of system is point-to-point. There are two user in system and they can communicate directly each other. The frequency of the link is 2.4GHz ISM band. In the network, one user is coordinator and other user is full-function device. Nature of WPAN link is half-duplex, one should listen when other transmits. However, software implementation of system let the users not to care about transmission time slot. Before transmission, data are buffered and if the link is idle, data is transmitted. Otherwise, system waits the link to become idle. So, system automatically listens the line and transmit data when it is idle.

In literature, cryptographic algorithm and wireless communication implementations on hardware are deeply studied. Most of studies are based on either algorithmic or wireless communication implementations. In our study, both of these topics are integrated and implemented. In addition, low power and low cost design approaches take into account in design phase. Our system gives relatively good results compared to other systems.

There are also COTS products, which are communicating over GSM and 3G band. These devices are encrypted mobile phones. They are able to be used as usual mobile phone, but they are also capable to send message and voice after encrypted. Such products are TÜBİTAK's MilCep, GMSK's CryptoPhone, Nabishi's Q8500 and Tripleton's Enigma products.

The main purpose of the system is to close the gap and be an alternative between encrypted wireless sensor networks and encrypted mobile phones.

For future works, it is planned to be communicated more users in designed system's network. Also, security level will be improved changing AES-128 to AES-256. Coverage area will be increased by changing wireless communication protocol.

Finally, all implementation will be designed on a single pcb and mind to be manufactured.

1. GİRİŞ

Kablosuz haberleşme, kullanıcılar arasında herhangi bir fiziksel bağlantı olmadan bilginin elektromanyetik dalgalarla gönderildiği iletişim yöntemidir [1]. Günümüzde en yaygın kablosuz haberleşme sistemleri, televizyonlar, cep telefonları, radyolar, kablosuz modemler, telsizler ve uydular olarak verilebilir. Bu sistemler, elektromanyetik dalgaları alarak bu dalgalardaki verileri çözümleyip bilgiyi kullanıcıya iletmektedir.

Kriptografi şifreleme bilimidir. Verilerin ve bilgilerin açık ortamlarda yetkili olmayan kişiler tarafından kullanılmasını, gözlenmesini ve değiştirilmesini engellemek amacıyla bu bilgilerin saklanmasına ve gizlenmesine yönelik yapılan işlemlerin bütünüdür [2].

Teknolojik açıdan hızla ilerleyen dünyada bilgi güvenliği, insanlığın teknolojik pencerede ilgilendiği önemli konuların başında yer almaktadır. Bu kapsamda, bilgi güvenliği konusu birçok uygulama alanına sahiptir. Bunlardan bazıları, haberleşme güvenliği, veri güvenliği ve ağ güvenliği olarak sayılabilir. Bu uygulama alanlarında verilerin gizliliği önemlidir ve bilgilerin iletilmesi, dağıtılması ve saklanması güvenli yöntemlerle gerçekleştirilmelidir.

Bu ihtiyaçları karşılamak adına geliştirilen şifreleme algoritmaları bulunmaktadır. Bu algoritmalar arasında, Joan Daemen ve Vincent Rijmen tarafından geliştirilen Rijndael [3] algoritması da bulunmaktadır. Bu algoritma, güvenlik, performans ve gerçekleme kolaylığı gibi özellikler göz önüne alınarak yapılan değerlendirmeler sonucunda Amerikan Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standards and Technology, NIST) tarafından yapılan yarışma sonrasında Gelişmiş Şifreleme Standardı (Advanced Encryption Standard, AES) olarak belirlenmiş ve Federal Bilgi İşleme Standardı (Federal Information Processing Standards (FIPS)) olarak yayımlanmıştır [4].

AES algoritması günümüzde veri şifrelemesinde en ileri düzeyde güvenlik sağlayan algoritmaların başındadır. Bilinen tüm saldırı yöntemlerine başarıyla karşı koyan bu

algoritma, şu anda birçok ülkenin veri güvenliğinde tercih ettiği algoritmalar arasında yer almaktadır.

Günümüzde şifreleme algoritmalarının farklı uygulama alanlarına yönelik tasarım önerileri, sahada programlanabilir kapı dizileri (FPGA) ve uygulamaya özel tümdevreler (ASIC) üzerinde gerçeklenerek sunulmaktadır. Düşük güç gereksinimi gerektiren kablosuz yerel alan ağları, kablosuz kişisel alan ağları ve RFID (Radio-Frequency Identification) gibi uygulamalarda güvenlik amacıyla başvurulan şifreleme algoritmalarının tasarımı önem kazanmaktadır. AES-Rijndael algoritması işlevsel açıdan kolay gerçeklenebilir olması ve yüksek güvenlik düzeyi nedeniyle bu tip uygulamalarda en çok tercih edilen şifreleme algoritmasıdır.

1.1 Tezin Kapsamı

Tez kapsamında sunulan çalışma, IEEE 802.15.4 Kablosuz Kişisel Alan Ağı (Wireless Personal Area Network, WPAN) standardı üzerinden kablosuz haberleşen iki kullanıcı arasında mesaj, resim ve ses verilerinin alış-verişini sağlayan FPGA tabanlı sistem tasarımıdır. Bu özelliğine ek olarak, verilerin güvenli şekilde iletimini sağlayabilmek amacıyla sisteme AES-128 algoritmasını kullanarak şifreleme özelliği kazandırılmıştır.

Sistem, kısıtlı kaynak kullanımı gerektiren ortamlara göre özelleştirilmeye çalışılmıştır. Düşük güç tüketimi gerektiren ortamlara uygun olması için, kablosuz haberleşme standardı düşük güç tüketimine özel geliştirilen IEEE 802.15.4 standardı kullanılmış ve tüm sistemin VHDL ile oluşturulan yazılımsal altyapısı literatürde önerilen güç tüketimini azaltan yaklaşımlarla tasarlanmıştır. Güç tasarrufu sağlamak amacıyla aktif olmayan modülleri kapatmak ve modüller aktif değilken saat darbe üreteçlerini kapatmak gibi işlemler yapılmaktadır. Ayrıca, düşük maliyetli olması için yazılım teknikleriyle ve derleyicinin sunduğu imkânlarla FPGA üzerinde harcanan kaynak miktarı azaltılmaya çalışılmıştır. Bu sayede, daha az kaynağa sahip daha ucuz FPGA yongalarıyla aynı kabiliyette sistem tasarımı gerçeklenmeye çalışılmıştır. Bu kapsamda yapılan çalışmalar ve tasarım akışları tez içeriğinde sunulmaktadır.

Literatürde, kablosuz haberleşme sistemleriyle alakalı donanım gerçeklemeleri ve AES şifreleme algoritmasıyla alakalı uygulama alanına ve bu alanlarda tercih

edilebilecek yöntemlere yönelik çalışmalar bulunmaktadır. Önerilen sistemin performans parametreleri, düşük güç tüketimi, maliyet-etkin yapısı ve donanım altyapısının yüksek hızda çalışabilmesidir. Bu performans parametreleri bazında, benzer sistemlerle olan karşılaştırmalar verilecektir. Ayrıca, sistemimizin bu çalışmalara göre getirdikleri ve üstünlüklerinden bahsedilecektir. Bunun yanı sıra, ürün haline gelmiş ve şu anda kullanılan benzer sistemlerle olan karşılaştırmaları da tez kapsamında sunulacaktır.

Bu tezde, kullanıcılar arasında güvenli haberleşme arayüzü sağlamak amacıyla donanım tabanlı veri iletimi yapan sistem tasarımının donanımsal altyapısı, yazılımsal altyapısı, kullanılan teknolojiler, izlenilen yöntemler ve literatürdeki benzer sistemlerle karşılaştırmaları verilmektedir.

1.2 Tezin Konuya Katkısı

Literatürde, genel olarak kablosuz haberleşme sistemleri üzerine çalışmalar bulunmaktadır. Gerek, standartlar bazında(WLAN, WPAN, ZigBee, Bluetooth vb.) gerekse bu standartların donanımsal gerçeklemeleri hakkında öneriler yapılmaktadır. Ayrıca, düşük güç tüketimi gerektiren ortamlar için özelleşen standartlarla ilgili (WPAN, Zigbee, Bluetooth) çalışmalar da yapılmaktadır.

AES şifreleme algoritması, literatürde fazlaca işlenen konular arasındadır. Uygulamaya yönelik olarak, düşük güç tüketimi ve düşük kaynak kullanımı gerektiren ortamlar için özelleşmiş çalışmalar yapılmaktadır. Düşük güç tüketimine yönelik uygulamalarda, algoritmanın işlevsel akışındaki veya gerçekleme yöntemlerindeki çalışmalar sunulmaktadır. Diğer çalışmalarda ise algoritmanın gerçeklenmesine yönelik alternatifler ortaya koyulmaktadır. Algoritmanın donanımsal gerçeklemeleri ise genel olarak FPGA ve ASIC yongaları üzerinde yapılan çalışmalar halinde verilmektedir.

Tezde önerilen sistem, donanım tabanlı şifreli kablosuz haberleşme sistemi tasarımıdır. Birden fazla kaynaktan gelen ve farklı formatlardaki verilerin (mesaj, resim ve ses verileri) kablosuz ağ üzerinden güvenli haberleşme arayüzü sağlayarak alış-verişini sağlamaktadır. Sistem, hem donanımsal olarak kablosuz haberleşme sistemi tasarımını hem de AES-128 algoritmasının FPGA üzerinde gerçeklenmesini kapsamaktadır. Kablosuz ağ haberleşme mekanizmasının yanı sıra, veri şifreleme ve

şifre çözme mekanizmalarını da barındırmaktadır. Donanımsal gerçeklemelerinin yanı sıra düşük güç tüketimi ve düşük kaynak kullanımına yönelik uygulamalar ve yazılım tasarımlarıyla ön plana çıkmaktadır. Bu açılardan, literatürde işlenen konular arasında sisteme özgü yapılan çalışmalarla konuya katkıda bulunmaktadır.

2. ÖNERİLEN SİSTEMİN LİTERATÜRDEKİ BENZER SİSTEMLERLE KARŞILAŞTIRILMASI

2.1 Sistemin Hedefi

Tezde önerilen FPGA tabanlı şifreli kablosuz haberleşme sisteminden, görece daha yakın konumlanmış kullanıcılar arasında düşük bant genişliğine ve veri hızlarına ihtiyaç duyan uygulamalarda maliyet-etkin bir çözüm sunması hedeflenmektedir. Önerilen sistemin, kablosuz duyarga ağları ve mobil cihaz uygulamalarının ara alternatifi olması amaçlanmaktadır. Kapsama alanı düşük uygulamalarda farklı kaynaktan gelen verilerin iletimini mümkün kılmaktadır.

Hâlihazırda var olan mobil cihazlardan başlıcaları şunlardır;

- MilCep-K1, K2 [15]
- GSMK Cryptophone [16]
- Nabishi Q8500 [17]
- Tripleton Enigma [18]
- GoldLock 3G [19]
- Snapcell-300 [20]

[15], [16], [17], [18], [19], [20] GSM bandında haberleşme yapan cep telefonlarıdır. Ses, mesaj ve dosya transferlerinin kullanıcının seçimine göre şifreli veya şifresiz olarak iletimini gerçekleştirmektedir. Verilen referanslarda, ses, mesaj ve dosya iletimi kabiliyetleri bu cihazların en büyük özellikleri şeklinde tanıtılmaktadır.

Önerilen sistem, [15], [16], [17], [18], [19], [20]'de verilen sistemlerle aynı kabiliyette bina içi veya düşük kapsama alanı gereksinimi duyan uygulamalar için özelleşmiş halidir. Önerilen sistemin, düşük güçlü ve maliyet-etkin bir alternatif olması hedeflenmiştir.

2.2 Sistemin Performans Parametreleri

Tezde önerilen FPGA tabanlı şifreli kablosuz haberleşme sistemi, kullanıcılar arasında güvenli haberleşme arayüzü üzerinden verilerin aktarımını sağlamaktadır. Sistemin temel işlevlerinin yanı sıra tasarım aşamalarında dikkat edilen farklı özellikleri de bulunmaktadır. Bu sistem, düşük veri hızlarında iletim yapan düşük güç tüketimli, maliyet-etkin bir çözüm olarak tasarlanmıştır. Düşük güçlü, maliyet-etkin ve yüksek çalışma hızına sahip bir tasarım için, bu tasarımı daha etkin hale getirecek yaklaşımlar ile yazılım ve donanım altyapıları kurulmuştur.

Önerilen sistemin performans parametreleri;

- Düşük güç tüketimi,
- Maliyet-etkin tasarım,
- Sistemin çalışma hızı

olarak belirtilebilir.

Düşük güç tüketimi, sistemin güç tüketimini en aza indirmek amacıyla donanım ve yazılım tasarımında yapılan iyileştirmeler bütünü olarak tanımlanabilir. Günümüz uygulamalarında en çok öne çıkan performans parametrelerinden biridir. Düşük güç tüketimi, taşınabilir(mobil), pil ile çalışan sistemlerin teknolojisinde önemli bir göstergedir. Bu sistemin ileriki adımlarında gerçekleştirilmek istenen cihaz haline getirilmiş taşınabilir şifreli kablosuz haberleşme sistemi tasarımıdır ve tez kapsamında ön çalışmaları yapılmıştır.

Bu sistem için verilen maliyet etkin tasarım parametresi, sistemin en az ile en çoğu yapması olarak tanımlanabilir. Donanımsal açıdan en uygun bileşenlerin seçilmesi, yazılımsal açıdan ise bu bileşenleri yönetecek en iyi tasarımın yapılmasıdır. Benzer sistemlerle olan kıyaslaması, o uygulamaların FPGA üzerinde harcadığı kaynak sayısıyla ölçülebilir. Daha az kaynak demek, daha küçük ve daha az maliyetli donanımlar kullanmak anlamına gelmektedir. Daha iyi yazılımsal tasarım da FPGA kaynaklarını daha az kullanacağı için bu parametreye doğrudan etkisi bulunmaktadır.

FPGA tabanlı sistemlerin tipik performans parametrelerinden biri sistemin çalışma hızıdır. Sistemin çalışabileceği en yüksek saat darbesine ait frekans değerini belirtmektedir. Yazılım tasarımında kullanılan teknikler ile dili kullanım profesyonelliğine göre bu değer yükseltilebilmektedir. Yüksek saat darbesi

frekansında çalışan sistemler, düşük hızdaki sistemlere göre girdiyi daha hızlı işleyerek daha hızlı çıktı üretebilmektedir. Bu da sistemin birim zamanda daha fazla girdi/çıktı işlemesini sağlamaktadır. Bu parametre, bir işlemcinin çalışma frekansıyla benzeştirilebilir.

Diğer bölümlerde, yukarıda verilen parametrelere göre literatürde yapılan benzer çalışmalarla önerilen sistemin karşılaştırması yapılacaktır.

2.3 Literatürdeki Benzer Çalışmalar ve Karşılaştırmalar

İlk bölümde, cihaz haline getirilmiş ve piyasada kullanılan sistemlerle olan temel benzerlikleri verilen sistemimizin, bu bölümde literatürde işlenen sistemlerle olan karşılaştırmaları verilecektir.

Literatürde, FPGA üzerinde AES şifreleme algoritmasının gerçeklenmesi üzerine farklı uygulama alanlarına yönelik çalışmalar gerçekleştirilmiştir. Bunun yanı sıra, FPGA tabanlı kablosuz haberleşme sistemi tasarımları da literatürde işlenmiştir. Önerilen sistemdeki, AES algoritmasının 128 bitlik anahtar uzunluğuna sahip versiyonu gerçeklenmiş ve kablosuz haberleşme standardı olarak IEEE 802.15.4 Kablosuz Kişisel Alan Ağı standardı kullanılmıştır.

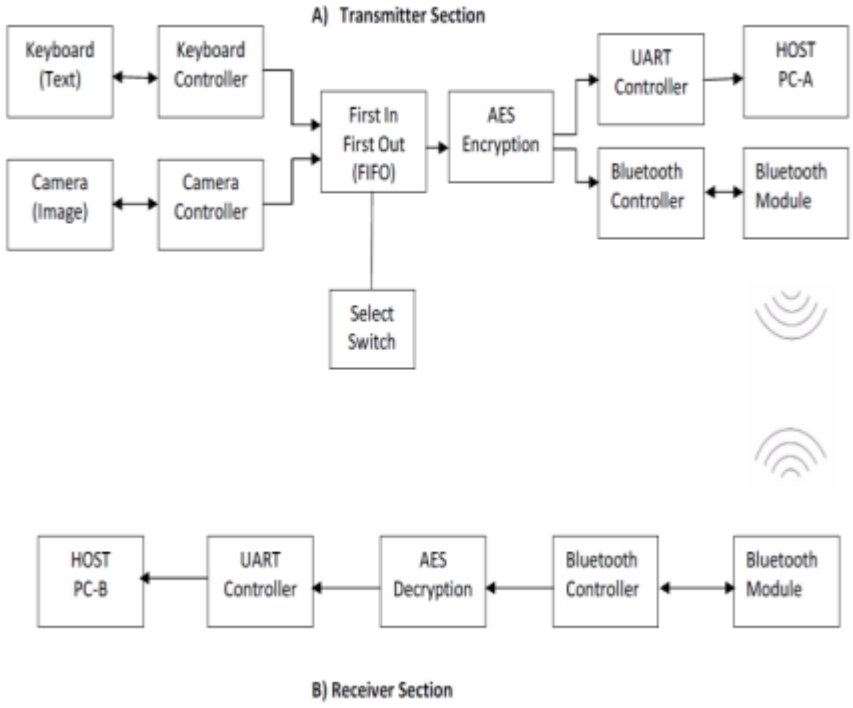
FPGA tabanlı sistemlerde, kullanılan FPGA ailesi sistem parametrelerinde farklılıklara sebep olmaktadır. Örneğin, aynı donanım tanımlama deyimleri kullanılarak sentezlenen bir tasarımda, FPGA aileleri arasında farklı kaynak kullanımları ve çalışma frekansları ortaya çıkabilir. Bu, o FPGA ailesinin teknolojisinden ileri gelmektedir. Bu nedenle, sistemlerin karşılaştırması yapılırken birebir karşılaştırma yapmak mümkün olamayabilir. Bazı durumlarda, her iki sisteme ait değerler ve FPGA altyapıları verilerek değerlendirmelerde bulunulacaktır.

Tezde önerilen sistemde, Digilent firmasının ürettiği Nexys-2 geliştirme kartı kullanılmıştır. Bu kart üzerinde, Xilinx firmasının Spartan 3E ailesinin XC3S500-4FG320 modeli bulunmaktadır.

Literatür taramaları sonucunda, tezde önerilen sisteme yakın özelliklerdeki sistemlerin işlevleri verilerek karşılaştırmaları tablolar halinde sunulacaktır.

[5]'de önerilen sistemde, Bluetooth kablosuz haberleşme protokolü üzerinden mesaj ve görüntü verisi aktarımı gerçekleştirilmektedir. Kameradan alınan görüntü verisi

ile tuş takımından alınan mesaj verisi birbirinden farklı noktalara konumlanan kullanıcılar arasında Bluetooth modülleri yardımıyla iletilmektedir. Veri şifrelemesi AES-128 algoritması kullanarak yapılmıştır. RC-10 FPGA geliştirme kartı üzerinde gerçeklenen sistemde, bir kullanıcı gönderici, diğer kullanıcı alıcı olarak çalışmaktadır. Şekil 2-1'de [5]'te belirtilen sistemin blok şeması verilmektedir.



Şekil 2-1 : [5]'de önerilen sistemin blok şeması.

[6]'da önerilen sistemde, iki kullanıcı arasında kurulan kablolu haberleşme veriyolunda güvenli haberleşme uygulaması gerçekleştirilmektedir. FPGA geliştirme kartı üzerinde gerçek zamanlı şifreleme ve şifre çözme işlemleri gerçekleştirilmekte ve veriler UART arayüzü üzerinden kullanıcılar arasında iletilmektedir. Bu uygulamada, AES128 algoritması gerçeklenmiştir.

[7]'de, kablosuz haberleşme protokolleri için uygunlaştırılmış ve optimize edilmiş AES ve DES şifreleme algoritmalarının FPGA üzerinde gerçeklenmesi sunulmaktadır.

[8]'de, IEEE 802.15.4 standardında kablosuz haberleşen birimler için FPGA üzerinde gerçeklenmiş düşük güç tüketen AES şifreleme birimi tasarımı gerçekleştirilmiştir. Bu çalışmada, kullanıcılar arasındaki veri hızı standardın öngördüğü 250 kbps haberleşme hızına sabitlenmiş giriş verisi alan birim tasarlanmıştır.

Literatürde, AES algoritmasının FPGA üzerinde gerçeklenmesi fazlaca işlenen bir konudur. Çeşitli uygulamalara yönelik olarak düşük güçlü ve yüksek hızlı yaklaşımlar öneren çalışmalar bulunmaktadır. Bu çalışmaların ana konuları, AES algoritmasının gerçeklenmesine yönelik yöntem önerileridir. Tezde anlatılan çalışmada, burada verilen çalışmalara ek olarak haberleşme altyapısını sağlayan işlevler de bulunmaktadır.

Bu çalışmalardan bazıları, [9], [10], [11] ve [12]'de verilmektedir.

Çizelge 2.1'de, karşılaştırılan sistemlerin FPGA ailesi, çalışma frekansları ve veri işlem hacimleri verilmektedir.

Çizelge 2.2'de, karşılaştırılan sistemlerin FPGA üzerinde kullandıkları kaynaklar verilmektedir.

Çizelge 2.1 : Frekans ve veri işlem hacmi karşılaştırma tablosu.

Sistem	FPGA Ailesi	Çalışma Frekansı (MHz)	İşlem hacmi (Gbps)
Önerilen Sistem	Spartan3E XC3S500E	93.3	11.95
Sood, Wagh, Cheema [5]	Spartan3 XC3S1500I	61.5	7.9
Paul, Saha, Sau, Chakrabarti [6]	Spartan3E XC3S500E	50	0.00003
Sood, Wagh, Cheema [7]	Virtex4 XC4VLX85	500	64
Song, Kim [8]	Stratix EPIS10F484C5	2	0.256
Bulens, Standaert [9]	Virtex5	350	4.1
Doğan [10]	Virtex4 XC4VLX200	215.8	-
Kaur, Bhardwaj, Kumar [11]	Virtex2 XC2VP30	247.3	-
Rais, Qasim [12]	Virtex5 XC5VLX50	339	4.34

Çizelge 2.2 : Dilim, LUT, bellek birimi ve güç tüketimi karşılaştırma tablosu.

Sistem	Dilim Sayısı	LUT Sayısı	Bellek birimi sayısı	Güç tüketimi
Önerilen Sistem	3094 / 4656	4970 / 9312	6 / 20	114 mW
Sood, Wagh, Cheema [5]	2546 / 13400	4200 / 30000	8	141 mW
Paul, Saha, Sau, Chakrabarti [6]	2495 / 4656	2871 / 9312	-	-
Sood, Wagh, Cheema [7]	8901 / 13400	-	40	-
Song, Kim [8]	691 / -	4160 / -	-	0.47 mW
Bulens, Standaert [9]	800 / -	-	0	-
Doğan [10]	23144 / -	42988 / -	-	404 mW
Kaur, Bhardwaj, Kumar [11]	1127 / 13696	2029 / 27392	-	124 mW
Rais, Qasim [12]	339 / 7200	1338 / 28800	0	-

Literatürde önerilen ve incelenen yapılar, özellikle kablosuz haberleşme sistemlerinde kullanılmak üzere AES şifreleme algoritmasının farklı yöntemlerle gerçeklenmesi üzerinedir. Tezde önerilen sistem, AES şifreleme ve şifre çözme algoritmalarının yanı sıra mesaj, resim ve ses verilerinin kablosuz veriyolu üzerinden iletimini sağlayan altyapıyı da kapsamaktadır. Bu altyapı, görece maliyeti düşük Spartan3E FPGA ailesi kullanarak gerçekleştirilmiştir. Sonuçlardan da görüleceği üzere, önerilen sistem FPGA çalışma frekansı, veri işlem hacmi, FPGA kaynak kullanım miktarı ve güç tüketimi bakımından birçok sistemden daha verimli, diğer sistemlerle de yarışacak seviyededir.

Önerilen sistem, sistem mimarisinin tasarımı ve kodlama teknikleri sayesinde düşük güç tüketimi ve maliyet-etkin yapısıyla incelenen sistemler arasında ön plana çıkmaktadır.

3. FPGA TABANLI KRİPTOLU KABLOSUZ HABERLEŞME SİSTEMİ

3.1 FPGA Teknolojisi

Tüm programlanabilen tümleşik devreler, temelde mantıksal kapı devrelerinin bir fonksiyonu gerçeklemek amacıyla farklı şekillerde bağlanmasıyla oluşan yapılardır. Programlanabilen tümleşik devreler, birbirlerinden ara bağlantı düzenleri, mantıksal kapıların çeşitliliği ve yapısı ve hafıza yapıları bakımından farklılık gösterirler. Sigorta tabanlı programlanabilen devrelerde ara bağlantılar bir kere oluşturulduktan sonra değiştirilememektedir. Programlanabilen lojik dizi(programmable logic array) adı verilen yapılarda 've' ve 'veya' mantıksal kapıların farklı dizilimleriyle fonksiyonlar gerçeklenmektedir [13].

Gelişen teknoloji ve karmaşık hale gelen fonksiyonların bu altyapılarla gerçeklenmesinin zorlaşmasıyla birlikte programlanabilen tümleşik devre teknolojisinin gelişimi hız kazanmıştır. 1960'larda programlanabilen salt okunur belleklerle başlayan bu gelişim süreci, günümüze kadar birçok aşamadan geçerek son teknoloji ürünü sahada programlanabilir kapı dizilimlerinin (field-programmable gate arrays, FPGA) ortaya çıkmasıyla gelişimine devam etmektedir [13].

FPGA, mantıksal kapılar, hafıza birimleri, çözümleyiciler ve durum makineleri gibi gelişmiş mantıksal birimler kullanılarak farklı fonksiyonların gerçekleştirilebildiği gelişmiş yongalardır. Hem ara bağlantılar seviyesinde hem de mantıksal kapı seviyesinde programlanabilen birimlerdir. Bu özelliklerinden dolayı, diğer programlanabilen tümleşik devrelerden daha üstündürler.

Mühendislik ve geliştirme maliyetlerini düşüren şekilde tekrar programlanabilir yapıda olması, mantıksal kapıların çalışma prensibine dayalı olarak fonksiyonların veya modüllerin paralel çalışabilmesi ve kod güvenliği sağlamasından dolayı, önerilen çalışmanın ana işlemcisi olarak FPGA yongası seçilmiştir.

3.2 Sistemin Çalışma Prensibi

FPGA tabanlı şifreli kablosuz haberleşme sistemi, birbirlerinden farklı noktalarda konumlanmış kullanıcılar arasında güvenli haberleşme arayüzü sağlamak ve verilerin bu kanal üzerinden kullanıcının seçimine göre şifreli veya şifresiz gönderilip alınmasını sağlamak amacıyla tasarlanmıştır.

Önerilen sistem, hem mesaj, hem resim hem de ses verisi alış-verişini kablosuz veriyolu üzerinden sağlamaktadır. Bu veriyolunda, kullanıcının isteğine göre şifrelenmiş veri veya şifrelenmemiş veri gönderip almak mümkündür. İlgili verilerin ayrımını yapıp karşı kullanıcıda uygun şekilde inceleyebilmek amacıyla veri paketleme protokolü oluşturulmuştur. Bu protokolde, her bir veri tipi için farklı başlık ve sonlandırma paketleri oluşturulmuş ve gönderilecek veriler bu paketleme yapısına göre yapılandırılmıştır. Her bir veri tipinin (mesaj, resim ve ses verileri) farklı başlangıç ve bitiş baytlarına sahip olmasıyla alıcı tarafta ayrıştırma kolayca gerçekleştirilmiştir.

Mesaj verilerinin oluşturulması ve resim verilerinin seçilebilmesi amacıyla bilgisayar üzerinde kullanıcı arayüz programı yazılmıştır. Bu arayüz üzerindeki alanlara mesaj verileri girilebilmekte, seçim alanlarından bilgisayarda kayıtlı resim dosyaları seçilebilmektedir. Yazılan mesajlar veya seçilen resimler, bilgisayar ile FPGA kartı arasındaki seri port arayüzü olan UART (Universal Asynchronous Receiver and Transmitter) arayüzünden FPGA kartına gönderilmektedir.

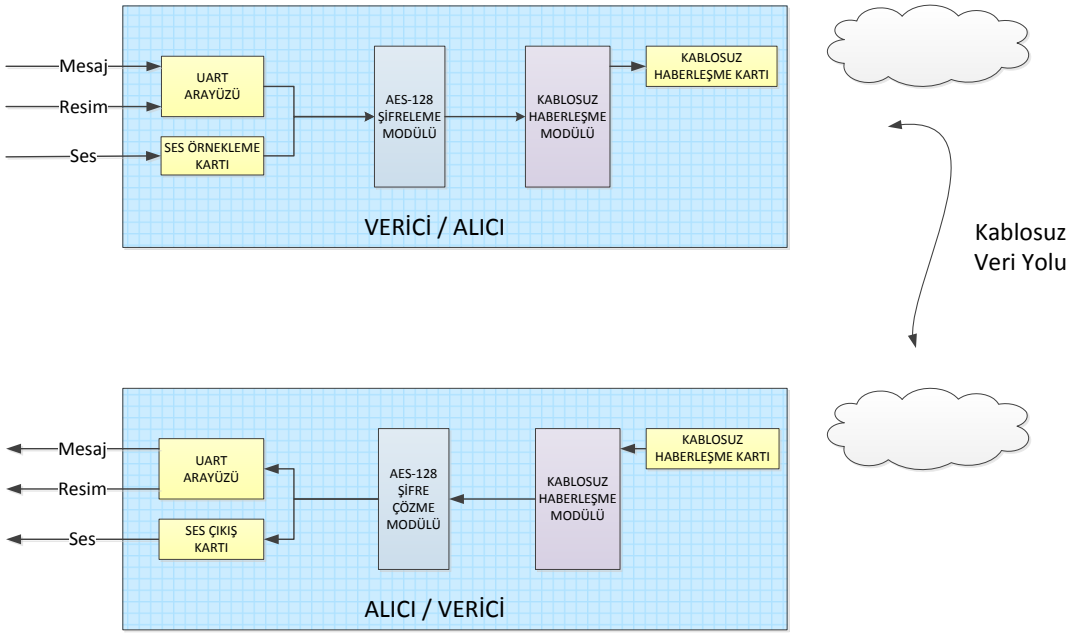
Ses verisi, analog sesi sayısal ses paketlerine dönüştüren ses örnekleme biriminden alınmaktadır. Ses paketleri de paketlenerek kablosuz haberleşme birimine iletilip alıcıya gönderilmektedir.

Tüm veri tipleri, kullanıcının seçimine göre ister şifreli, ister şifresiz olarak iletilebilmektedir.

Elektromanyetik sinyaller halinde gönderici modülden çıkan veriler, alıcı tarafta kablosuz haberleşme birimi tarafından yakalanır. Alıcı tarafındaki kullanıcının gelen verileri anlamlandırabilmesi için iki kullanıcının da şifreleme bloğunu aynı anda aktif etmesi veya aynı anda kapalı konumda tutması gerekir. Alıcıdaki kullanıcı, şifre çözme bloğunu aktif hale getirmemişse veya gönderici şifreli veri göndermediği durumda alıcı bu bloğu aktif etmişse veriyi anlamlandıramaz. Veri paketlerindeki başlangıç ve bitiş verileri kontrol edilerek, verilerin hangi veri tipi olduğuna karar

verilmekte ve mesaj ve resim verisi olması durumunda seri arayüz üzerinden kullanıcı arayüz programına gönderilmekte, ses verisi olması durumunda ise ses çıkış birimine iletilmektedir.

Sistemin veri akış şeması Şekil 3-1'de verilmektedir.



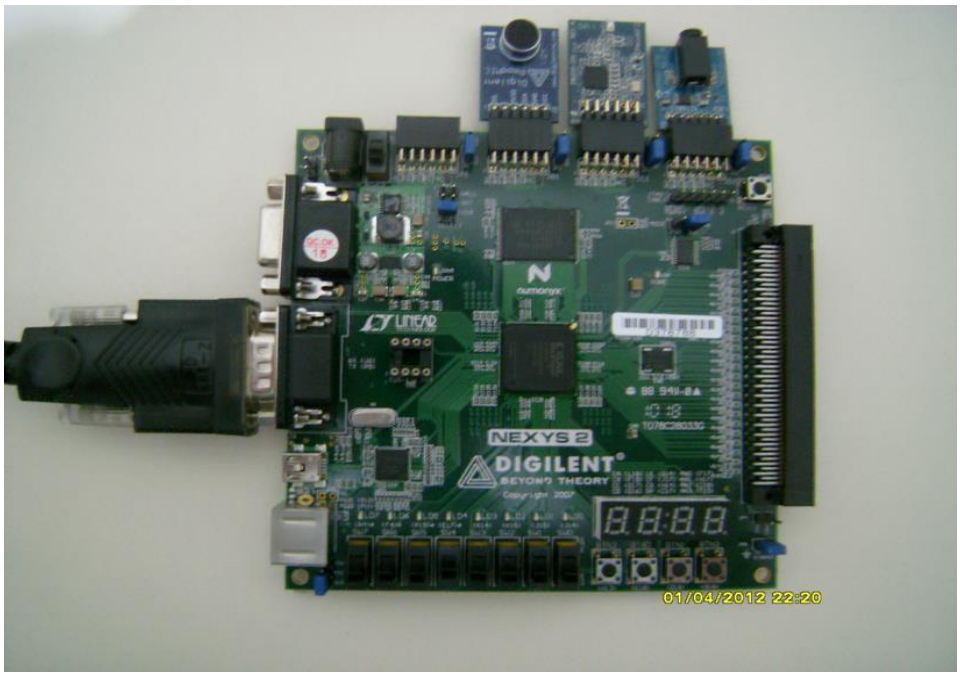
Şekil 3-1 : Sistemin veri akış şeması.

Düşük güç tüketimi, önerilen sistemin temel özellikleri arasındadır. Sistemin taşınabilir versiyonunun tasarımında, başta uzun batarya ömrü olmak üzere düşük maliyeti ve küçültülmüş ölçekte tasarımı önem kazanmaktadır. Bu nedenle, sistemin güç bakımından etkili hale gelebilmesi için sağlamak amacıyla, sistemin haberleşme standardı olarak IEEE 802.15.4 Kablosuz Kişisel Alan Ağı (Wireless Personal Area Network, WPAN) seçilmiştir. IEEE 802.15.4 standardı, düşük güç tüketimi, düşük veri hızları ve düşük maliyetli uygulamalar için geliştirilmiştir.

3.3 Sistemin Donanımsal Altyapısı ve Bileşenleri

Teze konu olan FPGA tabanlı şifreli kablosuz haberleşme sistemi temelde donanım tabanlı bir sistemdir. Sistemin ana işlemcisi olarak FPGA tabanlı geliştirme kartı kullanılmaktadır. Sistemde kablosuz haberleşmeyi sağlamak, ses örneklemesi yapmak ve ses çıktısı üretmek amacıyla FPGA kartına bağlanan çevresel birim kartları da yer almaktadır.

Sistemin görseli Şekil 3-2'de verilmektedir.



Şekil 3-2 : Sistemin görseli.

Sistemin donanımsal bileşenleri dört başlık altında detaylandırılacaktır:

1. FPGA tabanlı geliştirme kartı
2. Kablosuz haberleşme modülü
3. Ses örnekleme (mikrofon) modülü
4. Ses çıkış modülü

3.3.1 FPGA tabanlı geliştirme kartı

Sistem, temel işlemlerin tümünü gerçekleştiren FPGA tabanlı geliştirme kartı üzerine kurulmuştur. Geliştirme kartı, Digilent firması tarafından geliştirilen Spartan 3E-500 FG320 FPGA yongası kullanan Nexys-2'dir.

Nexys-2 üzerinde çevresel birimlerin bağlanabildiği özel konektörler, veri kaydı için bellek bölgesi, USB arayüzü, RS232 arayüzü, VGA arayüzü, 7-parçalı gösterge, LED, buton ve anahtarlar ve 50 MHz'lik saat üreteci barındırmaktadır [21].

FPGA kartı, temel olarak çevresel birim kartlarını yönetmekle ve buralardan gelen verileri ilgili yerlere iletmekle sorumludur. Ses örnekleme birimi ve UART arayüzünden gelen verileri alıp paketledikten sonra şifreleme algoritmasına tabi tutup kablosuz haberleşme birimi üzerinden diğer kullanıcıya iletmekte ve diğer kullanıcı tarafında kablosuz haberleşme biriminden gelen verileri şifre çözme algoritmasına

tabi tuttuktan sonra paket başlangıç verilerine göre ayırıp ilgili yerlere göndermektedir.

Temel olarak, FPGA kartı aşağıda verilen işlemleri gerçekleştirir;

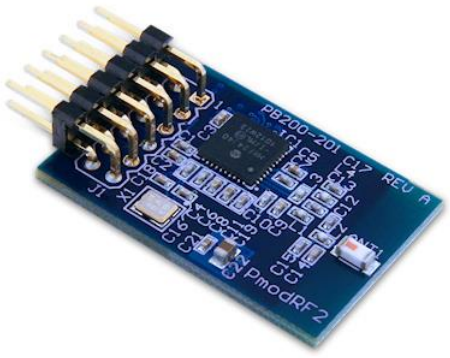
- UART arayüzü üzerinden gelen verileri almak, kaydetmek ve UART arayüzünden veri göndermek
- Ses örnekleme biriminden gelen sayısal ses verilerini almak, kaydetmek ve ses çıkış birimine sayısal ses verisini göndermek
- Kaydedilen verileri kullanıcının seçimine göre şifreleme / şifre çözme algoritmalarına tabi tutmak
- Kablosuz haberleşme birimini ilklendirmek, birimin çalışmasını kontrol etmek ve veri gönderip almasını sağlamak

Çalışma kapsamında, FPGA yongasının seçilmesinin temel nedeni, mühendislik maliyetlerini düşüren tekrar programlanabilir yapıda olması ve mantıksal birimlerin getirdiği paralel programlanabilir altyapıya sahip olmasıdır.

3.3.2 Kablosuz haberleşme modülü

Kablosuz haberleşme modülü, Digilent firması tarafından üretilen PmodRF2 adı verilen çevresel birim karttır. Modül, IEEE 802.15.4 WPAN standardını desteklemektedir. Microchip firmasının MRF24J40 2.4 GHz RF alıcı/verici yongasını kullanmaktadır. Yonga, bu standardın 2.405 – 2.48 GHz ISM bandında çalışmaktadır. 250 kbps (normal mod) ve 625 kbps (turbo mod) veri hızlarını desteklemektedir [21].

PmodRF2 kartı, Şekil 3-3'te verilmektedir.



Şekil 3-3 : PmodRF2 çevresel birim kartı.

PmodRF2 kartının pin dizilimi Çizelge 3.1'de verilmektedir.

Çizelge 3.1 : PmodRF2 pin açıklamaları.

Pin	Sinyal	Açıklama
1	**~CS**	Aktif pini
2	**SDI**	Seri veri giriş pini
3	**SDO**	Seri veri çıkış pini
4	**SCK**	Seri saat darbesi giriş pini
5	**GND**	Toprak pini
6	**VCC**	Güç pini (3.3V)
7	**INT**	Kesme çıkış pini
8	**~RST**	Donanımsal reset pini
9	**WAKE**	Donanımsal uyandırma pini
10	**NC**	-
11	**GND**	Toprak pini
12	**VCC**	Güç pini (3.3V)

Kablosuz haberleşme modülü, kullanıcılar arasında kablosuz ağ üzerinden veri alış verişini sağlamakla görevlidir.

IEEE 802.15.4 WPAN standardı, düşük güç tüketimi ve düşük veri hızları gerektiren uygulamalar için özelleştirilmiştir. IEEE 802.15.4 standardında tanımlanan veri hızları saniyede 20, 40, 100 ve 250 kbps'dir. Yaklaşık olarak 20 metrelik menzilde belirtilen veri hızları sağlanabilmektedir [22].

Bu standartta kullanılan kanal sayıları ve taşıyıcı frekansları ise şu şekildedir;

868 – 868.6 MHz : Avrupa, üç haberleşme kanalına izin verilmektedir.

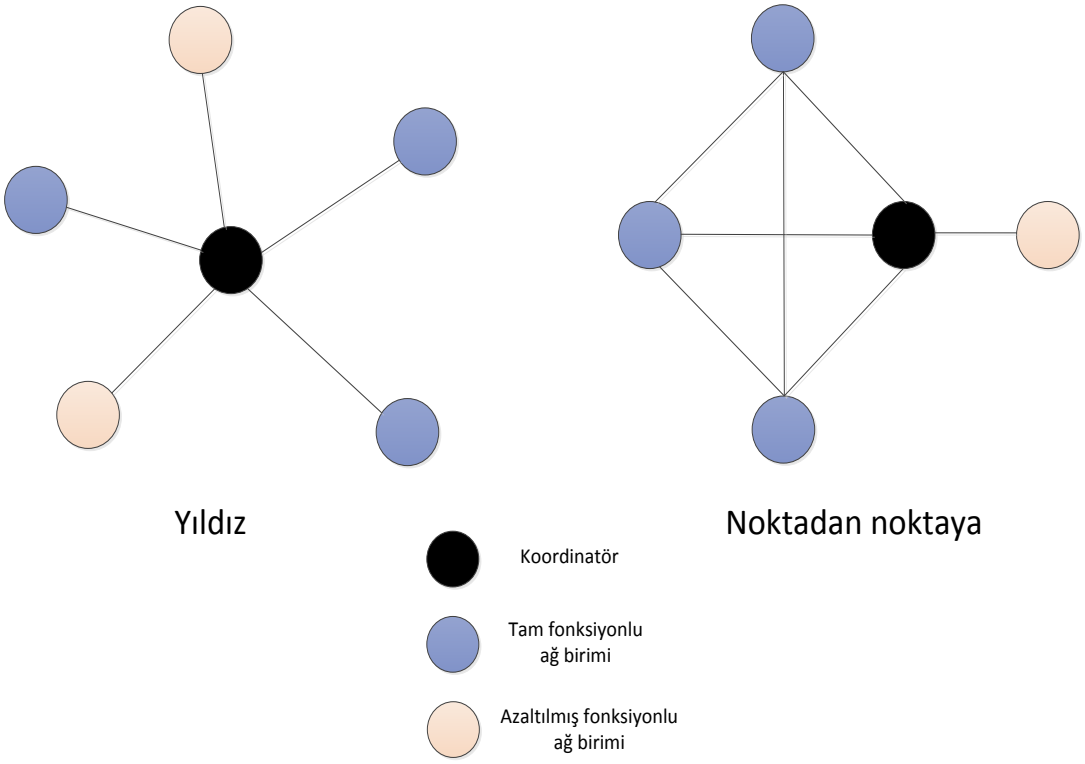
902 – 928 MHz : Kuzey Amerika, otuz haberleşme kanalına izin verilmektedir.

2400 – 2483.5 MHz : Dünya geneli, on altı haberleşme kanalına izin verilmektedir.

IEEE 802.15.4 standardında iki tip ağ birimi tanımlanmıştır. Bunlar; tam fonksiyonlu birim (full-function devices) ve azaltılmış fonksiyonlu birim (reduce-function device) olmak üzere ikiye ayrılmaktadır. Tam fonksiyonlu ağ birimi, ağdaki tüm birimlerle haberleşebilen ve ayrıca ağda koordinatör görevini de üstlenebilen birimlerdir. Ağ koordinatörü olarak atanması durumunda, ağdaki tüm birimlerin koordinasyonunu sağlamakla görevlidir. Azaltılmış fonksiyonlu ağ birimi, sadece

veri gönderim görevi olan ve sadece ağ koordinatörüyle haberleşen birimdir. Ağda kendisine gelen verileri alır ve veri gönderimini sadece tam fonksiyonlu birime yapabilir. Azaltılmış fonksiyonlu birimler arası haberleşme yapılamamaktadır [22].

IEEE 802.15.4 standardında, noktadan noktaya (point-to-point) ve yıldız (star) ağ yapıları oluşturulmaktadır. Şekil 3-4'te noktadan noktaya ve yıldız ağ yapıları verilmektedir.



Şekil 3-4 : Yıldız ve noktadan noktaya ağ yapıları.

Her ağda en az bir adet tam fonksiyonlu birim, koordinatör olarak görev almalıdır. Diğer birimler, tam fonksiyonlu veya azaltılmış fonksiyonlu birimler olarak görev alabilirler. Koordinatör ağda bulunan birimlerin veri akışlarının kontrolünü üstlenir.

Ağda bulunan her birimin, 64-bitten oluşan tanımlayıcısı bulunmaktadır. Tüm ağa yapılan yayınlarda her birim gelen veriyi dinler ve kendi tanımlayıcısını içeren veri paketlerini alır.

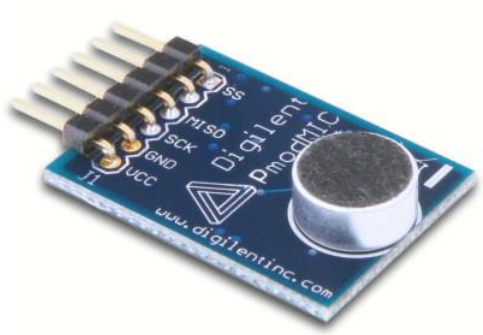
Önerilen sistemde, noktadan noktaya ağ yapısı kurulmakta ve kullanıcılar arasında doğrudan haberleşme gerçekleştirilmektedir. Sistemde bir birim koordinatör iken diğer birim tam fonksiyonlu birimdir. Sistemde azaltılmış fonksiyonlu birim görev almamaktadır.

3.3.3 Ses örnekleme (mikrofon) modülü

Ses örnekleme(mikrofon) modülü, Digilent firması tarafından üretilen ve PmodMIC adı verilen çevresel birim kartıdır. Modül üzerinde National Semiconductor firması tarafından üretilen ADCS7476AIM 12-bit analog-sayısal çevirici yonga ve mikrofon birimi bulunmaktadır [21]. PmodMIC kartı, mikrofondan aldığı analog ses verisini örnekleyerek sayısal ses verisine çevirmekte ve seri arayüz üzerinden FPGA kartına iletmektedir.

Sistem, ses verilerinin şifrelemesini ve güvenli ağ üzerinden gönderimini de gerçekleştirmektedir. Ses verilerini işleyebilmek için sayısallaştırmak gerekmektedir. Bu nedenle, PmodMIC kartı analog ses verilerini sayısal ses verilerine dönüştürülmesi amacıyla kullanılmaktadır. Bu sayede, kullanıcılar arasında kablosuz veriyolu üzerinden ses verileri gönderilebilmektedir.

PmodMIC kartı, Şekil 3-5'te verilmektedir.



Şekil 3-5 : PmodMIC çevresel birim kartı.

PmodMIC kartının pin açıklamaları, Çizelge 3.2'de verilmektedir.

Çizelge 3.2 : PmodMIC pin açıklamaları.

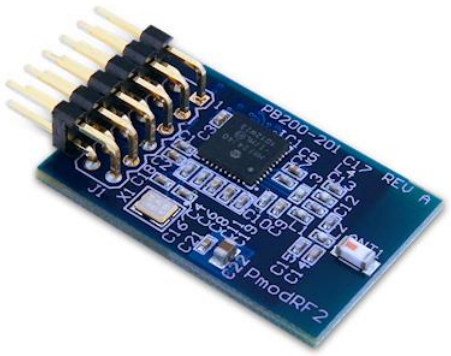
Pin	Sinyal	Açıklama
1	**~CS**	Aktif pini
2	**NC**	-
3	**SDO**	Seri veri çıkış pini
4	**SCK**	Seri saat darbesi pini
5	**GND**	Toprak hattı
6	**VCC**	Güç hattı (3.3V)

3.3.4 Ses çıkış modülü

Ses çıkış modülü, Digilent firması tarafından üretilen ve PmodI2S adı verilen çevresel birim kartıdır. Modül üzerinde Cirrus Logic firmasına ait CS4344 24-bit ses sayısal / analog çeviricisi bulunmaktadır [21].

Ses çıkış modülü, Birleşik Entegreler Arası Ses (Integrated Interchip Sound, I2S) seri arayüzü üzerinden, aldığı sayısal ses verisini analog ses verisine çevirmektedir. Karşı kullanıcıdan gönderilen ses verisi, diğer kullanıcı tarafında bu modül tarafından analog veriye dönüştürülmektedir. Modüle bağlanan hoparlör ile de ses seviyesi ayarlanabilmekte ve kullanıcı tarafından anlaşılır seviyeye yükseltilmektedir.

PmodI2S kartı, Şekil 3-6'da verilmektedir.



Şekil 3-6 : PmodI2S çevresel birim modülü.

PmodI2S kartının pin açıklamaları, Çizelge 3.3'te verilmektedir.

Çizelge 3.3 : PmodI2S pin açıklamaları.

Pin	Sinyal	Açıklama
1	**MCLK**	Ana saat darbesi girişi
2	**LRCK**	Sağ / Sol saat darbesi girişi
3	**SCLK**	Seri saat darbesi girişi
4	**SDIN**	Seri veri girişi
5	**GND**	Toprak hattı
6	**VCC**	Güç hattı (3.3V)

4. SİSTEMİN YAZILIMSAL ALTYAPISI

4.1 Kontrol Yazılımı Altyapısı

FPGA tabanlı sistemlerde, yazılım geliştirme işlemleri donanım tanımlama dilleri ile yapılmaktadır. Donanım tanımlama dilleri, programlanabilen tümleşik devrelerde mantıksal birimlerin istenen fonksiyonu gerçekleştirmesi amacıyla kullanılan deyimlerin dilbilgisi kurallarını tanımlamaktadır.

Kullanılan donanım tanımlama dilleri, VHDL ve Verilog'dur.

VHDL(Very High Speed Integrated Circuits Hardware Description Language), Çok yüksek hızlı tümleşik devre donanım tanımlama dili'nin İngilizce kısaltmasıdır.

Literatürde, VHDL ile Verilog arasında bazı karşılaştırmalar olsa da birbirlerine olan üstünlükleri konusunda kayda değer farklar bulunmamaktadır. Tezde önerilen sistemde, VHDL ile FPGA üzerindeki yazılım altyapısı geliştirilmiştir ve bu tamamen kişisel tercih olarak değerlendirilmelidir.

Sistemin FPGA tabanlı kontrol yazılımı altyapısı, "bottom-up" yaklaşımı ile oluşturulmuştur. Sistem, en alt donanım birimlerine kadar ayrılıp analiz edildikten sonra, bu alt donanım birimlerini kontrol edecek yazılım modülleri oluşturulmuş ve bu modüller birleştirilerek tüm sistemi kontrol eden yapı ortaya çıkarılmıştır.

FPGA teknolojisinin sağladığı imkan sayesinde bu modüller birbirleriyle paralel yapıda çalışabilmektedir. Paralel çalışabilme özelliği sayesinde, farklı modüller aynı anda işlevlerini yerine getirmekte ve seri mantıkta işleyen mikroişlemci ve mikrokontrolcü yapılarına nazaran daha hızlı çalışabilmektedir.

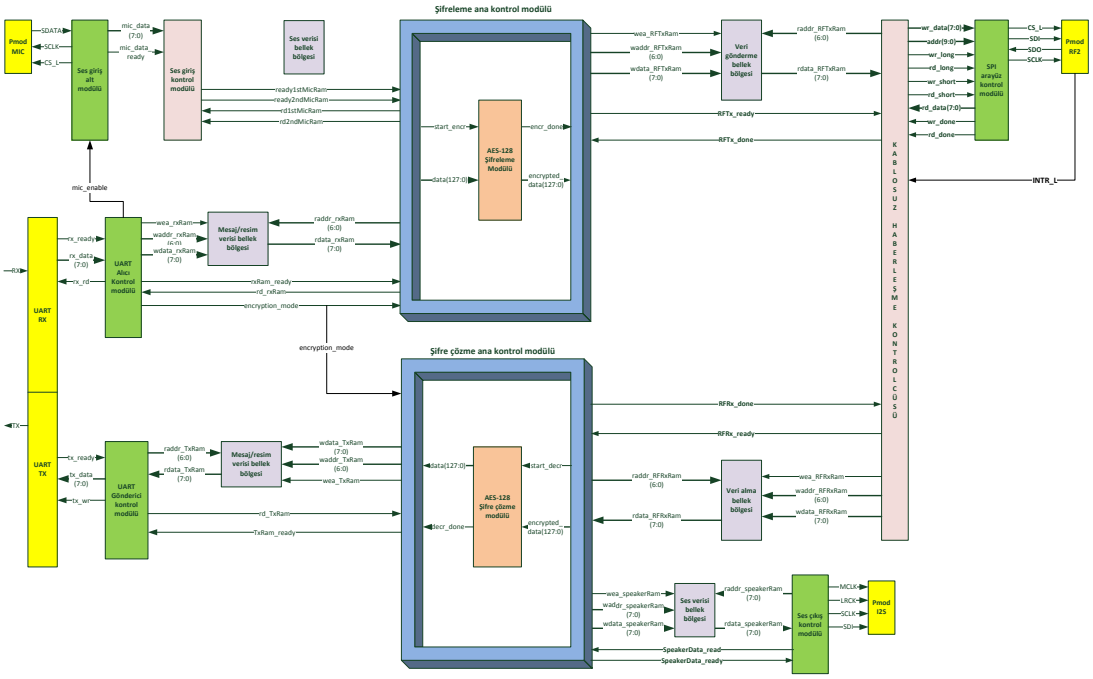
Sistemin FPGA'de VHDL kullanılarak yazılan yazılım modülleri aşağıda belirtilen şekildedir:

- Şifreleme ana modülü
    - AES-128 şifreleme modülü

    - Şifreleme kontrol modülü
- Şifre çözme ana modülü
    - AES-128 şifre çözme modülü
    - Şifre çözme kontrol modülü
- Kablosuz haberleşme ana modülü
    - RF alıcı/verici kontrol modülü
    - SPI arayüz kontrol modülü
- Ses giriş ana modülü
    - Ses giriş kontrol modülü
    - Ses giriş alt modülü
- Ses çıkış ana modülü
- UART alıcı ana modülü
    - UART alıcı kontrol modülü
    - UART alıcı modülü
- UART gönderici ana modülü
    - UART gönderici kontrol modülü
    - UART gönderici modülü

Yukarıda bahsi geçen yazılım modülleri, kablosuz haberleşme birimini, ses giriş birimini, ses çıkış birimini, bilgisayar – FPGA arası haberleşmeyi ve AES-128 şifreleme algoritmasını gerçekleştirmek için VHDL dilinin sentezlenebilir deyimleri kullanarak oluşturulmuştur.

Sistemin FPGA'de oluşturulan yazılım modülleri ve ara haberleşme sinyalleri gösterimi Şekil 4-1'de verilmektedir.



Şekil 4-1 : Yazılım modülleri ve ara haberleşme sinyalleri.

4.1.1 Şifreleme ana modülü

Şifreleme ana modülü, gelen veriyi şifre anahtarını kullanarak AES-128 algoritmasına göre şifrelemekle sorumludur. UART arayüzünden gelen mesaj, resim ve ses örnekleme modülünden gelen sayısal ses verisini şifrelemektedir. Şifreli veri, karşı kullanıcıya gönderilmek üzere kablosuz haberleşme modülünün bellek bölgesine yazılmaktadır. Bu modül, kullanıcı arayüz yazılımı üzerinden etkin hale getirilebilir.

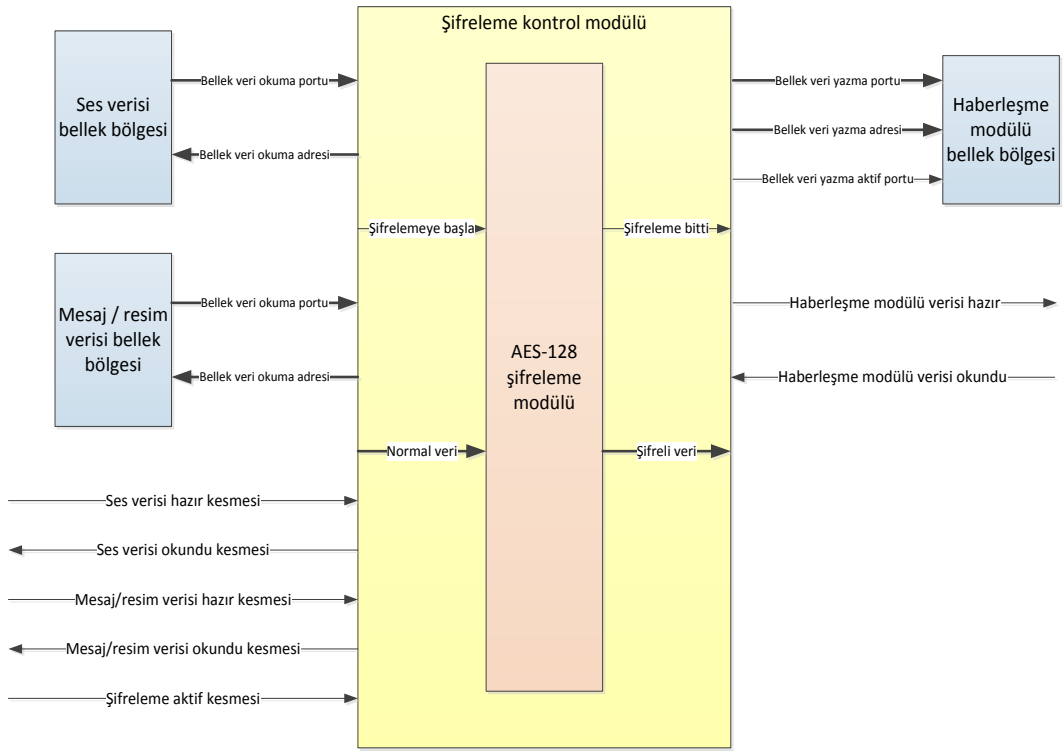
Şifreleme ana modülü, iki alt yazılım modülünden oluşur. Bunlar; şifreleme kontrol modülü ve AES-128 şifreleme modülüdür.

Şifreleme kontrol modülü, AES-128 şifreleme modülü ile kablosuz haberleşme ana modülü, UART alıcı ana modülü ve ses alıcı ana modülü arasında arayüzü sağlamaktadır. Bu modüle, UART alıcı modülünden ve ses alıcı modüllerinden gelen, veri hazır kesme sinyallerine göre ilgili modülün verilerini bellek bölgelerinden okuyup AES-128 şifreleme modülüne göndermekte ve AES-128 şifreleme modülünden çıkan şifreli veriyi haberleşme modülünün bellek bölgesine yazmaktadır.

AES-128 şifreleme modülü, AES-128 algoritmasının gerçeklendiği yazılım birimidir. Şifreleme kontrol modülünün blok halinde girişine verdiği 128-bitlik veriyi, algoritmanın adımlarını izleyerek şifrelemektedir.

Bölüm 5. ’te AES algoritması hakkında bilgiler verilmektedir.

Şifreleme ana modülünün blok şeması, Şekil 4-2’de verilmektedir.

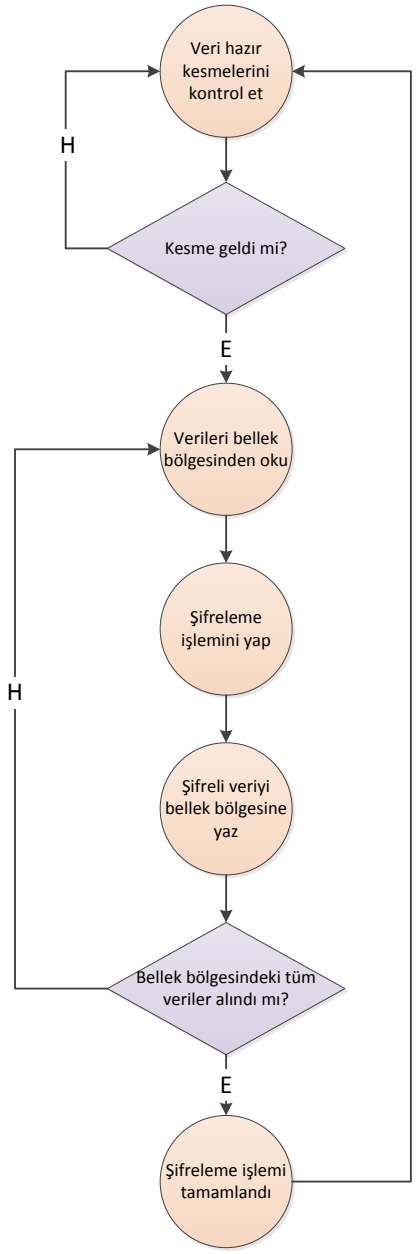


Şekil 4-2 : Şifreleme ana modülü blok şeması.

Şifreleme ana modülünün sözde kod akışı, Şekil 4-3’da verilmektedir.

Verilen sözde kod akışına göre, bilgisayardan gönderilen mesaj ve resim verileri ve ses biriminden gelen sayısal ses verisi ilk olarak bellek bölgelerine kaydedilir. Verilerin kaydedilmesinden sonra, verinin bellek bölgesinde hazır olduğunu bildiren kesmelerle şifreleme kontrol modülü bellek bölgesindeki verileri okur. Algoritma gereği, giriş verisi 128 bitlik blok halinde şifreleme modülüne aktarılmalıdır. 8 bitlik veriler halinde kaydedilen mesaj, resim ve ses verileri 128 bitlik bloklar halinde AES-128 şifreleme modülüne aktarılır. Kullanıcı arayüzü üzerinden şifreleme işlemi aktif edilmemişse, giriş verisi doğrudan çıkışa aktarılır. Aktif edilmişse algoritmanın adımları izlenerek veri üzerine şifreleme işlemi uygulanır. Şifreleme başlatıldıktan sonra, kontrol modülü şifrelemenin bitmesini bekler ve yeni bir giriş verisini AES-128 şifreleme modülüne iletmez. Şifreleme bittikten sonra, yine 128-bit

uzunluğundaki şifreli veriyi kablosuz haberleşme ana kontrolcüsünün bellek bölgesine kaydeder ve verinin hazır olduğunu bildiren kesmeyi aktif eder. Bu işlemlerin sonunda, giriş belleğindeki verilerin okunduğunu ve işlendiğini belirten kesmeleri de UART ve ses kontrol modüllerine iletir. Kablosuz haberleşme modülü verileri ilettikten sonra şifreleme ana modülüne tüm verilerin gönderildiğini bildiren kesmeyi iletir.



Şekil 4-3 : Şifreleme ana modülü sözde kod akışı.

4.1.2 Şifre çözme ana modülü

Şifre çözme ana modülü, gelen şifreli veriyi şifre anahtarını kullanarak AES-128 algoritmasına göre çözmekle sorumludur. Kablosuz haberleşme ana modülü ile ses

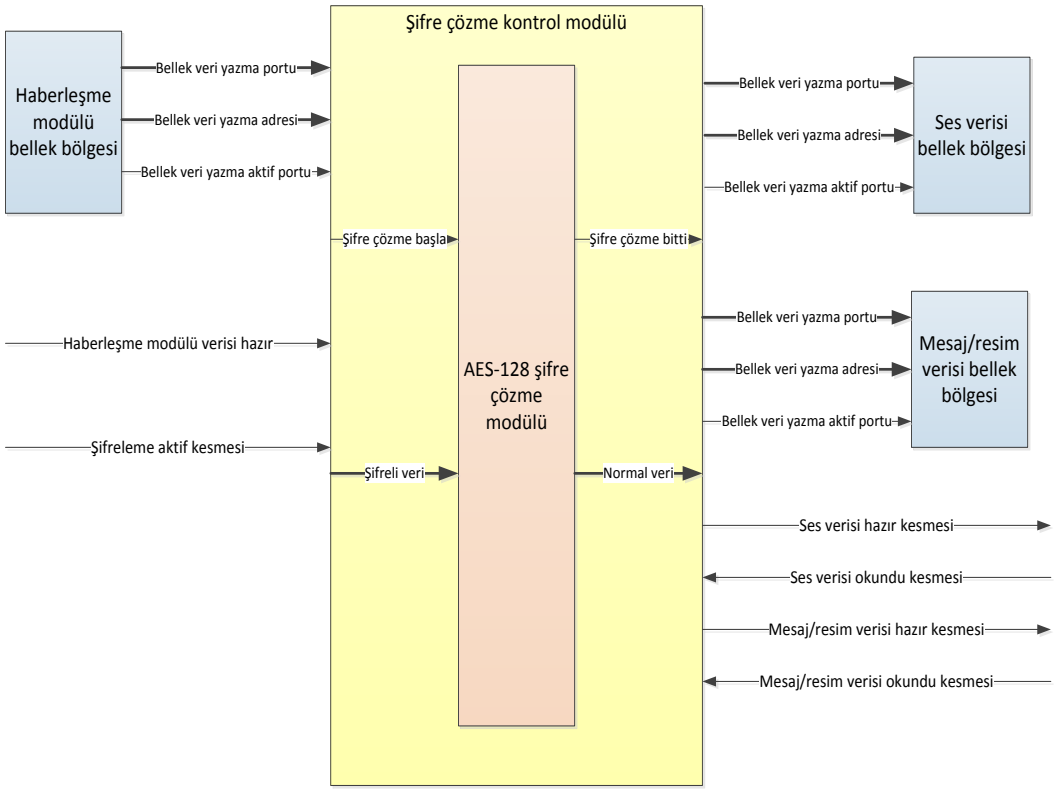
çıkış ana modülü ve UART gönderici ana modülü arasında arayüzü kurmaktadır. Bu modül, kullanıcı arayüz yazılımı üzerinden etkin hale getirilebilir.

Şifre çözme ana modülü, iki alt yazılım modülünden oluşur. Bunlar; şifre çözme kontrol modülü ve AES-128 şifre çözme modülüdür.

Şifre çözme kontrol modülü, AES-128 şifre çözme modülü ile kablosuz haberleşme ana modülü, UART gönderici ana modülü ve ses çıkış ana modülü arasında arayüzü sağlamaktadır.

Bölüm 5. ’te AES algoritmasının detayları anlatılmaktadır.

Şifre çözme ana modülünün blok şeması, Şekil 4-4’da verilmektedir.

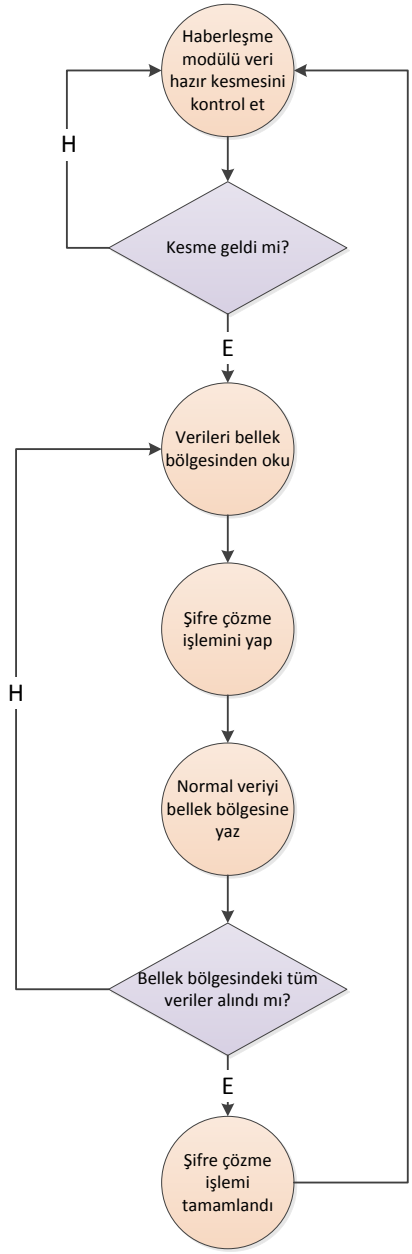


Şekil 4-4 : Şifre çözme ana modülü blok şeması.

Şifre çözme ana modülü, sözde kod akışı Şekil 4-5’de verilmektedir.

Verilen sözde kod akışına göre, karşı kullanıcı tarafından gönderilen verilerin kablosuz haberleşme birimi ile alınmasından sonra, kablosuz haberleşme ana modülü gelen şifre çözme modülünün bellek bölgesine kaydeder ve şifre çözme kontrol modülüne verinin hazır olduğunu bildiren kesme sinyali gönderir. Şifre çözme kontrol modülü, bu sinyali algıladıktan sonra bellek bölgesinde 8 bitlik veriler halinde kaydedilen bilgiyi 128-bitlik blok halinde AES-128 şifre çözme modülüne

iletir. AES-128 şifre çözme modülü öncelikle şifre çözme işlevinin aktif olup olmadığını kontrol eder. Aktif değilse giriş verisini doğrudan çıkışa aktarır ve işlemin bittiğini bildiren kesmeyi aktif eder. Aktifse 128-bitlik giriş verisi üzerine algoritmanın adımlarını uygular ve işlemin bittiğini bildiren kesmeyi aktif eder. Şifre çözme işlemlerinden sonra paket yapısındaki başlangıç baytına göre, veriyi ya ses ya da mesaj/resim bellek bölgelerine kaydeder ve UART gönderici ana modülünü uyarır.



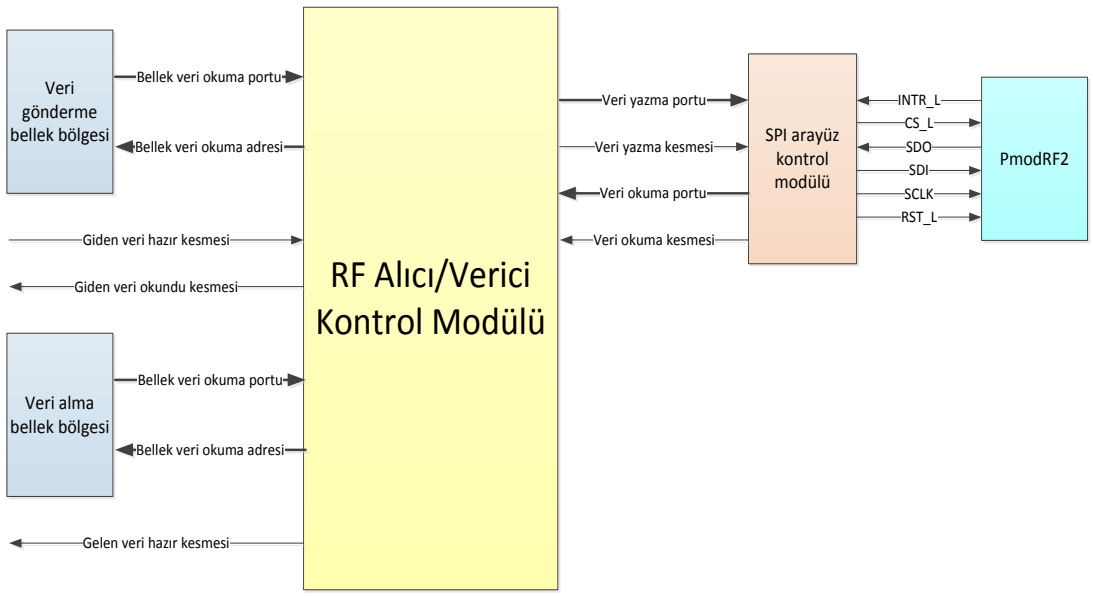
Şekil 4-5 : Şifre çözme ana modülü sözde kod akışı.

4.1.3 Kablosuz haberleşme ana modülü

Kablosuz haberleşme ana modülü, iki kullanıcı arasında iletişimi sağlayan kablosuz haberleşme biriminin ilklendirilmesini, kontrolünü ve diğer modüllerle olan arayüzünü sağlamaktadır.

Kablosuz haberleşme kartında bulunan MRF24J40 802.15.4 RF alıcı/verici tümleşik devresinin istenilen işlevleri yerine getirmesi için seri çevresel arayüz (serial peripheral interface, SPI) üzerinden saklayıcılarının ayarlanması ve belirli değerlerin yazılması gerekmektedir. Sistem ayağa kalktıktan hemen sonra, ilk olarak bu tümleşik devrenin saklayıcı ayarlarını yapar. Ayarların yapılmasıyla tümleşik devre aktif hale gelir ve veri alıp gönderme işlerini gerçekleştirebilir. RF alıcı/verici kontrol modülü tümleşik devreyi ayarlamakla sorumludur.

Kablosuz haberleşme ana modülünün blok şeması Şekil 4-6'de verilmektedir.

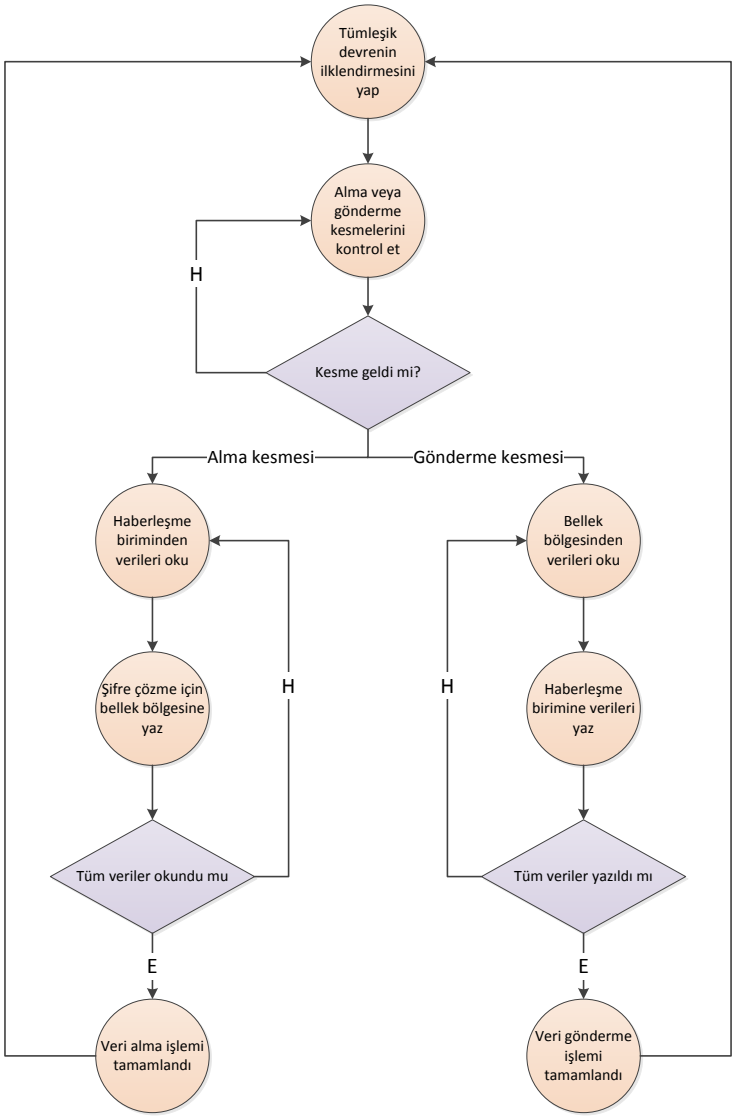


Şekil 4-6 : Kablosuz haberleşme ana modülü blok şeması.

Kablosuz haberleşme ana modülü sözde kod akışı Şekil 4-7'de verilmektedir.

Verilen sözde akış şemasına göre, hem şifreleme hem de şifre çözme ana kontrol modülleriyle arayüze haberleşmektedir. Şifreleme işlemleri sırasında, şifrelenen veya şifrelenmeden gelen 128-bitlik bilgi veri gönderme bellek bölgesine yazılır. Tüm veriler yazıldıktan sonra şifreleme modülü, kablosuz haberleşme kontrol modülüne verinin hazır olduğunu bildirir. Kablosuz haberleşme ana modülü, bellek bölgesinden verileri okur ve SPI arayüzü üzerinden tümleşik devrenin içine gönderir. Tümleşik

devre aktive edildikten sonra hat üzerinde kendisine gönderilen veri olmaması durumunda verileri karşı sisteme iletir. Veri çakışması veya veri gönderememe durumları oluşursa tümleşik devre bunu otomatik olarak algılar ve aynı veriyi belirli bir sayıda tekrar göndermeyi dener. Kablosuz haberleşme modülü şifreleme ana modülüne tüm verilerin gönderildiği bilgisini iletir. Yeni veriler gelene kadar, kablosuz haberleşme modülü kapatılır ve güç harcaması azaltılır.



Şekil 4-7 : Kablosuz haberleşme ana modülü sözde kod akışı.

Şifre çözme modülüyle olan arayüzünde, karşı kullanıcıdan gelen veriler tümleşik devre tarafından alınır ve SPI arayüzü üzerinden okunarak bellek bölgesine yazılır. Gelecek veri miktarı paket formatında tutulduğu için o kadar verinin gelmesi

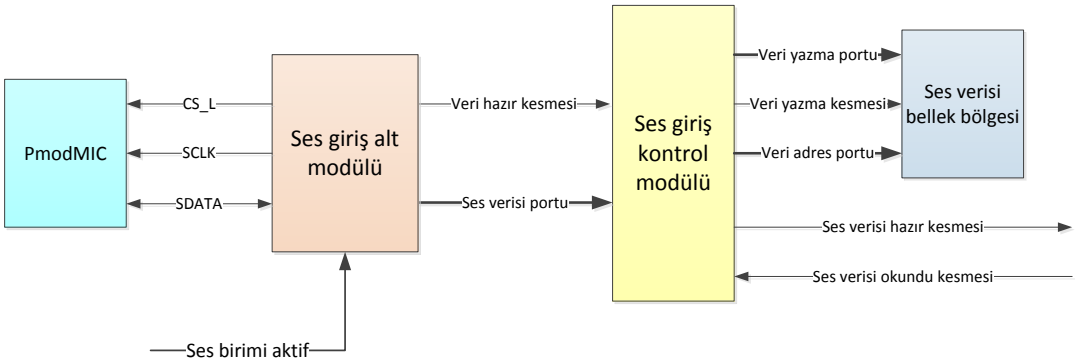
beklenir. Tüm veriler alındıktan sonra, şifre çözme ana modülüne kesme sinyali gönderilir ve işlevini bitirmesi beklenir.

Kablosuz haberleşme ana modülü temel olarak, verilerin kullanıcılar arasında gönderilip alınmasını sağlayan kablosuz haberleşme kartındaki tümleşik devreyi kontrol ederek verilerin alış-verişini yönetmektedir.

4.1.4 Ses giriş ana modülü

Sistem, kullanıcılar arasında ses alış-verişini sağlayabilecek altyapıya sahiptir. Ses verisini örneklemek ve sayısal ses verisine dönüştürmek amacıyla ses örnekleme kartı kullanılmakta ve bu kartın yazılımsal kontrolünü ses giriş ana modülü sağlamaktadır. Ses giriş ana modülü, ses örnekleme kartı ile şifreleme ana modülü arasındaki arayüzü sağlamaktadır.

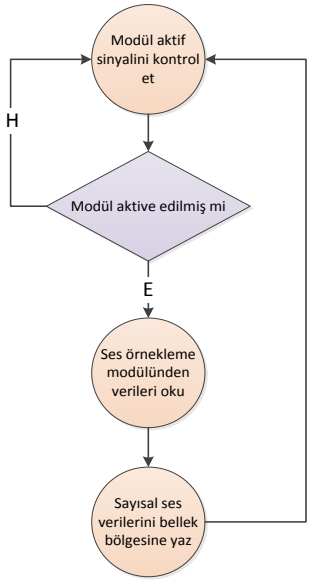
Ses giriş ana modülü blok şeması, Şekil 4-8'te verilmektedir.



Şekil 4-8 : Ses giriş ana modülü blok şeması.

Ses giriş ana modülü, ses giriş kontrol modülü ve ses giriş alt modülünden oluşmaktadır. Ses giriş alt modülü, 4800 Hz örnekleme frekansına göre üretilen saat darbesi sinyaliyle (SCLK) analog ses verisini sayısal ses verisine çevirerek SDATA pini üzerinden örneklenen veriyi almaktadır. Bu modül, alt seviye işlemleri gerçekleştirmektedir. Ses örnekleme birimindeki tümdevrenin arayüzünden alınan 12-bitlik sayısal ses verisi, ses giriş kontrol modülüne iletilir. Veriler, ses giriş kontrol modülü üzerinden ses verisine ait bellek bölgelerine 16-bitlik veriler halinde kaydedilir. Bellek bölgesinde yazılımda belirlenen miktarda veri olmasıyla birlikte şifreleme modülüne veri hazır kesmesi gönderilir. Veri kaybı yaşanmaması için bellek bölgesinin yarısı dolduğu zaman veri hazır kesmesi aktif edilir. Veriler şifreleme modülü tarafından okunup işlendikten sonra verinin okunduğuna dair bilgi ses giriş kontrol modülüne iletilir.

Ses giriş ana modülü sözde kod akışı, Şekil 4-9'te verilmektedir.



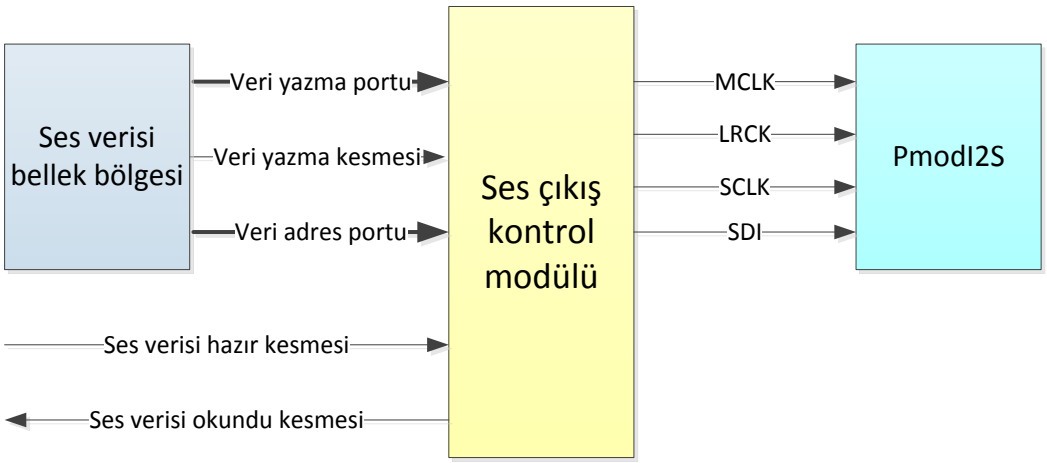
Şekil 4-9 : Ses giriş ana modülü sözde kod akışı.

Ses giriş ana modülü, kullanıcı arayüz programı üzerinden aktive edilebilir. Bu işlevin kullanılmadığı durumlarda, güç tüketimini azaltmak için sisteme bu kabiliyet kazandırılmıştır.

4.1.5 Ses çıkış ana modülü

Sistem, karşı kullanıcıdan gelen sayısal ses verisini analog ses verisine çeviren ses çıkış çevresel birim kartına sahiptir. Bu kartın kontrolü için yazılımsal ses çıkış ana modülü görev yapmaktadır.

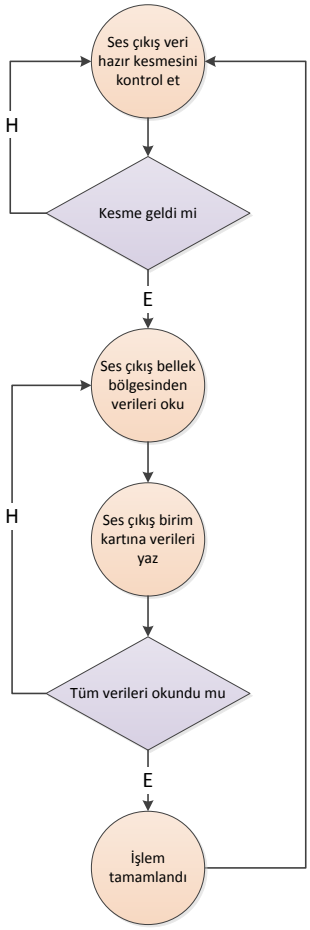
Ses çıkış ana modülü blok şeması, Şekil 4-10'da verilmektedir.



Şekil 4-10 : Ses çıkış ana modülü blok şeması.

Ses çıkış ana modülü sözde kod akışı, Şekil 4-11'de verilmektedir.

Ses çıkış ana modülü, şifre çözme ana modülü ile ses çıkış birim kartı arasındaki yazılımsal arayüzü sağlamaktadır. Şifre çözme modülünde başlangıç baytlarına göre ayrılan veri, ses paket verisi olması durumunda ses çıkış ana modülünün bellek bölgesine kaydedilir. Veriler kaydedildikten sonra, birim kartının portları üzerinden I2S arayüzü ile sayısal ses verisi birime iletilir. Veriyi iletmek için, birim kartının MCLK, LRCK, SCLK ve SDATA pinleri kullanılmaktadır.



Şekil 4-11 : Ses çıkış ana modülü sözde kod akışı.

4.1.6 UART arayüzü alıcı ve gönderici ana modülleri

UART, seri bir haberleşme kanalı olup donanımlar arasında bilgi alış verişinin yapıldığı çok temel bir arayüzdür. Genellikle, seri haberleşmeye destek veren bilgisayar, mikroişlemci, mikrokontrolcü ve tümleşik devrelerin birbirleriyle ve çevresel birimlerle haberleşmesi amacıyla kullanılmaktadır.

UART ile haberleşme yapan sistemlerde, bir gönderici bir de alıcı taraf bulunmaktadır. Alıcı ve gönderici aynı anda veri iletimi yapabilmektedir. Bu tip iletim altyapısına full-duplex haberleşme denir. Alıcı ve gönderici, seri hat üzerinden birbirlerine belirlenen formata göre veri gönderimi yaparlar. UART arayüzündeki veri yapısı Şekil 4-12'de verilmektedir.

Bit sayısı	1	2	3	4	5	6	7	8	9	10	11	12
	Başlangıç biti	5-8 veri bitleri								Eşlik biti	Bitiş bit(ler)i	
	Başlangıç	Veri 0	Veri 1	Veri 2	Veri 3	Veri 4	Veri 5	Veri 6	Veri 7	Eşlik	Bitiş	

Şekil 4-12 : UART arayüzü veri yapısı.

UART arayüzünde, başlangıç biti 1 bit, veri biti 5 ile 8 bit, eşlik biti 1 bit, bitiş biti 1, 1.5 ve 2 bit olarak ayarlanabilir. Alıcı ve gönderici tarafta, veri hızı, veri biti sayısı, eşlik biti sayısı ve bitiş biti sayısı aynı olmalıdır. Parametrelerin doğru ayarlanmaması durumunda doğru veri gönderimi gerçekleştirilemez.

Sistemde UART arayüzü, 8 veri biti, çift(even) eşlik biti, 1 bitiş biti ve sembol zamanı 115200 kbaud/s olarak ayarlanmıştır. Hem bilgisayar tarafında hem de FPGA tarafındaki ayarlamalar aynıdır.

Sembol zamanı kavramı, her bir sembolün – 0 veya 1 - hatta kalma süresi olarak tanımlanabilir. Örneğin, 115200 baud/s haberleşen bir altyapıda bir saniyede 115200 adet sembol gönderimi gerçekleştirilebilir anlamına gelmektedir. Bu sembollerin her biri 0 veya 1 bilgilerini içermektedir.

Tezde önerilen sistemde UART arayüzü, bilgisayar üzerinde gerçeklenen kullanıcı arayüz programı ile FPGA ana kartı arasındaki haberleşmeyi sağlamak amacıyla kullanılmaktadır. Bu arayüz ile mesaj ve resim verileri FPGA kartına iletilmektedir. Aynı zamanda, FPGA'den gelen mesaj ve resim verileri de kullanıcıya iletilmektedir. Ayrıca, arayüz üzerinden şifreleme / şifre çözme işlevlerini aktif etme, ses giriş birimin aktif etme işlemleri için kontrol baytları gönderilmektedir.

Sistem altyapısında, mesaj, resim ve ses verilerinin iletimi gerçekleştirilmektedir. Bu verilerin alıcı tarafında doğru yorumlanabilmesi ve yönlendirilebilmesi için (mesaj verisinin mesaj şeklinde görüntülenmesi, resim verisinin resim dosyası halinde kaydedilmesi ve ses verisinin ses çıkış birimine iletilmesi) paket formatı geliştirilmiştir. Ses, mesaj, resim ve kontrol verilerinin her birinin farklı başlangıç baytları bulunmaktadır. Yazılım, veri paketi formatını ayrıştırarak verinin hangi

kaynaktan geldiğine, hangi birime yönlendirileceğine, hangi uzunlukta olduğuna(bayt cinsinden) ve veriye göre neler yapacağına karar verebilmektedir.

Sistemde tanımlanan veri paketi formatı Şekil 4-13'da verilmektedir.

Başlangıç 1 bayt	Uzunluk 1 bayt	Veri N bayt	Bitiş 1 bayt

Şekil 4-13 : Veri paketi formatı.

Başlangıç baytı, mesaj verisi için *0xCC*, resim verisi için *0xDD,* sayısal ses verisi için *0xBB* olarak belirlenmiştir. Mesaj verisinin uzunluğu 1 ile 95 bayt arasında seçilebilir. Resim ve sayısal ses verisi için bir paketteki uzunluk sabittir ve 95 bayttır. Bitiş baytı ise tüm veri tipleri için *0xFF* olarak belirlenmiştir.

Kontrol baytları, şifreleme ve şifre çözme ana modüllerini aktive etmek için *0xAA,* ses giriş ana modülünü aktive etmek için *0xDD* olarak seçilmiştir. Bu modülleri kapatmak için bu verilerin bir kez daha sisteme gönderilmesi gerekmektedir. Şifreleme / şifre çözme ve ses giriş biriminin aktif olduğunu göstermek amacıyla geliştirme kartı üzerindeki ledler kullanılmaktadır.

Bu yapı sayesinde, karşıdaki kullanıcıya gönderilen verilerin hangi yazılımsal modüle yönlendirileceği rahatlıkla analiz edilmekte ve karışıklık ortadan kaldırılmaktadır.

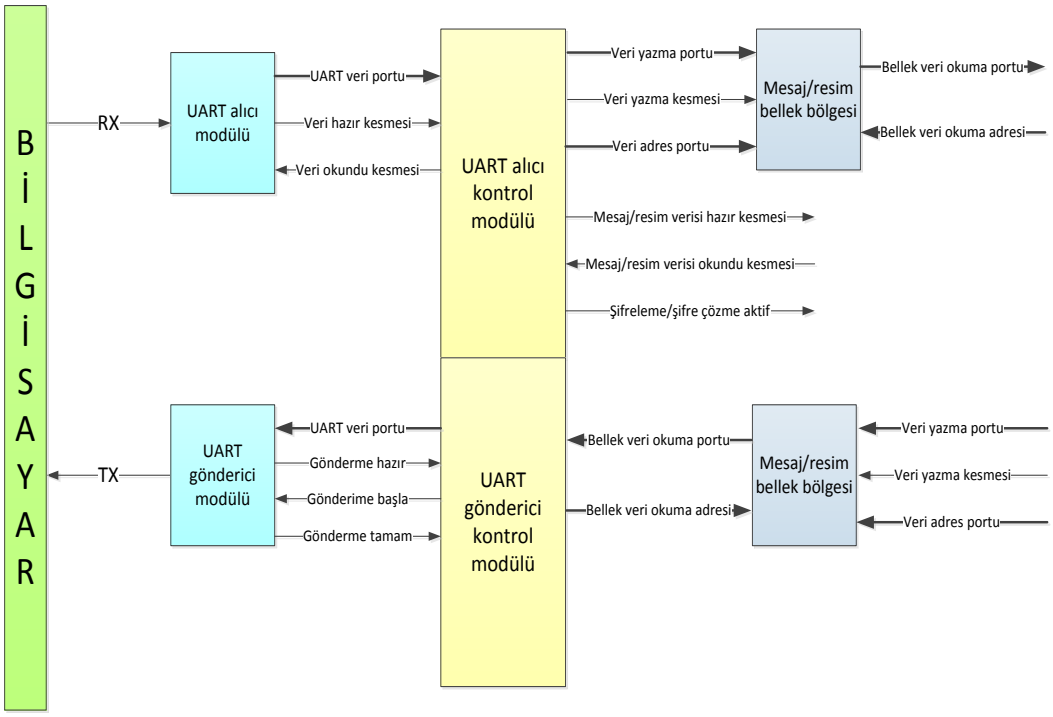
UART alıcı ana modülü, kullanıcı arayüz programından bilgisayar üzerindeki seri port haberleşmesi kullanılarak FPGA kartına gönderilen mesaj, resim ve kontrol verilerinin alınmasını, mesaj ve resim verisi olması durumunda bellek bölgesine yazılmasını ve kontrol verisi olması durumunda modüllerin aktive edilmesini (şifreleme, şifre çözme ve ses giriş ana modülleri) sağlamaktadır.

UART alıcı ana modülü, UART alıcı kontrol modülü ve UART alıcı modülü olmak üzere iki alt modülden oluşmaktadır.

UART alıcı modülü, standardın belirttiği zamanlama diyagramları, sembol zamanları, veri, eşlik ve bitiş bitlerinin sayısını göz önüne alarak alt seviyede FPGA ile bilgisayar arasındaki seri port haberleşmesini sağlayan yazılımsal kod parçasıdır. Seri port arayüzü üzerinden gelen verileri alarak UART alıcı kontrol modülüne bu arayüzden gelen veriyi iletmekle görevlidir.

UART alıcı kontrol modülü, UART alıcı modülünden gelen verileri yorumlayarak bu verileri bellek bölgelerine yazmak ve şifreleme modülüne veri hazır kesmesi göndermek veya kontrol baytlarına göre modülleri aktive etmekle görevlidir.

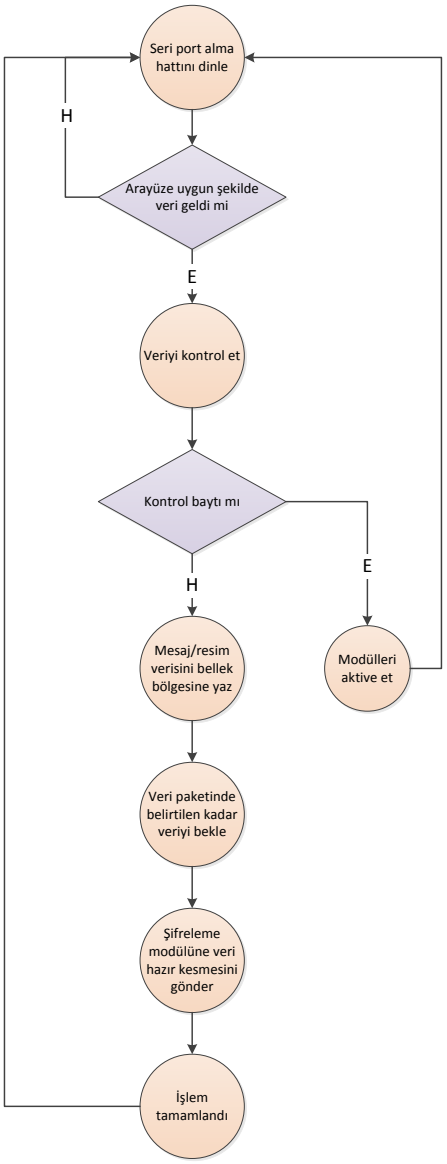
UART arayüzü alıcı ve gönderici ana modülleri blok şeması Şekil 4-14'de verilmektedir.



Şekil 4-14 : UART alıcı/gönderici ana modülü blok şeması.

UART alıcı ana modülü sözde kod akışı Şekil 4-15'de verilmektedir.

Şekil 4-15'deki sözde akış şemasından da anlaşılacağı üzere UART alıcı modülü, sistemin RX hattını dinleyerek haberleşmenin başlayıp başlamadığını kontrol eder. Haberleşmenin başladığını gösteren başlangıç sembolü gelmişse aynı hat üzerinden veri bitlerini ve eşlik bitini alır. Veri bitlerini "xor" işlemine tabi tutarak çıkan değerle eşlik bitini karşılaştırır. Doğru sonuç elde etmesi durumunda, UART alıcı kontrol modülüne 8 bitlik veriyi iletir. Kontrol modülü, bilgisayar ile belirli bir paket formatında haberleştiği için gelen ilk bayta göre ne tür bir işlem yapacağına karar verir. Kontrol baytı olması durumunda modülleri aktive eder, mesaj/resim verisinin başlangıç baytı olduğunda uzunluk baytına bakarak gelen verileri bellek bölgesine kaydeder. Tüm veriler alındıktan sonra, şifreleme algoritmasına verinin hazır olduğunu bildirir.



Şekil 4-15 : UART alıcı ana modülü sözde kod akışı.

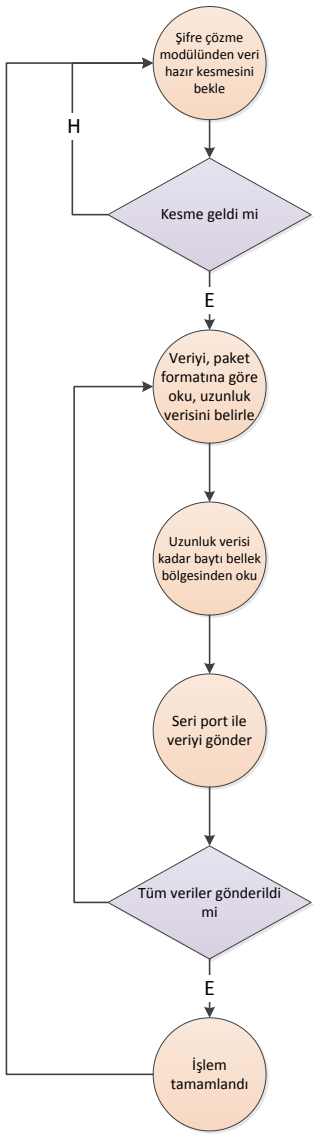
UART gönderici ana modülü, UART gönderici kontrol modülü ve UART gönderici modülü olmak üzere iki alt modülden oluşmaktadır.

UART gönderici modülü, standardın belirttiği zamanlama diyagramları, sembol zamanları, veri, eşlik ve bitiş bitlerinin sayısını göz önüne alarak alt seviyede FPGA ile bilgisayar arasındaki seri port haberleşmesini sağlayan yazılımsal kod parçasıdır. Kendine iletilen veriyi seri port arayüzü üzerinden bilgisayara göndermektedir.

Karşı kullanıcıdan gelen veriler, kablosuz haberleşme biriminden geçip şifre çözme bloğuna iletildikten sonra paket formatındaki başlangıç baytlarına göre mesaj ve resim verisi UART gönderici modülünün bellek bölgesine yazılır. Veriler yazıldıktan sonra verinin hazır olduğu UART gönderici ana modülüne iletilir. Baytlar halinde

okunan veri paket formatı içeriğiyle bilgisayardaki kullanıcı arayüz programına gönderilir. Tüm verilerin gönderimi bittikten sonra şifre çözme modülüne verilerin okunduğu bilgisi gönderilir ve işlevine devam etmesi sağlanır.

UART gönderici ana modülü sözde kod akışı Şekil 4-16'de verilmektedir.



Şekil 4-16 : UART gönderici ana modülü sözde kod akışı.

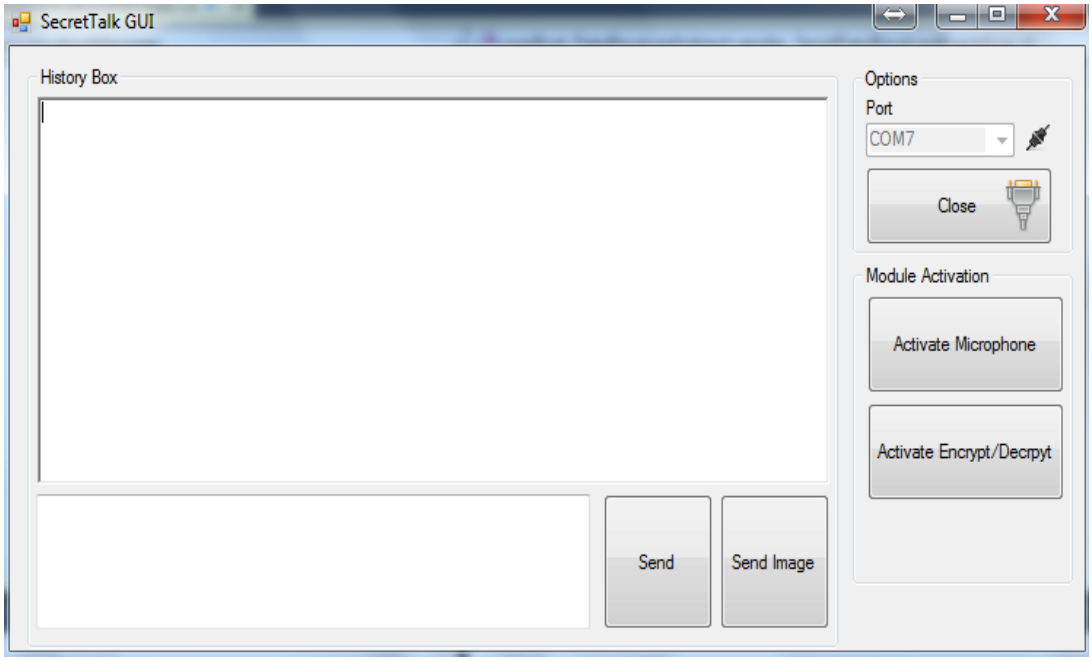
4.2 Kullanıcı Arayüzü Yazılımı

Sistemde, donanımsal altyapının yanı sıra bu yapıya ek yazılımsal birimler de bulunmaktadır. VHDL ile oluşturulan ve donanımı kontrol eden yazılım modülleriyle birlikte kullanıcı tarafındaki arayüzü sağlayan, kontrol verilerini göndermesi ve

mesaj ve resim verilerini gönderip alabilmesi için özelleşmiş arayüz programı oluşturulmuştur.

Kullanıcı arayüz programı C# dili kullanarak oluşturulmuş bir bilgisayar programıdır. Bu program, kullanıcıya sunduğu pencereler ve seçim noktalarından aldığı verileri seri port üzerinden FPGA kartına göndermekte, FPGA kartından seri port ile gönderilen verileri de ekrandaki pencerelerde gösterebilmektedir.

Kullanıcı arayüz programına ait ekran çıktısı Şekil 4-17'te verilmektedir.



Şekil 4-17 : Kullanıcı arayüz programı ekran çıktısı.

Mesaj ve resim verileri gönderilirken veri paketleme işlemini kullanıcı arayüzü gerçekleştirir. Mesaj kutularına veri girdisi yapılması durumunda, girilen veriyi kullanıcı arayüzü paketler. Resim verisi için de aynı işlemi yapar. Mesaj ve resim verileri bir paketin boyu olan 95 baytı geçmesi durumunda yeni paketleri otomatik olarak oluşturur. Kullanıcı dilediği boyutta ve uzunlukta resim ve mesaj verisi tanımlayabilir.

5. AES (ADVANCED ENCRYPTION STANDARD) ALGORİTMASI

5.1 AES Algoritmasının Tarihçesi

Amerika Birleşik Devletleri Ulusal Standart ve Teknoloji Enstitüsü (National Instute of Standards and Technology, NIST) mevcut şifreleme algoritmalarının güvenilirlik düzeyinin gelişen teknolojiye ayak uyduramaması üzerine yeni bir kripto algoritması geliştirilmesi üzerine bilim adamlarına çağrıda bulunmuştur. 1997 yılında başlatılan çalışmaların ardından detaylı analizler sonucunda beş algoritma finale seçilmiştir. Bunlar, IBM tarafından geliştirilen MARS algoritması, Ronald Rivest tarafından geliştirilen RC6, Joan Daemen ve Vincent Rijmen tarafından geliştirilen Rijndael, İngiltere - İsrail – Norveç tarafından geliştirilen Serpent ve Bruce Schneier tarafından geliştirilen Twofish algoritmalarıdır [14].

Finale kalan algoritmalar üzerinde yapılan ve dört seneyi bulan çalışmalar sonucunda Belçikalı bilim adamları Joan Daemen ve Vincent Rijmen tarafından geliştirilen Rijndael algoritmasını Gelişmiş Şifreleme Standardı (Advanced Encryption Standard, AES) olarak belirlemişlerdir [14].

Rijndael algoritması, hem donanım hem de yazılım kaynaklarını kullanma bakımından diğer algoritmalara göre üstün özelliklere sahiptir. Algoritmanın çok düşük hafıza gereksinimi, alan kısıtlı uygulamalar için algoritmayı uygun kılmaktadır. Algoritmanın matematiksel yapısı da zaman ve güç ile yapılan saldırılara karşı çok dirençlidir [14].

2001 yılında NIST tarafından standartlaştırılan AES algoritması, ilk olarak Amerika'da elektronik verilerin şifrelenmesi için kullanılmaya başlanmış ve devamında tüm dünyada en çok kullanılan şifreleme algoritması olmuştur.

5.2 AES Algoritması ve Algoritmik Yapısı

Rijndael algoritması, değişken giriş verisi blok uzunluğu ve değişken anahtar uzunluğunu desteklemektedir. Giriş verisi blok uzunluğu ve anahtar uzunluğu en az 128 bit ve en çok 256 bit olmak üzere 32 bitin katları şeklinde seçilebilmektedir.

AES adı altında gerçeklenen algoritmada, Rijndael algoritmasının verdiği destekten farklı olarak giriş verisi blok uzunluğu 128 bit olarak sabit tutulmaktadır. Anahtar uzunlukları ise 128 bit, 192 bit ve 256 bit olarak seçilebilmektedir. Rijndael algoritmasında belirlenebilen farklı giriş verisi bloğu ve anahtar uzunlukları AES kapsamına alınmamıştır. Bu nedenle, AES algoritması anahtar uzunluğuna göre AES-128, AES-192 ve AES-256 olarak isimlendirilmektedir.

Tez boyunca anlatılacak ve teze konu olan çalışmada gerçekleştirilen AES-128 algoritmasıdır.

Blok şifreleme algoritmaları, giriş verisi sabit uzunlukta olan ve işlemlerin bu sabit bloklar üzerine uygulandığı algoritmalardır. Genel olarak, yüksek miktarda verinin şifrelenmesine yönelik algoritmalarda tercih edilen bir yaklaşımdır [23].

Simetrik anahtarlı şifreleme algoritmaları, hem şifreleme (encryption) hem de şifre çözme (decryption) işlemlerinde aynı anahtarı kullanan algoritmalardır. Simetrik şifreli algoritmalar arasında, Twofish, Serpent, AES(Rijndael), Blowfish, CAST5, RC4, 3DES, IDEA bulunmaktadır.

AES algoritmasında giriş verisinin uzunluğu standarda göre 128 bit olarak sabitlenmiştir. AES algoritmasında, aynı anahtar ile şifreleme ve şifre çözme işlemleri gerçekleştirilmektedir. Bu özelliklerinden dolayı, AES algoritması, blok ve simetrik anahtarlı şifreleme algoritmasıdır.

5.2.1 Algoritmik yapı

AES algoritmasının en temel yapı taşını baytlar oluşturur. Algoritmanın belirttiği her bir adım 4x4 sütun-temelli bayt matrisi yapısı üzerinde gerçekleştirilir. Bu matris yapısına durum(state) adı verilmektedir.

128 bitlik giriş verisi, her bir $a_{(x,y)}$ 8 bitlik veriyi göstermek üzere Denklem 5-1'de verilmektedir.

$$G(i) = a_{(0,0)}\ a_{(1,0)}\ a_{(2,0)}\ a_{(3,0)}\ a_{(0,1)}\ a_{(1,1)}\ a_{(2,1)}\ a_{(3,1)}\ a_{(0,2)}\ a_{(1,2)}\ a_{(2,2)}\ a_{(3,2)}\ a_{(0,3)}\ a_{(1,3)}\ a_{(2,3)}\ a_{(3,3)} \quad \textbf{(5-1)}$$

128 bitlik giriş verisi için 4x4 sütun temelli matris yapısı Şekil 5-1'de verilmektedir. Algoritmanın başlangıç durumu, 128 bitlik veriyi 8 bitlik verilere bölerek Denklem 3-1'de verilen şekilde indislendirildikten sonra Şekil 5-1'de verilen matris yapısına oturtmakla oluşturulmaktadır. Algoritmadaki tüm fonksiyonlar da bu matris üzerine uygulanmaktadır.

$a_{(0,0)}$	$a_{(0,1)}$	$a_{(0,2)}$	$a_{(0,3)}$
$a_{(1,0)}$	$a_{(1,1)}$	$a_{(1,2)}$	$a_{(1,3)}$
$a_{(2,0)}$	$a_{(2,1)}$	$a_{(2,2)}$	$a_{(2,3)}$
$a_{(3,0)}$	$a_{(3,1)}$	$a_{(3,2)}$	$a_{(3,3)}$

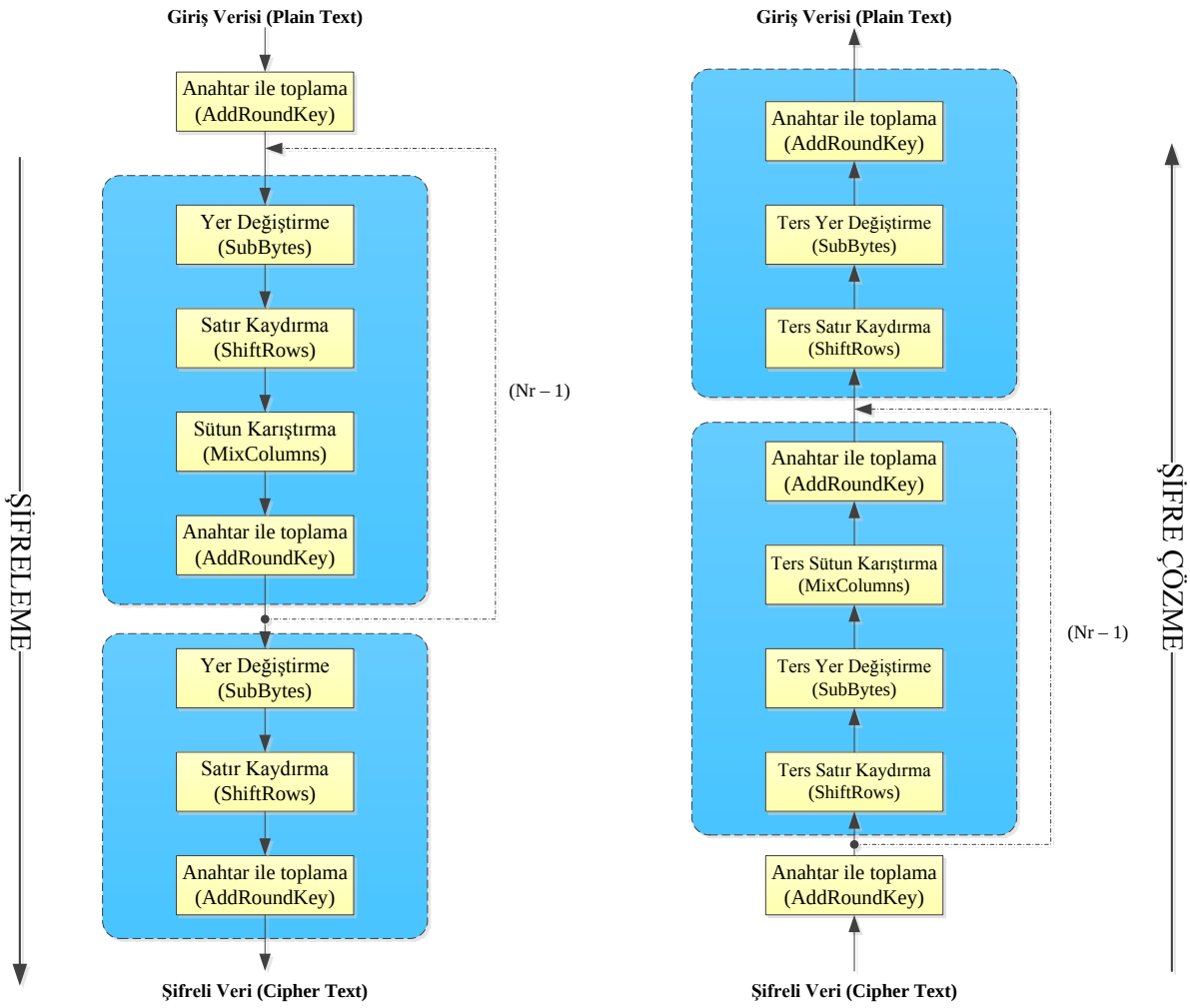
Şekil 5-1 : 4x4 sütun temelli matris yerleşimi.

AES algoritması, temel olarak dört farklı fonksiyonun durum matrisleri üzerine uygulanması ile gerçekleştirilmektedir. Her bir fonksiyonun çıkışında diğer fonksiyonun giriş durum matrisi oluşmaktadır. Bu fonksiyonlar aşağıda verildiği şekildedir;

1. Anahtar ile toplama (AddRoundKey)
2. Yer Değiştirme (SubBytes)
3. Satır Kaydırma (ShiftRows)
4. Sütun Karıştırma (MixColumns)

Yukarıda verilen fonksiyonlar, anahtar uzunluğuna göre değişen sayılarda durum matrisleri üzerine uygulanmaktadır. *Nr,* döngü sayısı olmak üzere; 128 bit anahtar için *Nr* = 10, 192 bit anahtar için *Nr* = 12, 256 bit anahtar için *Nr* = 14'tür.

AES algoritmasının akış şeması Şekil 5-2'de verilmektedir.



Şekil 5-2 : AES algoritmasının akış şeması.

5.2.1.1 Anahtar ile toplama (addroundkey)

Anahtar Genişletme Rutini (Key Expansion Routine) adı verilen işlemde, belirli bir yordam kullanılarak ana anahtardan her bir döngüde kullanılacak alt anahtarlar üretilir. *Nr*, döngü sayısı olmak üzere; AES-128'de *Nr* + 1 = 11; AES-192'de *Nr* + 1 = 13; AES-256'da *Nr* + 1 = 15 adet alt anahtar dizisi mevcuttur.

Anahtar ile toplama fonksiyonu, bit bazında XOR işlemine karşılık gelmektedir. Üretilen alt anahtarlar ile durum matrisleri, birbirleriyle aynı aynı indisli döngülerde "xor" işlemine tabi tutulmaktadır.

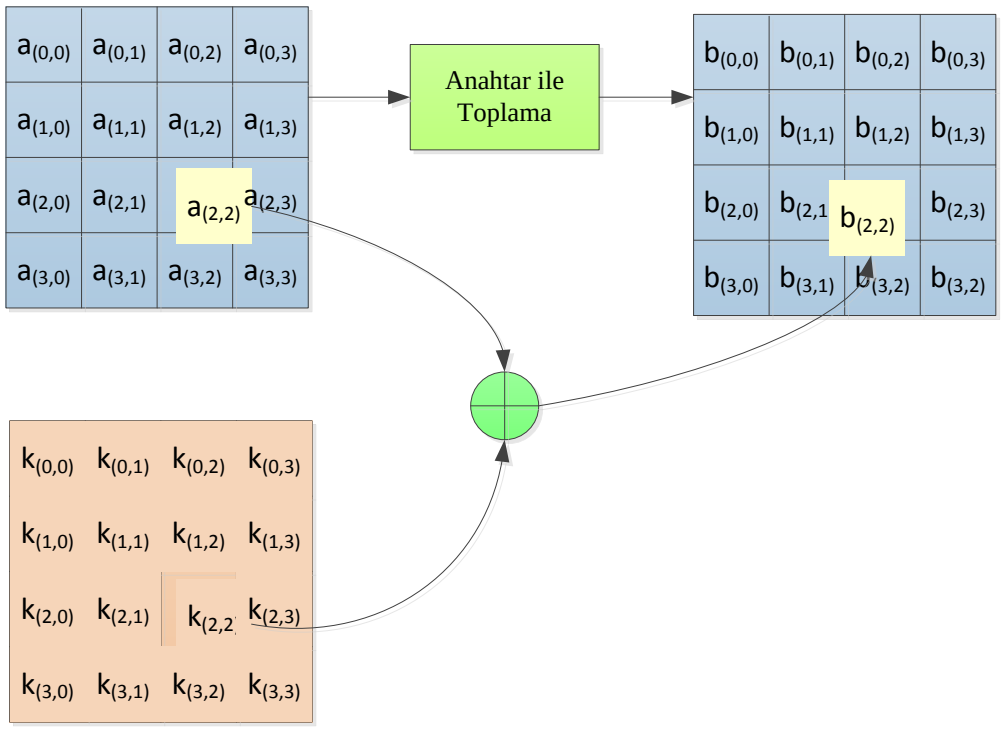
Örneğin; 3.döngüdeki durum matrisindeki veri

G(3) = 0x291045821FD2EFC89A043607DCB7E32C,

anahtar üretme rutininde ile oluşturulmuş ve 3.döngüde kullanılacak alt anahtar verisi K(3) = 0x432109477829347423 90DFE1CB37982A olmak üzere;

G(3) xor K(3) = 0x6A314CC567FBDBBCB994E9E617807B06 olarak hesaplanır.

Anahtar ile toplama işlemi, Şekil 5-3'te verilmektedir.



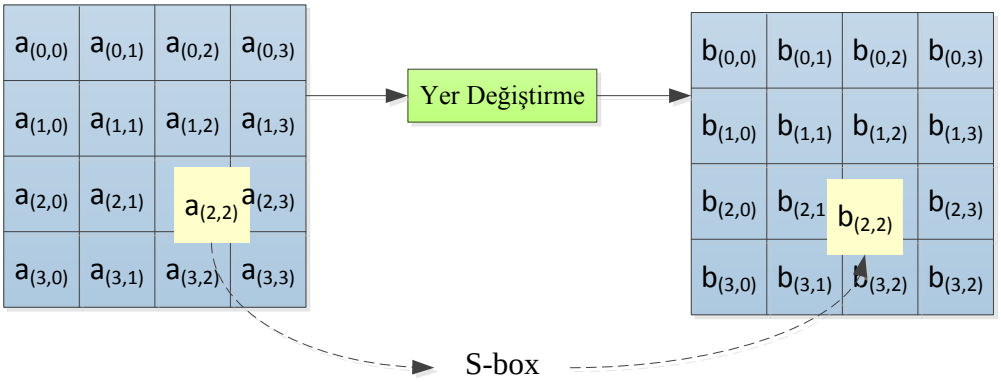
Şekil 5-3 : Anahar ile toplama işlemi.

5.2.1.2 Yer değiştirme (subbytes) ve ters yer değiştirme (invsubbytes)

Şifreleme algoritmalarının en temel ve güvenilirlik sağlayan yapıları doğrusal olmayan dönüşümler gerçekleştirmeleridir.

Yer değiştirme işlemi, yer değiştirme matrisi (substitution box, S-box) kullanılarak yapılan ve doğrusal olmayan bir dönüşümdür. Durum matrisindeki her bir baytın en anlamlı dört biti ile en anlamsız dört bitinin yer değiştirme matrisinde kesiştiği noktadaki verinin yeni durum matrisi oluşturmasıyla gerçekleştirilmektedir.

Yer değiştirme işleminin durum matrisi üzerinde uygulanması Şekil 5-4'te verilmektedir.



Şekil 5-4 : Yer değiştirme işlemi.

Yer değiştirme matrisi, Şekil 5-5'te verilmektedir.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Şekil 5-5 : Yer değiştirme matrisi.

Örneğin; $a_{(1,0)}$ = 0xE7 olmak üzere, bu verinin en anlamlı ilk dört biti $a_{(1,0)}[7:4]$ = 0xE, en anlamsız son dört biti $a_{(1,0)}[3:0]$ = 0x7'dir. Yer değiştirme matrisinin düşey ekseni en anlamlı veriyi, yatay ekseni en anlamsız veriyi göstermek üzere yer değiştirme işlemi sonucu $a_{(1,0)}$ = 0xE7 olmak üzere; $b_{(1,0)}$ = 0x94 olarak bulunur.

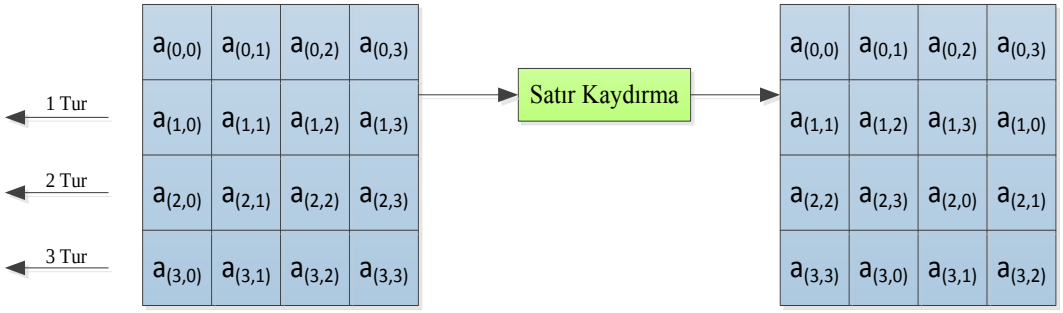
Ters yer değiştirme işlemi, bu rutinin tam tersidir ve aynı yer değiştirme matrisi üzerinden $b_{(1,0)}$ verisi kullanılarak $a_{(1,0)}$ verisine ulaşılmaktadır.

5.2.1.3 Satır kaydırma (shiftrows) ve ters satır kaydırma (invshiftrows)

Satır kaydırma işlemi, durum matrisine satır bazında uygulanan kaydırma işlemidir. İlk satırın indisi 0, ikinci satırın indisi 1, üçüncü satırın indisi 2 ve dördüncü satırın

indisi 3 olmak üzere satırlardaki baytların indis sayıları kadar sola kaydırılması işlemidir.

Satır kaydırma işlemi, Şekil 5-6'da verildiği şekilde gerçekleştirilmektedir.



Şekil 5-6 : Satır kaydırma işlemi.

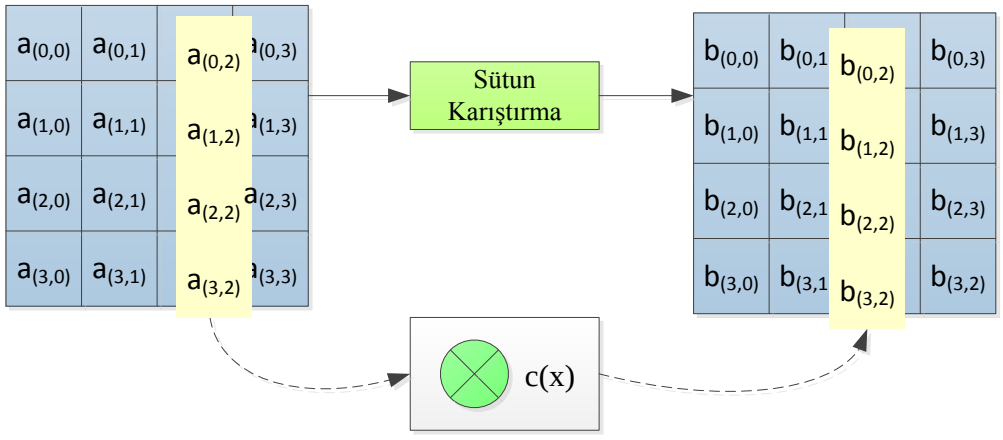
Ters satır kaydırma işlemi, şifre çözme işlemlerinde satır kaydırma işlemiyle aynı şekilde uygulanmaktadır.

5.2.1.4 Sütun karıştırma(mixcolumns) ve ters sütun karıştırma(invmixcolumns)

Sütun karıştırma işlemi, durum matrisinin her bir sütunundaki verilerin sabit bir polinomla çarpılması işlemidir.

Çarpan polinomu *c(x)* olmak üzere; $c(x) = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}$ şeklindedir.

Sütun karıştırma işleminin gösterimi, Şekil 5-7'de verilmektedir.



Şekil 5-7 : Sütun karıştırma işlemi.

c(x) polinomundaki '1' değerin aynısının alınacağı, '2' değerin iki kere sola kaydırılacağı, '3' değerin iki kere sola kaydırıldıktan sonra ilk değerle 'xor' işlemine

tabi tutulacağı anlamına gelmektedir. Denklem 5.2'de durum matrisi sütunu ile *c(x)* polinomunun çarpım denklemi verilmektedir.

$$\begin{bmatrix} b1 \\ b2 \\ b3 \\ b4 \end{bmatrix}_{1x4} = \begin{bmatrix} a1 \\ a2 \\ a3 \\ a4 \end{bmatrix}_{1x4} x \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}_{4x4} \quad \textbf{(5-2)}$$

Yukarıda matris elemanları üzerine uygulanan çarpma işlemi sonucunda herhangi bir sonuç verisi 0xFF değerinden büyük çıkarsa fonksiyon gereği 0x1B değeri ile xor işlemine tabi tutulur ve çıkan sonuç değerlendirmeye alınır.

Ters sütun karıştırma işlemi, durum matrisi şifreli veri durum matrisi üzerine yukarıda bahsedilen işlemlerin uygulanması ile gerçekleştirilmektedir.

5.3 AES Algoritmasının Karmaşıklığı ve Bilinen Ataklar

Şifreleme algoritmalarında, kullanılan anahtarın uzunluğu basit anlamda algoritmanın kırılma güçlüğünü göstermektedir. Algoritmanın direnci, algoritmik akışta belirtilen işlemlerin karmaşıklığından ve doğrusal olmayan dönüşümler içermesinden ileri gelmektedir. AES algoritması, anahtar verisinin uzun olması ve doğrusal olmayan dönüşümler içermesinden – S-box dönüşümü – dolayı direnci yüksek algoritmalar arasındadır.

Algoritmaların işlem karmaşıklığı, anahtar uzunluğu *N* olmak üzere, 2^N olarak hesaplanmaktadır.

Çizelge 5.1'de anahtar uzunluğu ile kombinasyon sayıları verilmektedir.

Şifreleme algoritmalarına yönelik birçok atak yöntemi bulunmaktadır. Bilinen en temel atak yöntemi, tekil deneme atağıdır(brute-force attack). Bu yöntemde, tüm anahtar kombinasyonları sistematik olarak denenerek şifreli veriden normal veriye ulaşılmaya çalışılır.

Tekil deneme atağı için gerekli olan işlem gücü, anahtar uzunluğuna bağlı olarak üssel artış gösterir. 128 bitlik AES algoritmasının kırılabilmesi için, anahtar uzayında 3.4×10^{38} farklı kombinasyonun denenmesi gerekmektedir. Anahtar kırma işlemi için özel donanımsal tasarımlar bulunmaktadır. FPGA ve grafik işlemcileri kullanarak tasarımlar gerçekleştirilmiştir. Bunların yanı sıra, süperbilgisayarlar da şifre kırma işlemleri için kullanılmaktadır.

Çizelge 5.1 : Anahtar uzunluğu – Kombinasyon sayısı ilişkisi.

Anahtar uzunluğu	Kombinasyon sayısı
1-bit	2
2-bit	4
4-bit	16
8-bit	256
16-bit	65536
32-bit	4.2×10^{9}
56-bit (DES)	7.2×10^{16}
64-bit	1.8×10^{19}
128-bit (AES)	3.4×10^{38}
192-bit (AES)	6.2×10^{57}
256-bit (AES)	1.1×10^{77}

Dünyanın en hızlı süperbilgisayarı Çin tarafından üretilen Tianhe-2'nin [24] işlem gücü 33.86 petaflops'tur. Petaflops, kayan sayı aritmetiğine göre bir saniyede yapılan işlem sayısıdır.

AES algoritmasında bir şifrenin denenmesi için gerekli olan işlem sayısı 1000 olarak farz edilir ise; bir saniyede yapılacak deneme sayısı $33.86 \times 10^{15} / 1000 = 33.86 \times 10^{12}$'dir. Bir yılda, 60 x 60 x 24 x 365 = 31536000 saniye vardır. Tianhe-2 süperbilgisayarı ile AES anahtar kombinasyonlarını denemek için gerekli olan süre; $3.4 \times 10^{38} / (33.86 \times 10^{12} \times 31536000) = 3.18 \times 10^{17}$ yıldır. Dünyanın yaşının 5 milyar yıl olduğu düşünülürse gereken zaman dünyanın yaşının milyarlarca katıdır.

5.4 Uygulama Alanları

AES algoritması, hem donanımsal hem de yazılımsal olarak kolay gerçeklenebilir olması nedeniyle birçok alanda ve uygulamada kullanılmaktadır. Bunun yanı sıra, güvenlik düzeyinin yüksek olması da gizli seviye uygulamalar için idealdir.

AES algoritmasının uygulama alanları şu şekilde sıralanabilir;

- Haberleşme güvenliği uygulamaları,

- Veri güvenliği uygulamaları,
- Görüntü / ses uygulamaları,
- Ağ güvenliği uygulamaları.

Haberleşme güvenliği, özellikle ülkeler bazında azami derecede dikkat gösterilen bir alandır. Diplomatik ve üst düzey veri trafiği, bankalar arası veri trafiği, kurumlar arası veri trafiği ve insanların bankalarla, kurumlarla ve özel amaçlı olarak gerçekleştirdikleri haberleşmelerin gizliliği çok önemlidir. Herhangi bir alanda, gizli veriye ulaşılmaya çalışılması ve bu verilerin değiştirilmesi, açığa çıkarılması ve kullanılması günümüz dünyasında telafisi mümkün olmayan sorunlara sebep olabilmektedir.

Yakın zamanda, Wikileaks adlı internet sitesinin kurucusu olan Julian Assange isimli Avusturalyalı bir bilgisayar programcısının dünyaya sızdırdığı bilgiler, özellikle Amerika'yı büyük sıkıntıya sokmuş ve diğer ülkelerle sorunlar yaşamasına sebep olmuştur.

Teknolojinin bu denli ilerlediği ve yasadışı yollarla ülkelere ait bilgilere bile ulaşılabiliyor olmanın veri güvenliğinin ne derece dikkat edilmesi gereken bir konu olduğunu gözler önüne sermektedir.

Ağ güvenliği, internet gibi dünya çapında olan ve intranet gibi yerel ağların da güvenliğinin sağlanması amacıyla şifrelemeye ihtiyaç duymaktadır. Birçok özel bilginin internet aracılığıyla kişisel bilgisayarlarımızdan internet dünyasına açılıyor olması, bu bilgileri tehdit altında bırakmaktadır.

İnternet üzerinden birçok kişinin kişisel bilgilerini edinerek banka hesaplarına giren birçok kişi haberlere konu olmuştur ve olmaktadır.

5.5 AES Algoritmasının Önerilen Sistemdeki Rolü

AES algoritması günümüzde veri şifrelemesinde en ileri düzeyde güvenlik sağlayan algoritmadır. Bilinen tüm saldırı yöntemlerine başarıyla karşı koyan bu algoritma şu anda bile birçok ülkenin veri güvenliğinde tercih ettiği algoritmalar arasında sayılmaktadır.

Günümüzde teknolojinin de gelişmesiyle oldukça artan yasadışı şekilde verilerin ele geçirilmeye çalışılmasına karşı en güvenli yöntem şifreleme işlemidir.

Tez kapsamında sunulan yöntem, kablosuz haberleşme yapan iki kullanıcı arasında veri alış-verişini sağlayabilmektedir. Bu özelliğine ek olarak, verinin güvenli şekilde iletimini sağlayabilmek amacıyla şifrelenmesi düşünülmüş ve gerçekleştirilmiştir. Bu çalışma kapsamında, kablosuz haberleşme yapan iki kullanıcı arasında verinin şifrelenmesi AES-128 algoritmasıyla gerçekleştirilmektedir.

Ses, veri ve görüntü verilerini IEEE 802.15.4 WPAN standardına göre iletimini yapan sisteme aynı zamanda AES-128 algoritmasıyla şifreleme kabiliyeti kazandırılmış ve veri güvenliği sağlanmıştır.

6. SONUÇ VE ÖNERİLER

Bu çalışmada, FPGA tabanlı şifreli kablosuz haberleşme sisteminin detaylı tasarım mimarisi sunulmuştur. Sistemde kullanılan donanımsal birimler ve bu birimlerin işlevleri verilmiştir. Sistemin işlevselliğini sağlayan yazılım modüllerinin detaylı anlatımı yapılmıştır.

Şifreleme algoritması olarak bilinen saldırı tiplerine karşı en dirençli algoritma olan seçilen AES algoritması seçilmiştir. AES algoritmasının algoritmik akışı ve matematiksel altyapısı sunulmuştur. FPGA gerçekleme adımları verilmiştir.

Sistemin düşük güçlü ve düşük maliyetli tasarlanması için gerçekleştirilen yaklaşımlar sunulmuştur.

Tezde önerilen sistem, mimarisi ve kabiliyetleri açısından üstün özelliklere sahip, birçok gerçek cihazla benzerlikleri olan bir tasarım olarak karşımıza çıkmaktadır. Ayrıca, düşük güç tüketimi, az kaynak kullanımı ve çalışma hızları bakımında literatürde önerilen birçok uygulamadan daha üstün olduğu sonucuna varılmaktadır.

İleride planladığım çalışmalarımdan ilki, mevcut donanımsal altyapıyı muhafaza ederek kablosuz haberleşmeyi sağlayan IEEE 802.15.4 Kişisel Alan Ağı Standardı çevresel birim kartı yerine kapsama alanı daha yüksek olan IEEE 802.11 standardını destekleyen çevresel birim kartını sisteme eklemektir. Bu değişiklik sonrasında, 20 m olan kapsama alanı 100 m'ye çıkarılabilecektir. Böylece, sistem daha geniş alanlardaki kullanıcıların haberleşmesini sağlayabilecektir.

Bu çalışmanın ardından, sistemdeki kullanıcı sayısını artıracak değişiklikleri sisteme uygulamak olacaktır. Mevcut sistemde, iki kullanıcı arasında veri alış-verişi sağlanmaktadır. Yazılımsal boyutta yapılacak bu değişiklikle birlikte farklı kullanıcılardan birbirlerine veri alış-verişi altyapısı kurulabilecektir.

Devamında, AES-128 algoritması yerine AES-256 algoritması gerçeklenerek sistemin saldırılara karşı güvenilirliği bilinen en yüksek seviyeye çıkarılmaya çalışılacaktır. Ayrıca, anahtar değiştirme ve üretme yöntemleri konusunda

literatürdeki çalışmalar incelenerek sistemin her bir haberleşme oturumundan sonra anahtar değiştirme rutini tanımlanacaktır. Bu sayede, ağı dinleyenlerin anahtarı ele geçirme olasılıkları azaltılmaya çalışılacaktır.

Planlanan çalışmalardan sonuncusu ise tüm sistemin çevresel modüllerini ve FPGA kartını da barındıracak şekilde tek kart haline çevrilmesi ve cihaz haline getirilmesidir. Cihaz, telsiz ve cep telefonu benzeri bir sistem olarak düşünülmekte ve her kullanıcı kendine ait cihaz ile güvenli haberleşme arayüzü üzerinden haberleşebilmesi planlanmaktadır.

KAYNAKLAR

[1] **Tse, D., Viswanath, P.** (2005). Fundamentals of Wireless Communication, Cambridge University Press, ISBN-10:0521845270, England.

[2] **Paar, C., Pelzl, J., Preneel B.** (2011). Understanding Cryptography: A Textbook for Students and Practitioners, Springer, ISBN-10:3642041000.

[3] **Deamen, J., Rijmen, V.** (1999). AES Proposal, Rijndael (Version 2),

http://csrc.nist.gov/CryptoToolkit/aes/rijndael/Rijndaelammended.pdf

[4] **N.I.S.T** (2001). FIPS 197 : Advanced Encryption Standard, America.

[5] **Sood, M., Wagh, M., Cheema, M.** (2013). Implementation of a Wireless Communication System – A Review, *International Journal of Computer Applications,* Vol. 63, 45-50.

[6] **Paul, R., Saha, S., Sau, S., Chakrabarti, A.** (2012). Design and Implementation of Real Time AES-128 on Real Time Operating System for Multiple FPGA Communication.

[7] **Sood, M., Wagh, M., Cheema, M.** (2013). A Review on Various Data Security Techniques in Wireless Communication System, *International Journal of Engineering Research and Applications(IJERA),* Vol. 3, 883-890.

[8] **Song, O., Kim, J.** (2011). Compact Design of Advanced Encryption Standard Algorithm for IEEE 802.15.4, *Journal of Electrical Engineering and Technology,* Vol. 6, 418-422.

[9] **Bulens, P., Standaert, F. X., Quisquater, J. J., Pellegrin, P., Rouvor, G.** (2008). Implementation of AES-128 on Virtex-5 FPGA, *AfricaCrypt 2008, Lecture Notes on Computer Science,* Vol. 5023, 16-26, Fas.

[10] **Doğan, A. Y.** (2008). AES Algoritmasının FPGA Üzerinde Düşük Güçlü Tasarımı, *İstanbul Teknik Üniversitesi Fen Bilimleri Enstitüsü Yüksek Lisans Tezi,* 88 sayfa, Türkiye.

[11] **Kaur, A., Bhardwaj, P., Kumar, N.** (2013). FPGA Implementation of Efficient Hardware for the Advanced Encryption Standard, *International Journal of Innovative Technology and Exploring Engineering,* Vol. 2, 186-189.

[12] **Rais, M. H., Qasim, S. M.** (2010). Virtex-5 FPGA Implementation of Advanced Encryption Standard Algorithm, *Power Control and Optimization 3rd Global Conference*, 201-205.

[13] **Maxfield, C.** (2004). The Design Warriors Guide to FPGA : Devices, Tools and Flows, Newnes Publish, ISBN-10:0750676043.

[14] **Daemen, J., Rijmen, V.,** (2002) The Design of Rijndael – AES The Advanced Encryption Standard, Springer, ISBN-10:3540425802.

[15] www.bilgem.tubitak.gov.tr/sid/4/cid/9822/index.htm, alındığı tarih:12.12.2013

[16] http://esdcryptophone.com/products/mobile, alındığı tarih:12.12.2013

[17] http://ww2.nabishi.com/nab-admin/index.php/secure-gsm-mobiles/secure-voice-gsm/, alındığı tarih: 09.12.2013

[18] http://www.tripleton.com/products/secure-phones/secure-mobile-phone.htm, alındığı tarih: 05.12.2013

[19] https://www.gold-lock.com/en/home/, alındığı tarih: 05.12.2013

[20] http://www.snapdefense.com/, alındığı tarih: 05.12.2013

[21] http://www.digilentinc.com/Products/Catalog.cfm?NavPath=2,401&Cat=9&CFID=3363319&CFTOKEN=71931738, alındığı tarih:10.12.2013

[22] http://en.wikipedia.org/wiki/IEEE_802.15.4, alındığı tarih:12.12.2013

[23] http://en.wikipedia.org/wiki/Block_cipher, alındığı tarih: 08.12.2013

[24] http://en.wikipedia.org/wiki/Supercomputer, alındığı tarih: 12.12.2013

ÖZGEÇMİŞ

Adı Soyadı: Ilgaz AZ

Doğum Yeri ve Tarihi: Alanya / 29.05.1986

Adres: Koru Mah. 2640. Sok. Çayyolu Çamlık Sit. 9/6 Yenimahalle / ANKA RA

E-Posta: ilgaz.az@outlook.com

Lisans: Kocaeli Üniversitesi, Elektronik ve Haberleşme Mühendisliği, 2008

Mesleki Deneyim ve Ödüller:

- **Uzman Sistem Mühendisi, SDT Uzay ve Savunma Tekn. (2012-…)**
- **Araştırmacı, TÜBİTAK BİLGEM İLTAREN (2010, 2012)**
- **Tasarım Mühendisi, PAVO Elektronik, (2009, 2010)**