<u>İSTANBUL TEKNİK ÜNİVERSİTESİ</u>

<u>ELEKTRİK - ELEKTRONİK FAKÜLTESİ</u>

FPGA ÜZERİNDE GÜVENLİ FOTOĞRAF MAKİNESİ GERÇEKLEMESİ

BİTİRME ÖDEVİ

Oğuz ŞEN

040040309

BÖLÜMÜ : ELEKTRONİK HABERLEŞME MÜHENDİSLİĞİ

PROGRAMI : ELEKTRONİK MÜHENDİSLİĞİ

Danışmanı : Yrd. Doç. Dr. Müştak Erhan Yalçın

MAYIS 2008

ÖNSÖZ

Proje sonunda sayısal sistem tasarımı ve FPGA tasarımı konusunda çok değerli tecrübeler edinildi. Çok zaman yanlış yapıldı ancak zamanla doğrusunu öğrenmek suretiyle ve geçmişteki hatalardan ders çıkarılarak sonunda son derece başarılı bir çalışma ortaya kondu.

Problemin tespitinden çözüm yolunun belirlenmesine, sistemin tasarlanmasından gerçeklenmesine kadar toplamda bir yıllık bir emeğin ürünü olan bu çalışmada;

Yardımlarını benden esirgemeyip bana çok değerli olanaklar sunan hocalarım Sayın Yrd. Doç. Dr. Müştak Erhan Yalçın ve Sayın Yrd. Doç. Dr. S. Berna Örs Yalçın'a teşekkürü bir borç bilirim.

Ayrıca bana her zaman sonsuz güven duyan ve hiçbir şekilde desteğini esirgemeyen aileme, kendilerine çok şey borçlu olduğum İstanbul Teknik Üniversitesi'nin saygıdeğer öğretim üyesi ve asistanlarına, sayesinde aradığımı bulduğum dostum Ramazan Yeniçeri'ye, Gömülü Sistem Tasarımı Laboratuvarı'ndaki değerli arkadaşlarıma ve diğer tüm dostlarıma çok teşekkürler.

Mayıs 2008 Oğuz ŞEN

İÇİNDEKİLER

ÖZET .... **iv**
SUMMARY .... **v**

1 GİRİŞ **1**

2 KULLANILAN DONANIM ve YAZILIMLAR **3**
2.1 FPGA Teknolojisi 3
2.2 Xilinx XC3S400 FPGA ve Geliştirme Kiti 6
2.3 Donanım Tanımlama Dilleri ve VHDL 7
2.4 Xilinx ISE 7
2.5 Kamera Modülü 8

3 FOTOĞRAFIN ÇEKİLMESİ ve RAM'e YAZILMASI **10**
3.1 Fotoğrafın Çekilmesi 10
3.2 RAM Kullanımı 11
3.2.1 RAM'den Okuma 12
3.2.2 RAM'e Yazma 12

4 HASH FONKSİYONU **14**
4.1 Kriptografi 14
4.2 Hash Fonksiyonları 15
4.2.1 Anahtarlı Hash Fonksiyonları 17

5 GÜVENLİ FOTOĞRAFIN OLUŞTURULMASI **18**
5.1 Bitmap Fotoğraf Formatı 18
5.2 Hash Çıktısının Fotoğrafa Gömülmesi 18
5.3 Bitmap Formatının Gerçeklenmesi 21

6 FOTOĞRAF MAKİNESİ ARAYÜZÜ **22**
6.1 Kullanıcı Arayüzleri 22
6.2 FPGA – Bilgisayar Arayüzü 23

7 BİLGİSAYARDA FOTOĞRAFIN BÜTÜNLÜĞÜNÜN TEYİT EDİLMESİ **24**

8 SONUÇLAR **26**

KAYNAKLAR **28**

ÖZGEÇMİŞ **29**

ÖZET

FPGA ÜZERİNDE GÜVENLİ FOTOĞRAF MAKİNESİ GERÇEKLEMESİ

Bu bitirme çalışmasında, FPGA (Sahada Programlanabilir Kapı Dizileri) üzerinde, çektiği fotoğrafın kriptografik özünü hesaplayarak fotoğraf içine gömen ve bu sayede verinin bütünlüğünü yani görüntünün yakalandığı andan sonra hiçbir şekilde bozulmadığını garanti eden bir 'Güvenli Fotoğraf Makinesi' tasarımı ve gerçeklemesi yapılmıştır.

Giderek sayısallaşan fotoğrafçılık ve bu fotoğrafları düzenlemeye yarayan bilgisayar programlarındaki gelişmeler, her gün gördüğümüz onlarca fotoğrafın orijinalliğinde kuşku yaratıyor. Böyle bir ortamda bilginin bütünlüğünün garantilenebilmesi özellikle de bazı uygulama alanlarında giderek önem kazanmaktadır.

Gerçeklenen fotoğraf makinesinin çekeceği fotoğraflar şifrelenmiş formatta olmayacaktır, yani çekilen fotoğraflar herkes tarafından görülebilecektir. Ancak çekilen bu fotoğraflar bilgisayarda herhangi bir fotoğraf düzenleme programı tarafından herhangi bir şekilde değiştirilirse, fotoğraf çekimi sırasında fotoğrafın içine gömülen '*iz sözcük*' sayesinde fotoğrafın orijinal formunu korumadığı belirlenebilecektir.

Gerçekleme FPGA üzerinde, tasarım VHDL ile yapılmıştır. Bu amaçla bir kamera modülü, FPGA kitine bağlanmış ve fotoğraf çekme işlemi gerçekleştirilmiştir. Daha sonra çekilen fotoğraf FPGA geliştirme kitinde bulunan RAM'e yazılmış ve fotoğraf piksel bilgisi üzerinde tek yönlü kriptografik Hash fonksiyonu koşturulmuştur. Sonuç sözcük standartlara bağlı kalmak koşuluyla fotoğraf içinde oluşturulan yeni bir alana gömülerek '*güvenli fotoğraf*' hazırlanmıştır.

Doğrulama işlemi Matlab ve Xilinx benzetim ortamında yapılmaktadır. Yazılan kod, fotoğrafın içindeki '*iz sözcük*' ve kendi elde ettiği Hash fonksiyonu sonucunu karşılaştırarak fotoğrafın orijinal olup olmadığını tespit edecek, böylece herhangi bir yanıltma teşebbüsünden sistem sahibi kurum korunmuş olacaktır.

Projenin; özellikle askeri ve adli alanda, ayrıca görsel medyada uygulama alanı bulabileceği düşünülmektedir.

SUMMARY

SECURE DIGITAL CAMERA IMPLEMENTATION ON FPGA

In this project, ‘Secure Digital Camera’ that calculates the cryptographic Hash result of the picture which is taken, and then embeds it into the picture in order to guarantee the integrity of the picture is designed and implemented on FPGA.

As the digital photography has penetrated the market and the image modification softwares have improved very much, that has resulted great suspicion about the integrity of the pictures we see everyday. In these circumstances to guarantee the integrity of the message becomes very important, especially in some areas of application.

The pictures taken by the designed machine are not in encrypted format, which means it is visible to the public. But in the case that these pictures are altered in anyway with one of the picture modification softwares, by the help of the ‘*trace word*’ which was embedded during picture taking process, it will be found out that the picture is not in the original form.

The implementation was held on FPGA, and VHDL was used for the design. For the stated purpose, a camera module was connected to the FPGA kit, and got a snapshot. Then the picture pixel information was written on the external RAM that is on the FPGA development kit, and one way cryptographic Hash function was run on this information. ‘*Secure Photograph*’ was finalized with embedding the output of the Hash function into the new identified area in the picture which is completely compatible with the picture standards.

The verification process takes place in Matlab and Xilinx simulation environment. The software compares the ‘*trace word*’ written in the picture, and the result it gets from the cryptographic Hash function calculation of the picture. This step discovers if the picture is in the form that was taken, in other words it is original. In this way, parties are prevented from diversion which would occur of the alteration of the picture.

It is supposed that the design may be useful for judicial, military cases or visual media.

1 GİRİŞ

Bu çalışmada giderek sayısallaşan fotoğrafçılık ve gelişen fotoğraf düzenleme programlarına karşı sayısal fotoğrafların delil niteliği taşımalarının güçlüğü problemine bir çözüm getirilmeye çalışılmıştır.

Günümüzde güvenlik, sürekli olarak daha çok endişe duyduğumuz unsurlardan biri haline gelmiştir. Bunda her geçen gün meydana gelen adli olayların sayısının artması en büyük nedendir. Bu adli olaylarda yetkilileri doğru hükme yönlendiren en önemli dayanak ise delillerdir. Ancak delillerin gerçekten olayın bir parçası mı yoksa tamamen düzmece bir hikâyenin unsurları mı olup olmadığını anlamak kimi zaman çok güçtür.

Fotoğraf makineleri yaygınlaşarak cep telefonlarımız ile sürekli yanımızda bulunur hale gelmiştir. Dolayısıyla olası bir adli olayda görsel deliller toplamak giderek daha da kolaylaşmakta ve yaygınlaşmaktadır. Ancak gelişen fotoğraf düzenleme programları pek çok zaman bu görsel delillerin inandırıcılığında bizleri şüpheye düşürmektedir.

Projede tasarlanan *Güvenli Fotoğraf Makinesi,* bu probleme bir çözüm bulmak ve adli makamlara bu konuda yardım etmek iddiasındadır. Tasarlanan makinenin adli ve askeri alanlar dışında görsel medyada da kullanım alanı bulabileceği düşünülmektedir.

FPGA'da gerçeklenen sistem, bir kamera modülü sayesinde görüntü almakta, bu görüntüyü FPGA geliştirme kiti üzerinde bulunan RAM'e yazmakta ve bu fotoğrafın üzerinde tek yönlü kriptografik Hash fonksiyonu koşturmaktadır. Bu şekilde oluşan 'Güvenli Fotoğraf' daha sonra bilgisayara gönderilerek kullanılmaktadır. Fotoğraf, kullanım sonrasında bir değişikliğe uğradığında bilgisayar tarafındaki yazılım, çekim sırasında oluşturulup fotoğrafın içine gömülen *iz sözcüğüne* bakarak fotoğrafın ilk çekim anındaki bütünlüğünü korumadığını ortaya çıkartmaktadır.

Tezde, gerçekleme sırasında kullanılan FPGA'dan ve FPGA teknolojisinden, donanım tanımlama dili VHDL'den, kriptografi ve Hash fonksiyonlarından kısaca bahsedilecektir.

Fotoğraf çekme, RAM kontrolü, Hash fonksiyonu, güvenli fotoğrafın oluşturulması, FPGA – bilgisayar ara bağlantısının kurulması ve oluşturulan *Güvenli Fotoğrafın* doğrulama işleminin adımları, bu işlemleri gerçeklemek için tasarlanan alt bloklar ayrıntılarıyla açıklanacaktır.

Kullanılan donanım ve yazılımlar bölümünde FPGA geliştirme kitinden, kamera modülünden, Xilinx ISE sayısal sistem geliştirme ortamından, ayrıca kısaca VHDL donanım tanımlama dilinden ve FPGA teknolojisinden bahsedilecektir.

Fotoğrafın çekilmesi ve RAM'e yazılması bölümünde kamera modülüne fotoğraf çektirebilmek için gerekli sinyalleri üreten sistem parçasından ve çekilen fotoğrafı RAM'e yazmak ve sonrasında da RAM'den okuyabilmek için RAM'e gerekli sinyalleri üreten sistem parçasından bahsedilecektir.

Hash fonksiyonu bölümünde kriptografi biliminden kısaca bahsedilecek, Hash fonksiyonlarının yapısı ve gerekliliği anlatılacaktır. Daha sonra bu işlem için tasarlanan sistem parçasının çalışması açıklanacaktır.

Güvenli fotoğrafın oluşturulması bölümünde oluşturulan fotoğrafın türü olan Bitmap formatından bahsedilecek, güvenli fotoğrafı oluşturan fikir açıklanacaktır.

Fotoğraf makinesi arayüzü bölümünde bilgisayar ile FPGA geliştirme kiti arasında kurulan RS232 bağlantısından, bu işlem için gerçeklenen sürücü devreden ve protokolden ayrıca fotoğraf makinesinin kullanıcı arabirimleri olan buton ve yedi parçalı led takımı sürücülerinden bahsedilecektir.

Bilgisayarda fotoğrafın bütünlüğünün test edilmesi bölümünde sistemin gerçekten de hedefine ulaştığı gösterilecek, bu amaçla bilgisayar tarafında gerçeklenen yazılımdan bahsedilecektir.

Sonuçlar bölümünde sistemin hedefleri ve sistem üzerinde ileriki dönemde yapılabilecek geliştirmelerden bahsedilecek VHDL tasarımda izlenen tasarım ilkeleri açıklanacaktır.

2 KULLANILAN DONANIM ve YAZILIMLAR

2.1 FPGA Teknolojisi

Sayısal elektronikte zaman içerisinde yaşanan gelişim çok büyük ölçekli sistemlerin tasarımını da beraberinde getirmiştir. Yarıiletken ve üretim teknolojilerinde gelinen nokta sayesinde bugün VLSI yongaları içerisinde milyonlarca transistor bulunmaktadır. Malzeme ve üretim teknolojilerinin daha iyi noktalara taşınmış olması bunun son ürünlere de yansıtılması gerekliliğini beraberinde getirmektedir. Nitekim gelişen teknoloji yanında tüketici istekleri de artan oranda büyümektedir.

Bilimdeki gelişmeleri mühendislik anlayışı içerisinde en kısa sürede ve verimlilikte tüketiciye ulaştırabilmek amacıyla yeni araç ve gereçler mühendislerin hizmetine sunulmaktadır. FPGA da sayısal tasarım mühendislerinin, bilimin yarattığı imkânları teknolojiye yansıtabilmesi için geliştirilmiş bir yongadır.

Bugün gelinen nokta itibariyle markette, FPGA üretimi alanında, çok fazla sayıda olmamakla birlikte çeşitli üretici firmalar mevcuttur. Bu firmaların geliştirdiği FPGA'lar da farklı mimarilere ve üretim teknolojilerine dayanmaktadır. Farklı mimarilerin ve teknolojilerin birbirlerine göre üstünlükleri, güvenlik, güç tüketimi, maliyet gibi alanlarda değişmektedir. [1]

FPGA'lar yani sahada programlanabilen kapı dizileri, PAL, PLA gibi mantıksal kapı dizilerine benzer mantıkta üretilen ancak onlardan çok daha üstün teknolojiye sahip yongalardır. İçlerinde bugün gelinen son teknolojiye göre milyonlarca mantıksal kapı barındıran FPGA'lar üzerinde gerçeklenecek olan sayısal devreler FPGA üreticisi firmanın bilgisayar destekli tasarım (CAD) araçları sayesinde tasarlanmakta ve yongalara yüklenmektedir.

FPGA'lar, üzerlerinde mantıksal kapı dizilerinden başka, hazır çarpıcı blokları, hazır RAM blokları, saat frekansı üretimi için DLL/PLL blokları ve hatta daha gelişmiş mimarilerde gömülü işlemci çekirdekleri bulundurmaktadır.

Bir sayısal tasarımda, gerçeklenen devrenin çalışabileceği en yüksek frekans değeri, gecikmenin en fazla yaşandığı kombinezonsal bloktaki gecikme miktarıyla ters orantılıdır. Yani devrede görülen en uzun gecikme *t* nanosaniye ise o tasarım en az *t* nanosaniye periyoda sahip saat işareti ile çalışabilir. Bloklardaki gecikme miktarları sadece kapı gecikmeleri değil, aynı zamanda kapılar arasındaki yollarda meydana gelen gecikmelerdir. Yarıiletken teknolojisinin gelişimi ve mikronaltı teknolojilerin pratikte uygulanmaya başlamasından itibaren bir zamanlar kapı gecikmelerinin yanında ihmal edilen yol gecikmeleri de hesaba katılmak durumunda kalmıştır.

İşte bu nedenle FPGA'larda kullanılan yarıiletken teknolojisi ile bağlantılı olarak, tasarımlar da farklı FPGA'larda farklı saat frekanslarında çalışabilmektedir. Esasında bu durum her geçen gün iyiye gitmektedir, bu projede yapılan tasarım kullanılan FPGA üzerinde yaklaşık 65 MHz saat frekansında çalışılmasına izin verirken daha yeni teknolojiye sahip başka bir FPGA üzerinde 80-90 MHz'de çalışılmasına imkan tanıyabilmektedir.

Yine aynı şekilde üzerinde daha fazla sayıda mantıksal birim ve daha büyük boyutlarda RAM blokları bulunduran FPGA'lar da daha fazla işleme imkân tanımasından dolayı daha kabiliyetlidir. Özellikle işaret işleme uygulamalarında kullanılan FPGA'larda, yonga üzerinde bulunan RAM bloklarının boyutları büyük öneme sahip olmaktadır.

Şimdiye kadar mikroişlemcilerle gerçeklenen pek çok uygulamanın bugün FPGA'larla gerçekleniyor olması elbette ki yalnızca yonga üzerinde bulunan birkaç megabayt blok RAM'dan dolayı değildir. FPGA'lar üzerinde gerçeklenen tasarımlar, mikroişlemcilerin aksine tamamen bir devreye karşılık gelmektedir. Bu durumda bir devrenin bir işlemi gerçekleme süresi, tasarıma bağlı olmakla birlikte sadece kapı gecikmeleri kadar uzun sürecektir. Hâlbuki mikroişlemcili sistemlerde bir tek komutun gerçeklenmesi, işlemcinin mimarisine bağlı olarak çok sayıda saat periyodu sürmektedir. Kısacası mikroişlemcilerde işler adım adım, sayısal işaret işlemcilerde (DSP) bir adımda üç, dört işlem şeklinde gerçeklenirken, FPGA'larda işlemler blok blok gerçeklenmektedir. Bu avantajından dolayı FPGA tabanlı gerçeklemeler özellikle gerçek zamanlı uygulamalarda yani gecikmeye tahammülün olmadığı, zamanlamanın çok önemli olduğu noktalarda mikroişlemcili bir sistem gerçeklemesine tercih edilmektedir.

FPGA'ların tercih edilmesinde tek unsur hız değildir. Bilindiği gibi mikroişlemci tabanlı sitemlerde, sistem üzerinde koşan işlem yazılımla gerçeklenir ve mikroişlemci tarafından adım adım gerçekleştirilir. Dolayısıyla sistemin program belleğine erişildiği anda sistem üzerinde koşan fonksiyonun ne olduğu da kolaylıkla anlaşılabilir. Bu durum mikroişlemcileri, kriptosistemler gibi güvenliğin büyük öneme sahip olduğu sistemlerin gerçeklemesinde devre dışı bırakmaktadır.

FPGA'lar ise gerçekledikleri sistemlere, üretimlerinde kullanılan teknolojiye bağlı olarak ama kesinlikle mikroişlemciler kadar düşük olmayacak seviyede yüksek güvenlik sağlarlar. Pek çok FPGA da aynı mikroişlemci gibi güç kesildiğinde üzerindeki bilgiyi kaybeder, dolayısıyla bir program belleğine ihtiyaç duyar ancak program belleğinden FPGA'ya yüklenen, mikroişlemcideki gibi komutlara karşılık düşen makine kodları değil, devre bağlantılarını belirten programlama dosyasıdır. Dolayısıyla istisnai durumlar bir kenara bırakılacak olursa bu dosyadan devrenin nasıl çalıştığı bilgisine erişmek pek mümkün değildir.

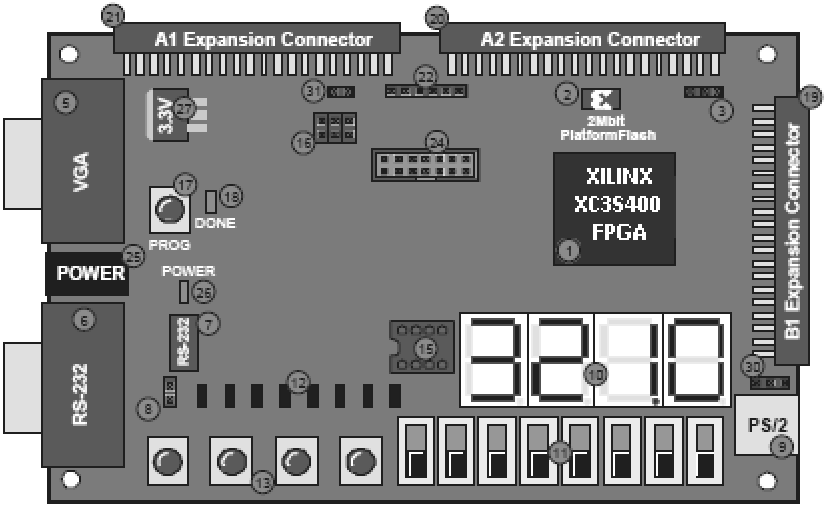
Ayrıca çok daha yüksek güvenlik vadeden bazı FPGA'larda bu dosyanın aktarımı da ortadan kaldırılmış, yonga, harici bir program belleğinden beslenmek yerine tamamen farklı bir mimari ile tasarlanarak SRAM tabanlı değil Flash bellek tabanlı üretilmiştir. Bu sayede yonga elektrik kesilse dahi üzerindeki bilgiyi korumaktadır ve dışarıdan tekrar tekrar programlanma gereği duymamaktadır.

FPGA teknolojisi günümüzde hala çok büyük miktarlarda üretimler söz konusu olduğunda ASIC teknolojisinden daha maliyetli bir çözümdür. Ayrıca ASIC çözümler FPGA'dan daha hızlıdır. Ancak FPGA tasarımları, pazara ulaşma süresinin çok kısa olması nedeniyle çok büyük miktarlarda üretimin söz konusu olmadığı durumlarda ASIC çözümlere tercih edilmektedir.

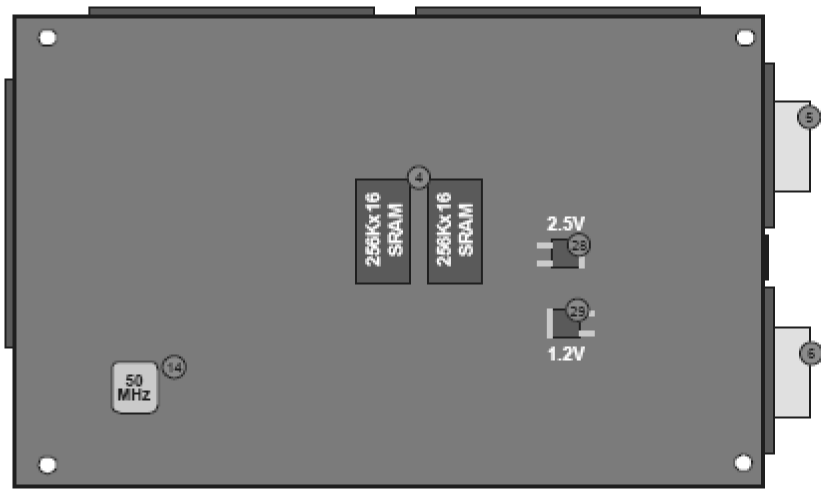
FPGA tasarımları bugün ASIC tasarımın ilk adımı olarak görülmektedir ve model üretimler ilk olarak FPGA'da gerçeklenmekte, sistemin olası hata ve eksiklikleri tespit edildikten sonra ASIC tasarım ve üretime geçilmektedir. Bunun nedeni ASIC üretimin ilk maliyetinin çok yüksek olmasıdır. Hâlbuki bu maliyet FPGA'da yaklaşık olarak hiç yoktur ve sonuca ulaşma süresi de yok denecek kadar kısadır. Bu nedenlerden ötürü FPGA üretimi sürekli artmakta, teknolojisi gelişmekte ve fiyatları da her geçen gün düşmektedir.

2.2 Xilinx XC3S400 FPGA ve Geliştirme Kiti

Proje kapsamında, ‘Güvenli Fotoğraf Makinesi’ Xilinx firmasının Spartan ailesinden XC3S400 FPGA’sı üzerinde gerçeklenmiştir. Bu FPGA, içerisinde 400.000 mantıksal kapı ve ayrıca toplam 344Kbit RAM bulundurmaktadır. Xilinx firmasının giriş seviyesi FPGA’larından bir tanesidir ve yine aynı firmaya ait geliştirme kiti üzerinde bulunmaktadır. Geliştirme kiti üzerinde FPGA’dan başka, giriş seviyesinde uygulamalar geliştirmek üzere, toplam 1MBaytlık SRAM, ledler, butonlar, anahtarlar, yedi parçalı led takımı, RS232 ve VGA portları ve 50MHz dâhili kristal bulunmaktadır. Kitin şeması Şekil 2.1’de görülmektedir.



Xilinx Spartan-3 Geliştirme Kiti Üstten Görünüm



Xilinx Spartan-3 Geliştirme Kiti Alttan Görünüm

Şekil 2.1: Xilinx Spartan-3 Geliştirme Kiti

2.3 Donanım Tanımlama Dilleri ve VHDL

VLSI teknolojisindeki gelişim ile çok büyük ölçekli sayısal sistemlerin tek bir yonga üzerinde gerçeklenmesi mümkün olmuştur. Aynı, insanların birbirlerine bir şeyleri ifade etmek için bir dile ihtiyaç duyması gibi bu sistemlerin bileşenlerini tanımlamak ve uyum içinde beraberce kullanılmalarını sağlamak üzere de bir dile ihtiyaç duyulmuştur. [2]

Bu amaçla donanım tanımlama dilleri oluşturulmuştur. Bu diller ile devrenin nasıl çalışması gerektiği tutucu seviyesinde ifade edilmektedir. Dilin kullanımında dikkat edilmesi gereken noktalar diğer dillerde olduğu gibi kullanıldıkça öğrenilmekte, keşfedilmektedir. Sayısal tasarımın ilkeleri doğrultusunda gerekli olan devre elemanları ve bunların birbirleri ile uyum içinde çalışması donanım tanımlama dilinin etkin kullanımına bağlıdır.

Donanım tanımlama dilleri birden fazladır ve temelde aynı işi görseler de yazım kuralları açısından birbirlerinden ayrılmaktadır. Başlıca donanım tanımlama dilleri VHDL, Verilog ve ABEL'dir. Projede sistem tasarımı VHDL ile yapılmıştır. Ancak tecrübeler VHDL ve Verilog kodlarının bir arada uyum içinde çalıştığını göstermektedir. Sonuçta birer devreye karşılık gelen kodların hangi dille yazılırsa yazılsın bir arada uyum içinde çalışması beklenen ve olması gereken bir özelliktir.

VHDL dilinin açılımı da 'çok yüksek hızlı tümdevre donanım tanımlama dili' olarak geçer ve ilk olarak Amerikan ordusunda bir standart olarak ortaya konmuştur. Teknolojinin lokomotifi olan pek çok alanda olduğu gibi bu alanda da askeri sistemler, gelişimin öncüsü olmuş, henüz çok erken dönemlerinde sayısal elektroniğin ileride geleceği nokta öngörülerek elemanların tanımlanması için ortak bir dil yaratma ihtiyacı duyulmuştur.

2.4 Xilinx ISE

FPGA tasarımları FPGA'nın üreticisi olan firmanın sağladığı bilgisayar destekli tasarım (CAD) araçları sayesinde yapılır. Proje tasarımında da Xilinx ISE aracının 9.1 versiyonu kullanılmıştır. Tasarlanan devrenin davranışsal benzetimleri de yine ISE benzetim ortamında yapılarak devrenin sentezlenmeden önce doğru karakteristiği gösterip göstermediği izlenmiştir.

Yazılım dillerinde kodlar derleyiciye verilerek işlemcinin anlayacağı şekilde makine koduna çevrilirken, donanım tanımlama dillerinde VHDL ile tanımlanan devre sentezleyiciye verilerek FPGA'ya yüklenecek devre konfigürasyonu hazırlanır.

Bir tasarımın FPGA'ya yüklenmeden önce, kullanılacak olan saat frekansında doğru çalışıp çalışmayacağını görmek için sentez sonrası benzetimi de yapılmalıdır. Ancak FPGA teknolojisinin sağladığı esneklikler sayesinde genelde, devrenin çalışabileceği en yüksek saat frekansı sentez raporundan bulunarak gerçeklemede kullanılacak saat frekansından küçük olmadığı teyit edilir, o andan sonra oluşturulan programlama dosyası FPGA üzerinde muhtemelen tanımlandığı karakteristikte çalışacaktır. Bu nedenle genelde çok küçük değişiklikler ardından her defasında benzetim yapmak yerine tanımlanan devreyi sentezletip oluşan konfigürasyon dosyasını hemen FPGA'ya yüklemek sıkça izlenen bir yoldur.

Bu nedenlerle FPGA tasarımında üretici firmanın sağladığı tasarım araçlarının kullanıcı dostu ara yüzlere sahip olması, hızlı ve doğru sonuçlar üretebilmesi, tasarımcıya esneklikler sağlayabilmesi tasarım sürecini ve gerekli iş gücünü önemli ölçüde azaltan ayrıntılardandır.

2.5 Kamera Modülü

Proje kapsamında gerçeklenen sistemin FPGA'da tasarlanan sayısal sistem dışında kalan en önemli parçası kamera modülüdür. Kullanılan kamera modülü 2007 yılında İTÜ Elektrik – Elektronik Fakültesi'nde gerçeklenen bir bitirme çalışması [3] kapsamında üretilmiştir. Kullanılan modüle ait fotoğraf Şekil 2.2'de görülmektedir. Kamera modülü çok kaliteli bir çıkış vermese de gerçeklenen sistemde amaç, çekilen fotoğraf üzerinde yapılacak kriptografik işlem olduğundan, yani fotoğrafın kalitesi çok önemli olmadığından bu durum göz ardı edilmiştir.

Üzerinde Hash fonksiyonu koşturulacak olan fotoğrafı çeken modül, varsayılan ayarlarında kullanılmıştır, bunun nedeni, kamera modülünün I^2C haberleşme hattının istendiği şekilde çalışmıyor olmasıdır. I^2C hattı normalde kamera modülüne, çekilecek olan fotoğrafa dair ışık ayarı, boyut gibi karakteristik özelliklerin belirtilmesini sağlar. Bu hat, işlevsel durumda olmadığından kamera modülü de varsayılan ayarlar altında kullanılmıştır.

Varsayılan ayarlara göre çekilen fotoğraf karesi düşeyde 100 satır, yatayda 120 sütun pikselden oluşmaktadır. Her piksel bilgisi bir bayt ile ifade edilmektedir ve çekilen fotoğraf gri tonlamalıdır. Dolayısıyla bir fotoğraf karesi 12.800 bayttan oluşmaktadır. Piksel bilgileri kamera modülü üzerinde bulunan CMOS görüntü sensoruna ait dokümanlarda belirtilen protokol uyarınca alınmaktadır.

Şekil 2.2: Kullanılan kamera modülünün resmi

Kamera ile 8.33 MHz saat frekansında asenkron haberleşme yapılmıştır. Kamera modülüne dair kullanılan pinler kameraya ait reset, düşey ve yatay senkronizasyon pinleri ve sekiz bitlik görüntü portudur.

Tam bir fotoğraf karesinin başarılı bir şekilde sisteme alınabilmesi için kamera modülünün haberleşme protokolü kuralları, sinyalleşme grafikleri incelenmiş ve bunlara uygun bir sürücü devresi tasarlanıp VHDL ile yazılmıştır. Bu amaçla tasarlanan kamera kontrolör devresi gayet verimli ve modüler yapıda kodlanmıştır. Aynı zamanda, yapılan çok sayıda benzetim ve test sonucunda sorunsuz çalıştığı görülmüştür.

Böyle bir kamera modülü ve tasarlanan modüler yapıdaki kamera kontrolör bloğu, görüntü işleme konusunda yapılacak ileriki çalışmalarda kullanıma oldukça uygundur. Bu açıdan da tasarlanan sistem üzerinde yapılacak olası geliştirmelerin önü açıktır.

3 FOTOĞRAFIN ÇEKİLMESİ ve RAM'e YAZIMASI

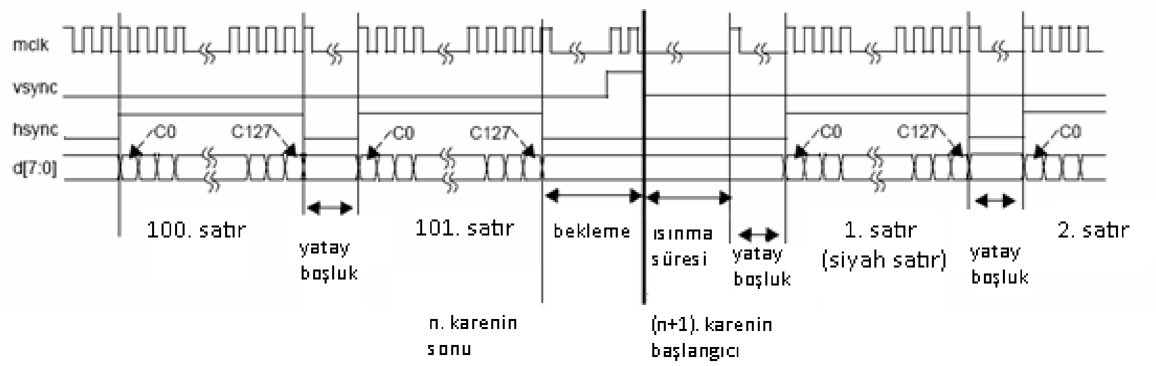
3.1 Fotoğrafın Çekilmesi

FPGA'dan kamera modülüne doğru çıkan VSYNC (düşey senkronizasyon) ve kamera modülünden FPGA'ya giren HSYNC (yatay senkronizasyon) sinyalleri ile fotoğrafın çekimi ve modülden FPGA'ya aktarımı işlemi gerçekleştirilir.

Fotoğraf çekilmesi isteği, kamera modülüne, VSYNC sinyalinin 2 saat periyodu süresince lojik–1 değerinde tutulması ardından tekrar lojik–0 değerine indirilmesi suretiyle iletilir. Burada saat periyodundan kasıt 8.33 MHz'lik saatin periyodudur. 50 MHz'lik sistem saatinden bu frekansta bir saat oluşturmak için bir frekans bölücü gerçeklenmiştir. Bu sinyali alan kamera modülü o anda fotoğrafı çekerek modül içerisinde bulunan 128x100'lük bir diziye yazacaktır. İlerleyen saat periyotlarında da protokolüne uygun şekilde piksel değerlerini görüntü portu yoluyla dışarı, yani FPGA'daki sisteme aktaracaktır.

Kamera modülü piksel bilgilerini satır satır göndermektedir. Ancak fotoğrafı çektikten sonra gönderdiği ilk satır tamamen siyah piksellerden oluşan bir satırdır. Kameradan gönderilen piksel bilgilerini FPGA üzerindeki sistem HSYNC (yatay senkronizasyon) sinyalini takip ederek içeri almaktadır.

HSYNC sinyali pikseller bayt bayt gönderildiği süre boyunca lojik–1 değerinde durmaktadır. 128 piksel yani 128 bayttan oluşan bir satırın aktarımı tamamlandığında HSYNC sinyali lojik–0 değerine inmekte, diğer satırın aktarımına başlanana kadar da öyle kalmaktadır. Bir satırı oluşturan 128 baytlık piksel bilgisi 8.33 MHz'lik saatin her çıkan kenarında görüntü portuna bir bayt konulmak üzere aktarılır. Dolayısıyla en baştaki siyah satır dahil olmak üzere toplamda 101 satır 128 sütunluk bir piksel dizisi görüntü portundan HSYNC ve saat işareti gözetilerek alınmış olunur. Bu haberleşme protokolü Şekil 3.1'de görülmektedir.



Şekil 3.1: Kamera modülünün sinyalleşme protokolü

3.2 RAM Kullanımı

Çekilen ve kamera modülünden alımı tamamlanan fotoğraf eş zamanlı olarak RAM’e yazılmaktadır. Bu işlem daha sonra fotoğraf üzerinde gerçeklenecek olan kriptografik ve görüntü işleme algoritmalarının gerçeklenmesini sağlamaktadır.

Xilinx FPGA geliştirme kiti üzerinde iki tane 256K (262.144) uzunluğunda, 16 bit kelime genişliğine sahip yani toplamda 1MB SRAM bulunmaktadır. Şekil 3.2’de bu yongaların yapısı canlandırılmaya çalışılmıştır.

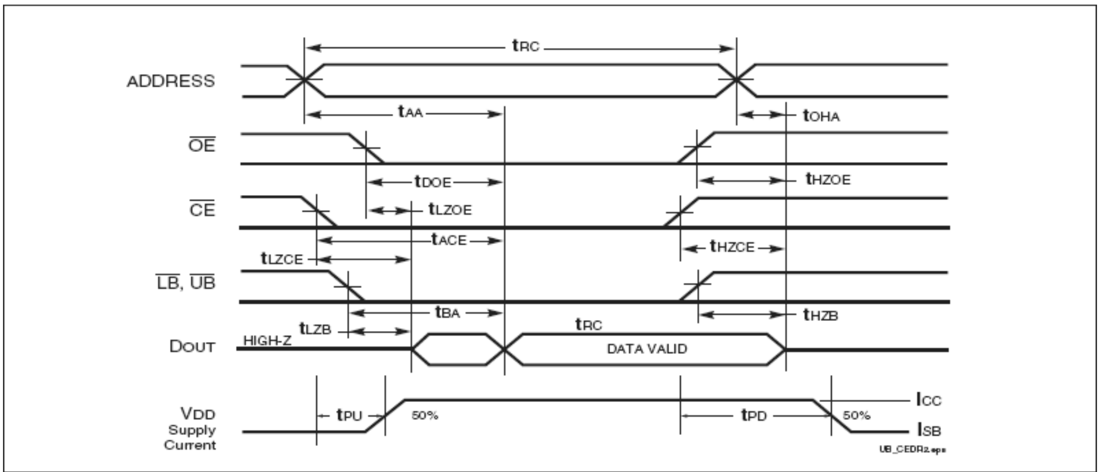
Adres	**1. Yonga, Üst Bayt**	**1. Yonga, Alt Bayt**	**2. Yonga, Üst Bayt**	**2. Yonga, Alt Bayt**
0	AA	1D	23	7E
1	03	41	00	12
2	8B	C3	1D	B0
.	.	.	.	.
.	.	.	.	.
.	.	.	.	.
262.144	15	B2	3E	02

Şekil 3.2: Kit üzerinde bulunan SRAM yongalarının yapısı

ISSI marka SRAM yongaları 12 nanosaniye gecikme ile okuma ve yazma imkânı sağlamaktadır. Sistem saati ise 20 nanosaniye periyoda (50MHz) sahiptir. Bu kıstaslar göz önüne alınarak RAM okuma ve yazma işlemleri için bir kontrolör devresi tasarlanmıştır. RAM ile devre arasında 32 bitlik iki yönlü bir veri yolu gerçeklenmiş, o nedenle iki SRAM yongası da kullanılmıştır. İki SRAM yongası da aynı adres yoluna, fakat farklı veri yollarına sahiptir. Her biri 16 bitlik olan bu veri yolları birleştirildiği vakit ana kontrol bloğu ile RAM kontrolör arasındaki 32 bitlik veri yolu ortaya çıkmaktadır. Ayrıca her bir RAM yongası için ve de bunların alt ve üst baytları için etkinleştirme sinyalleri bulunmaktadır. Ancak bu sinyaller SRAM çifti tam kapasitede kullanıldığı için hep birlikte aktif ve pasifleştirilmektedir.

3.2.1 RAM'den Okuma

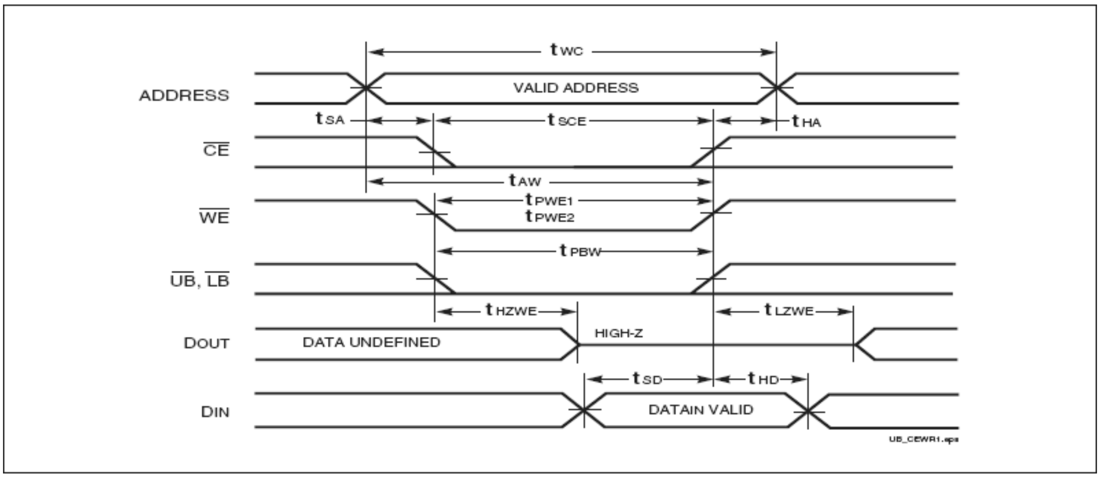
SRAM kontrolörü yongaların gecikme sürelerinin mümkün kıldığı en kısa sürelerde okuma ve yazma yapılabilmesine olanak sağlamak üzere tasarlanmış, her türlü benzetim ve testten başarı ile geçmiştir. RAM kontrolörü sistem ana kontrolöründen gelen oku emri ile birlikte SRAM'e adres bilgisi, oku sinyali, yongaların aktifleştirilmesi sinyalini yollar. Bu andan sonra belirlenen gecikme sonunda iki SRAM yongasının o adres değerine karşılık gelen gözlerindeki toplam dört baytlık veri RAM – FPGA veri yoluna yazılır. SRAM yongalarından veriyi alan RAM kontrolör bunu yine 32 bitlik veri yolu üzerinden ana kontrol bloğuna iletir. SRAM okuma süreci sinyalleşmesi Şekil 3.3'te görülmektedir.



Şekil 3.3: SRAM okuma sinyalleşmesi

3.2.2 RAM'e Yazma

SRAM çiftlerine yazma işlemi sırasında da ana kontrolör bloğundan RAM kontrolöre yaz emri beraberinde adres değeri ve yazılacak olan veri iletilir. Bunları alan RAM kontrolör aynı şekilde SRAM'e adres ve veri bilgisi, yaz sinyali, yongaların aktifleştirilmesi sinyalini yollar. Gerekli sinyalleşme sonunda SRAM yongalarının ilgili adres gözlerine gönderilen dört bayt yazılmış olur. SRAM yazma süreci sinyalleşmesi Şekil 3.4'te görülmektedir.



Şekil 3.4: SRAM yazma sinyalleşmesi

RAM'in yapısının 32bit işleme izin vermesi ve bu potansiyelin en iyi şekilde değerlendirilmesi aritmetik ve kriptografik işlem sürelerini kısaltması açısından önemlidir. Ayrıca tasarlanan RAM kontrolörünü bu geliştirme kitinin kullanılması halinde ileriki dönemde gerçeklemesi yapılabilecek olan görüntü işleme algoritmaları için de önemli bir kütüphane haline getirmektedir.

4 HASH FONKSİYONU

4.1 Kriptografi

Kriptografi; bilginin gizliliği, bütünlüğü ve tarafların kimlik denetimi gibi haberleşmede güvenlik kavramlarını sağlamak için çalışan matematiksel yöntemler bütünüdür. Bu yöntemler, bilginin iletimi esnasında karşılaşılabilecek aktif ya da pasif ataklardan bilgiyi, dolayısıyla da tarafları koruma amacı güder.

Bir bilginin güvenli olarak iletileceğinden ya da gelen bir bilginin güvenli bir şekilde alındığından yani iletim esnasında değiştirilmediğinden bahsedilebilmesi için kullanılan iletişim sistemlerinin sahip olması beklenen bazı temel güvenlik kavramları vardır. [4]

Gizlilik: Bilgiyi, görme yetkisi olanlar dışındaki hiç kimsenin göremeyeceği garantisidir.

Kimlik Denetimi: Alınan bir bilginin göndericisinin gerçekten de mesajda belirtilen taraf olduğunun garantisidir.

Bütünlük: Alınan bilginin iletimi esnasında mesaj üzerinde hiçbir şekilde; ekleme, çıkarma, düzenleme yapılmadığının yani mesajın, gönderim sırasındaki özgün halini koruduğunun garantisidir.

Reddedilemezlik: Alıcı ve gönderici tarafın mesajı aldığının ve gönderdiğinin ispatlanabilmesi garantisidir. Alıcı taraf, mesajı diğer tarafın gönderdiğini ve benzer şekilde gönderici taraf da alıcı tarafın mesajı aldığını ispatlayabilir.

Bu temel kavramlar dışında erişim kontrolü, zaman bilgisi, tanıklık, anonimlik, sahiplik, sertifikalandırma, imzalama gibi kavramlardan da bahsedilebilir.

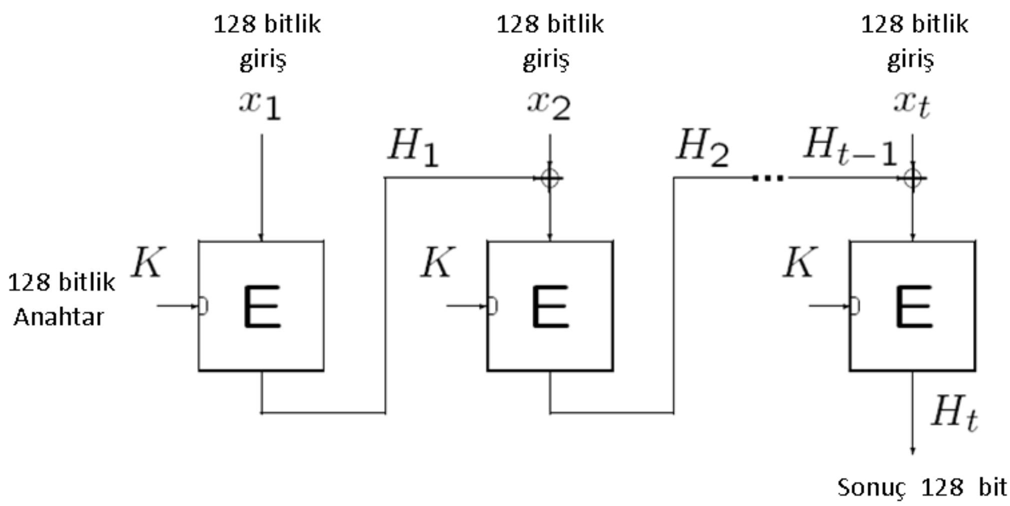
Bir kriptosistem yukarıda belirtilen kavramların bir ya da birkaçını aynı anda sağlamak üzere tasarlanabilir. Projede gerçeklenen 'Güvenli Fotoğraf makinesi' de bilginin bütünlüğü kavramı üzerine geliştirilmiştir. Dolayısıyla tasarlanan sistem bir kriptosistemdir ve sayısal fotoğraf makinesi ile çekilip çoğaltılan fotoğrafların hala orijinal olup olmadığının yani ilk çekildiği andaki halini koruyup korumadığının garantisini verebilmektedir.

4.2 Hash Fonksiyonları

Bilginin bütünlüğünü sağlamak için kullanılan yöntem Hash fonksiyonlarıdır. Hash fonksiyonları ya da diğer bir ismiyle öz fonksiyonları tek yönlü matematiksel ifadelerdir. Yani fonksiyonun çıkış değerinden giriş değerini bulmak mümkün değilken giriş değeri her zaman aynı çıkış değerine karşılık gelir.

Bir anlam bütünlüğü içermeyen ve rastgele sayılar dizisi görüntüsü veren Hash fonksiyonu çıktıları, girişteki mesaja özgüdür ve bu işlem tekrarlandığında hep aynı sonucu verir. Ancak mesajda yapılacak bir bitlik dahi değişiklik çıkışın tamamen başkalaşmasına neden olur. Böylece alıcı ve gönderici tarafın aynı Hash fonksiyonunu mesaj üzerinde koşturması sonucunda çıkış değerlerinin uyuşması mesajın bütünlüğünü garanti ederken, oluşan farklılık mesajın iletim esnasında değiştirildiğine işaret etmektedir.

Proje kapsamında tasarlanan kriptosistem anahtarlı bir Hash fonksiyonunu içermektedir. Dolayısıyla fotoğrafın bütünlüğünü teyit etme yetkisi de sadece anahtara sahip taraflarda olacaktır.



Şekil 4.1: Tasarlanan AES tabanlı Hash fonksiyonunun şeması

Şekil 4.1'de proje kapsamında tasarlanan Hash fonksiyonunun şeması görülmektedir. Şekilde görülen E kutuları şifreleme bloklarını temsil eder. K ise fotoğraf makinesinde ve fotoğrafın bütünlüğünü teyit edecek olan tarafta bulunan anahtardır ve bu sistem için 128 bitten oluşmaktadır.

Tasarlanan sistem anahtar paylaşımı problemine değinmemektedir ve sistemin her iki tarafının da simetrik anahtarı güvenli bir şekilde önceden paylaştığı varsayılmaktadır.

Şekilde görülen ve bir şifreleme algoritmasına dayanan Hash fonksiyonunun güvenilirliği, şifreleme bloğunun güvenilirliği ile doğru orantılıdır. Tasarlanan sistemde bu amaçla kullanılan şifreleme bloğu AES'tir. AES, gelişmiş şifreleme standardı, Rijndael olarak da bilinen ve ABD hükümeti tarafından beş yıllık bir sürecin ardından 2001 senesinde standartlaşmış blok şifreleme standardıdır. [5]

Günümüz itibariyle dünya çapında kabul görmüş ve en yaygın biçimde kullanılan şifreleme algoritması olan AES; daha az bellek gerektirmesi, daha hızlı olması ve daha kolay gerçeklenebilmesi yanında önceki blok şifreleme tekniklerine göre daha üst düzeyde bir güvenliği garanti etmektedir.

10 turdan oluşan bir SPN (yerine koyma – yer değiştirme ağı) olan AES, farklı boyutlarda bloklarla çalışma imkânı tanımaktadır. Artan blok boyutu daha üst düzey bir güvenlik getirirken daha fazla miktarda sistem kaynağı gerektirmektedir. Projede kullanılan AES bloğu 128 bitliktir, yani algoritma içerisinde aynı anda 128 bitlik bir veri bloğu dolaşmaktadır.

Mesajın şifreleme bloğuna şekilde görüldüğü gibi girmesi literatürde AES – CBC çalışma modu olarak geçmektedir. Yani şifreleme fonksiyonunun zincirleme bir şekilde giriş mesajına uygulanmasıdır. Yalnız buradan bir Hash fonksiyonu üretmek gerektiğinde sadece en son şifreleme bloğunun çıkışı kullanılacaktır. Bu nedenle önceki blokların çıkışları bir sonraki giriş ile 'ayrıcalıklı veya' (xor) işlemine tabii tutulmuştur.

Tasarlanan sistemde Hash fonksiyonunun çıkışı, giriş mesajının uzunluğundan bağımsız olacak şekilde 128 bittir. Çünkü yukarıda bahsedildiği şekilde, her şifreleme bloğu bir sonrakinin girişini etkiler ve sistemin çıkışı da sadece en son bloğun çıkışıdır. Kullanılan AES bloğunda da blok boyutu 128 bit olduğundan en son çıkış da 128 bit uzunluğunda olacaktır.

4.2.1 Anahtarlı Hash Fonksiyonları

Hash fonksiyonları anahtarsız sistemler olabileceği gibi bu tasarımda kullanıldığı gibi anahtarlı sistemler de olabilir. [6] Bu tür Hash fonksiyonlarına Hash – MAC (mesaj kimlik doğrulama kodu) denir. Yani bilginin bütünlüğünü doğrulama işlemini herkes değil sadece anahtara sahip kişiler yapabilir. Bu şekilde bir sistem tasarımı yapılması, aşağıdaki gibi bir senaryonun gerçekleşmesi durumunda, sistemin düşeceği muhtemel aldanmanın önüne geçilmesini amaçlamaktadır:

Örneğin; fotoğraf çekildikten sonra anahtarsız bir Hash fonksiyonundan geçirilsin ve çıkışı yine fotoğraf içerisine kaydedilsin. Bu durumda fotoğrafta bir değişiklik yapıldığında sistem fotoğrafın bütünlüğünün korunmadığını ortaya çıkartabilir. Ancak sistemi kandırmak isteyen kişiler, fotoğrafta bir değişiklik yaptıktan sonra oluşan yeni halinin Hash fonksiyonu çıktısını üretip yeniden fotoğrafın içine gömebilir, bu mümkündür çünkü aynı Hash fonksiyonunu koşturmak için herhangi bir anahtar gerekmemektedir. Bu durumda yeni oluşan fotoğraf aslında makinede üretilenden farklı olsa da sistem bunu fark edemeyecektir.

Böyle bir aldanmanın önüne geçilmesi amacıyla sistem anahtarlı Hash fonksiyonu ile gerçeklenmiştir. Ancak bu defa da simetrik anahtarın paylaşımı problemi ortaya çıkmaktadır. Ancak anahtar paylaşımı konusunda kabul görmüş protokollerinden bir tanesi kullanılarak bu problem çözülebilir.

Daha önce de bahsedildiği gibi Hash fonksiyonlarının girişine verilebilecek mesaj uzunluğunda bir sınır söz konusu değildir. Bu çalışmada da fotoğraf çekildikten ve RAM'e yazıldıktan sonra fotoğrafa ait piksel bilgileri toplam 12.800 baytlık bir yer kaplamaktadır. Bu 12.800 bayt 128 bitlik (16 bayt) parçalar halinde Hash modülüne giriş yapar. 800 iterasyon (12.800 / 16) sonunda Hash alma işlemi tamamlanır ve Hash fonksiyonu çıktısı, diğer bir adıyla '*iz sözcüğü*' oluşturulmuş olur.

Hash fonksiyonları; bilginin bütünlüğünden duyulan endişenin artmasıyla, günümüzde önemli bir çalışma konusu haline gelmiş, blok şifreleme yöntemleri konusunda yapılan çalışmalar sonucu ortaya çıkan AES standardının oluşturulması gibi Hash fonksiyonları konusunda da bir standart belirleme arayışına girilmiştir. Önümüzdeki dönemde bu konuda somut adımlar atılması ve dünya genelinde kabul görecek bir algoritmanın matematikçiler ve mühendisler tarafından oluşturulması beklenmektedir.

5 GÜVENLİ FOTOĞRAFIN OLUŞTURULMASI

5.1 Bitmap Fotoğraf Formatı

Kamera modülünde herhangi bir sıkıştırma veya görüntü işleme algoritması koşmadığından modülden doğrudan, ham piksel bilgisi gelmektedir. Ham piksel bilgileri doğrudan bilgisayarlardaki işletim sistemlerinde görünür bir formata sahip değildir. Bu ham piksel bilgilerini herhangi bir işleme tabii tutmadan olduğu gibi görünür kılmak için Bitmap formatına uyumlu hale getirmek uygun görülmüştür.

Bitmap formatı dört kısımdan oluşmaktadır: Bitmap başlık bölümü, Bitmap bilgi bölümü, renk paleti ve ham piksel verisi. Bitmap başlık bölümünde; Bitmap tipi fotoğrafa özgü iki bayt, fotoğrafın toplam boyutunu belirten kısım ve ham piksel bilgisinin hangi bayttan itibaren başladığını belirten bir adres kısmı bulunmaktadır.

Bitmap bilgi bölümünde bu bölümün hangi standarda ait olduğu ve boyutu, resmin piksel cinsinden en ve boyu, renk paletinde bulunan renk sayısı gibi bilgiler bulunur. Renk paleti ise piksel bilgilerinin yorumlanması açısından bir referans niteliğindedir. Piksel bilgisinin 0 – 255 aralığında alacağı değere karşılık kırmızı, yeşil ve mavi renk uzayında bu bileşenlerin alması gereken renk değerlerini belirtir.

5.2 Hash Çıktısının Fotoğrafa Gömülmesi

Gerçeklenen sistem gereği, fotoğraf üzerinde koşturulan Hash fonksiyonu çıktısının, fotoğraf üzerinde bir yere yazılması gerekmektedir. Bu yerin neresi olacağı önemli bir konudur ve yazılacak veri fotoğraf üzerinde bir bozulmaya ya da görüntü kalitesinin düşmesine neden olmamalı, fotoğraf üzerinde görünür bir iz bırakmamalıdır. Bu problem için çözüm yolu aranırken projeyi özgün yapan fikir ortaya atılmıştır; Bitmap formatına formatın özelliklerinden yola çıkarak yeni bir açılım getirmek. Buna göre dört kısımdan oluşan Bitmap formatı beş kısım olarak değiştirilecektir. Ancak bu, Bitmap standardında herhangi bir değişikliğe yol açmayacak, üretilen yeni Bitmap dosyası yine her bilgisayarda görüntülenebilecektir.

Oluşturulacak olan yeni bölüm renk paleti ile ham piksel bilgisi bölümleri arasında yer alacaktır yani Hash kısmı başlık bölümünün en altında yer alacaktır. Yeni bölümden dolayı fotoğraf boyutu bir miktar artacaktır. Ayrıca ham piksel bilgisinin başlangıç adresi de aynı oranda aşağıya kayacaktır. İşte bu yeni bölümün oluşturulması birinci Bitmap başlık bölümünde, fotoğrafın oluşan yeni toplam boyutu ve ham piksel bilgisinin başlayacağı yeni adres değerini düzenleyerek mümkün olmaktadır. Bu fikir ilk olarak bilgisayar üzerinde bir fotoğrafta yukarıda belirtildiği şekilde denenmiş ve olumlu sonuç alınmıştır, bu andan sonra da sistem bu fikir üzerine oturtulmuştur.

Tablo 5.1'de Bitmap formatındaki bir fotoğrafa ait kısımlar görülmektedir. Bu tabloda belirtilen içerikler tasarlanan sistemin çıktısı olan herhangi bir fotoğrafın ham piksel bilgisi dışında kalan başlık kısımlarının içeriklerini göstermektedir. Hash bilgisinin gömüldüğü alan 18 bayttan oluşmaktadır ancak bu alanın sadece 16 baytı kullanılmaktadır. Bunun nedeni sistemin gerçekleme aşamasında veri yollarının verimlilik esasıyla 4 bayt şeklinde tasarlanmasıdır. Bu nedenle Hash alanının boyutu da bu amaç doğrultusunda genişletilmiştir.

Sonuç olarak ham piksel bilgisi dışında kalan başlık bölümlerinin son boyutu 1096 bayt, piksel bilgisinin boyutu ise 12.800 bayt olarak gerçekleşmektedir. Fotoğrafta, eklenen Hash bölümünden ötürü görünen herhangi bir bozulma, değişme olmamaktadır, fotoğrafın boyutu sadece 18 bayt artmaktadır ve son fotoğraf standartlara uygundur.

İlerleyen dönemde bu sisteme bir de görüntü iyileştirme algoritmasının gerçeklemesi eklenecek olursa bu durumda fotoğrafın boyutunun artması beklenmemektedir, dolayısıyla başlık kısmı tamamen aynı kalacaktır. Ancak piksel bilgileri değişeceğinden elbette Hash fonksiyonu sonucu da değişecektir. Dolayısıyla böyle bir iyileştirme fonksiyonunun koşturulması durumunda bu işlem Hash fonksiyonunun öncesinde yapılmalı, Hash fonksiyonu en son koşturulmalı ve sonuçta oluşan *iz sözcüğü* de başlık kısmında bulunan Hash alanına gömülmelidir. Hash fonksiyonunun koşturulması *Güvenli Fotoğraf* oluşturma işleminin son adımı olduğundan bu noktadan sonra fotoğraf üzerinde hiçbir işlem yapılmamalıdır.

Tablo 5.1: Bitmap formatının bileşenleri ve yeni oluşturulan bölümün içeriği

Adres Aralığı	**Boyut(Bayt)**	**Bölüm Adı**	**İşlevi**	**Değeri**
0 - 1	2	Başlık	Bitmap'e özgü değerler, sihirli sözcük olarak da geçer. B ve M harflerinin ASCII karşılığı	42 4D
2 – 5	4		Toplam fotoğraf boyutu (13904 bayt)	48 36 00 00
6 – 7	2		Standart, görüntüyü oluşturana bağlı	00 00
8 – 9	2		Standart, görüntüyü oluşturana bağlı	00 00
10 – 13	4		Ham piksellerin başlangıç adresi (1104. bayt)	48 04 00 00
14 – 17	4	Bilgi	Bu bölümün bayt cinsinden boyutu (40 bayt)	28 00 00 00
18 – 21	4		Fotoğrafın piksel cinsinden eni (128)	80 00 00 00
22 – 25	4		Fotoğrafın piksel cinsinden boyu (100)	64 00 00 00
26 – 27	2		Kullanılan renk uzayı sayısı	01 00
28 – 29	2		Renk derinliği (8 bit)	08 00
30 – 33	4		Sıkıştırma metodu (RGB)	00 00 00 00
34 – 37	4		Ham piksel boyutu (12800)	00 32 00 00
38 – 41	4		Yatay çözünürlük	00 00 00 00
42 – 45	4		Düşey çözünürlük	00 00 00 00
46 – 49	4		Renk paletindeki renk sayısı (256)	00 01 00 00
50 – 53	4		Önemli renklerin sayısı (hepsi eş değerli)	00 00 00 00
54 – 57	4	Renk Paleti	R0 G0 B0 0	00 00 00 00
58 – 61	4		R1 G1 B1 0	01 01 01 00
62 – 65	4		R2 G2 B2 0	02 02 02 00
66 – 69	4		R3 G3 B3 0	03 03 03 00
70 – 73	4		R4 G4 B4 0	04 04 04 00
.	.	.	.	.
.	.	.	.	.
.	.	.	.	.
1074 – 1077	4		R255 G255 B255 0	FF FF FF 0
1078 – 1095	18	Hash Alanı	Bu alanın 16 baytı Hash sonucuna ayrılmıştır, geriye kalan alan 0'dır.	00 00 Hash(16 bayt)
1096 - 13895	12800	Piksel Alanı	Bu bölümde ham piksel bilgisi yer almaktadır. 128 x 100	
TOPLAM	13896		1096 bayt başlık kısımları, 12800 bayt piksel bilgisi	

5.3 Bitmap Formatının Gerçeklenmesi

Gerçeklenen sistemde çekilen her fotoğrafın fotoğraf boyutu, vs. aynı olacağından başlık kısmı Hash kısmı dışında birebir aynı olacaktır. Dolayısıyla fotoğrafların sahip olması gereken başlık kısımlarının içeriklerini belirlemek (Tablo 1'deki içerik kısımları) ve sonrasında bunları bir ROM'a yazmak gerçekleme açısından uygun görülmüştür.

Toplamda 1096 bayt olan başlık kısmı 274 x 4 baytlık bir ROM kullanılarak gerçeklenmiştir. Kelime uzunluğunun 4 bayt olarak seçilmesi sistem veri yollarının RAM ve kamera blokları için de 32 bit olarak tasarlandığından bu modüllerle uyumluluğu sağlayabilmek içindir.

Sistem ana kontrol bloğunun sonlu durum makinesinin birinci durumunda yani sistem ilk çalıştırıldığında veya reset uygulandığında, RAM'in ilk 13.896 baytına karşılık gelen 3474 adres sıfırlanır ki bu alan işlem süresince kullanılacak olan tüm RAM alanıdır. Bitmap formatı için başlık kısmı ilk 1.096 bayta karşılık gelen 274 adrese ROM'dan sırayla okunup RAM'e yazılmaktadır.

Burada kullanılan ROM FPGA üzerindeki mantıksal kapılardan yaratılmıştır, harici bir eleman değildir.

6 FOTOĞRAF MAKİNESİ ARAYÜZÜ

6.1 Kullanıcı Arayüzleri

Gerçeklenen sistem bir kullanıcı elektroniği ürünü olduğundan dışarıdan kontrol için bir çeşit arayüze ihtiyaç duymaktadır. O nedenle fotoğraf makinesinin süreci kontrol için harici butonları ve mevcut durumları izleyebilmek için de yedi parçalı ledleri bulunmaktadır. Bu çevre birimleri gerçeklemede kullanılan Xilinx Spartan -3 uygulama geliştirme kiti üzerinde hâlihazırda bulunmaktadır. Ancak bu çevre birimlerini kullanırken dikkat edilmesi gereken çeşitli hususlar vardır.

Butonlar mekanik elemanlardır ve mekanik elemanların hassasiyetleri elektronik elemanlar kadar yüksek değildir. Bu nedenle kullanıcı butona bir kere bastığını zannederken aslında sık aralıklarla çok defa butonun çıkışında lojik–1 değeri oluşmaktadır. Bu etkiye '*debounce etkisi*' denir. Bu etki açıktır ki devrenin istendiği şekilde çalışmasına imkan vermez, çünkü durum makinesinde bir durum atlama isteğine karşılık gelen butona basma işlemi sonunda çok sayıda istek geldiğinden durum makinesinde istenmeyen durumlara sapma yaşanabilir.

Bu etkiyi ortadan kaldırmak ve butona basıldığında sadece bir saat periyodu boyunca çıkışa lojik–1 vermek sonra çıkışı tekrar lojik–0 değerine çekmek için bir tasarım yapılmış ve VHDL ile kodlanmıştır. Tasarıma göre butona basıldığında oluşan ilk lojik–1 değeri ile butonun çıkışı pasifleştirilir ve 400 milisaniye süresince butonun çıkışının devrenin girişini etkilemesi önlenir. Bu sayede zararlı ardıl çıkışların oluşturacağı istenmeyen durumların önüne geçilmiş olur.

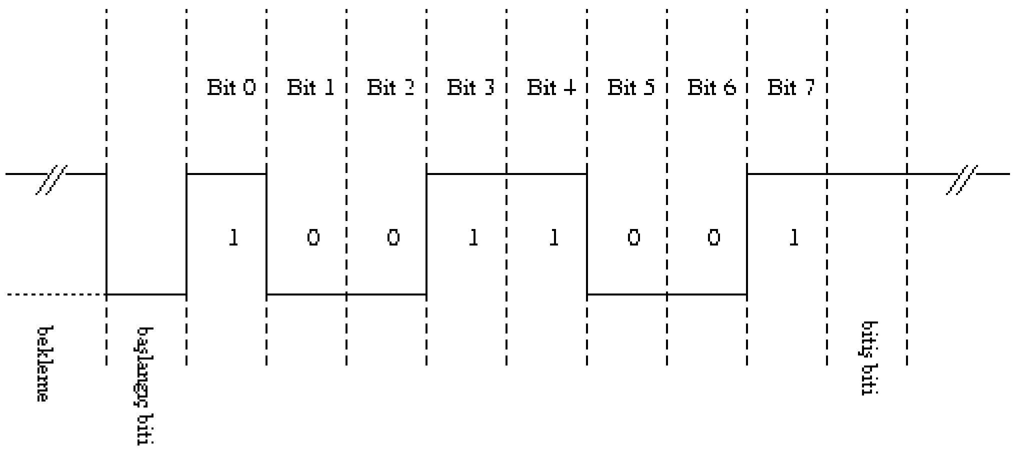
Yedi parçalı ledlerin kullanımı için de bir sürücü tasarlamak gerekmektedir. Kit üzerinde dört adet yedi parçalı led bulunmaktadır ve bunların adres ve veri hatları ortaktır. Yani girilen adres değerine göre karşılık düşen led takımı veri hattından gelen karakteri göstermektedir. Dört led takımının hepsi kullanılmak istendiğinden insan gözünün fark edemeyeceği hızda bu takımları taramak gerekmektedir. İşte bu işlemi gerçekleştiren ve dört led takımının da kullanılmasını sağlayan sürücü devresi tasarlanmış ve VHDL ile kodlanmıştır.

6.2 FPGA – Bilgisayar Arayüzü

Üretilen '*güvenli fotoğraf*' RS232 seri haberleşme protokolü ile FPGA kitinden bilgisayara aktarılmakta, bilgisayarda da gelen fotoğraf Matlab ortamında alınıp Bitmap dosyası şeklinde kaydedilmektedir. Gelen fotoğrafı Matlab ile karşılamak tamamen bir tercihtir ve herhangi bir zorunluluk içermemektedir. Nitekim Matlab'ın bu aşamada gelen veriyi toplayıp ".bmp" olarak dosyaya yazmaktan başka bir işlevi yoktur.

İletim saniyede 19.200 bit hızında gerçekleşmektedir. İletim hızının çok düşük tutulması gerçeklenen sistemin bir kriptosistem olmasından ve iletim esnasında oluşacak bir bitlik dahi bir hatanın yanlış sonuçlara yol açacak olmasıdır.

RS232 protokolünde iletim hattı normalde lojik–1 seviyesinde tutulur. Yollanan veri, başına başlangıç, sonuna da bitiş biti eklenerek 8+2=10 bit şeklinde yollanır. İsteğe bağlı olarak iletim sırasında oluşabilecek hatalara karşı bir de parite biti eklenebilir. Ancak gerçeklenen sistemde parite biti kullanılmamıştır. Şekil 6.1'de RS232 iletim hattında bir bayt verinin iletimi boyunca meydana gelen değişim görülmektedir. Bu örnekte "10011001" baytı hattan iletilmektedir.



Şekil 6.1: RS232 protokolü uyarınca bir baytın iletimi

Bilgisayar tarafında Matlab kodu seri portu dinler moda alındıktan sonra fotoğrafı kitten bilgisayara gönderme emri kullanıcı tarafından dışarıdan bir buton aracılığıyla verilir.

7 BİLGİSAYARDA FOTOĞRAFIN BÜTÜNLÜĞÜNÜN TEST EDİLMESİ

Oluşturulan '*güvenli fotoğrafın*' hedeflenen amaca hizmet edip etmediği Matlab ve Xilinx benzetim ortamları yardımıyla test edilmiştir.

Güvenli fotoğraf içerisinde bulunan Hash alanı ve buradaki Hash bilgisi, fotoğrafta MS Paint gibi giriş düzeyi bir programla oynama yapılmak istendiğinde yok olmaktadır. Dolayısıyla Hash alanının ve beraberinde Hash bilgisinin de yok olması fotoğrafı doğrudan güvenli olma sıfatından yoksun bırakmaktadır.

Ancak daha gelişmiş araçlarla fotoğraf üzerinde bu alan yok edilmeden bir değişiklik yapılmak istendiğinde sadece piksel bilgisi değişecek, diğer bölümler olduğu gibi kalacaktır.

Doğrulama işlemi için güvenli fotoğrafta Hash bilgisinin yazılı olduğu alan Matlab sayesinde okunmakta, daha sonra fotoğrafın piksel alanı üzerinde FPGA'daki sistemde bulunan anahtarla aynı anahtara sahip Hash fonksiyonu Xilinx benzetim ortamı sayesinde koşturulmakta ve bu iki sonuç karşılaştırılmaktadır.

İki Hash sonucunun da aynı çıkması durumunda sistem, fotoğrafın bütünlüğünü koruduğunu, aksi durumda ise çekildikten sonra değiştirildiğini belirtmiştir.

FPGA'da 12.800 piksele ait Hash bilgisinin oluşturulması işlemi, 50MHz saat işareti ile çalışan devre için 900 mikro saniye sürerken doğrulama adımında aynı işleme karşılık düşen benzetimin yapılması Intel 1.73GHz işlemcili bir bilgisayarda bir dakikadan uzun sürmektedir. Bu sonuç da gerçeklemede FPGA teknolojisinin tercih edilmesinin doğru olduğunu bir kez daha göstermektedir.

Sistemin çalışmasına dair çeşitli testler yapılmış, herhangi bir sorunla karşılaşılmamıştır. Bu testlerden bir tanesi de Şekil 7.1'de görülmektedir.

GÜVENLİ FOTOĞRAF OLUŞTURMA ADIMI

Orijinal Güvenli Fotoğraf

FPGA'da üretilen ve güvenli fotoğraf içerisine gömülen Hash sonucu:

E8368140E486116694C96661E9CF377F

FOTOĞRAFIN KULLANIMI

Değiştirilmeyen Fotoğraf

Değiştirilen Fotoğraf

(Bir ben eklenmiştir.)

DOĞRULAMA ADIMI

ANALİZ:

1. Fotoğraf Hash Sonucu: E8368140E486116694C96661E9CF377F
2. Fotoğraf Hash Sonucu: 37BFB6A256585728B3E2865ECF42610C

SONUÇ:

2. fotoğrafın çekildikten sonra bütünlüğünü korumadığı tespit edilmiştir.

Şekil 7.1: Sistem Testlerinden Bir Örnek

8 SONUÇLAR

Proje süresince yapılan taramalar sonucunda böyle bir sistemin, bu şekilde ilk kez gerçeklendiği görülmüştür. Bu açıdan bir ilk olan çalışma bundan sonra da benzer pek çok çalışmaya zemin hazırlayacaktır. Bu aşamadan sonra sisteme sayısal imza uygulamasının eklenmesi düşünülebilir. Bu sayede fotoğrafı çeken makine de daha sonra belli olabilecek ve olay anına dair edinilen bilgi düzeyi de arttırılmış olacaktır.

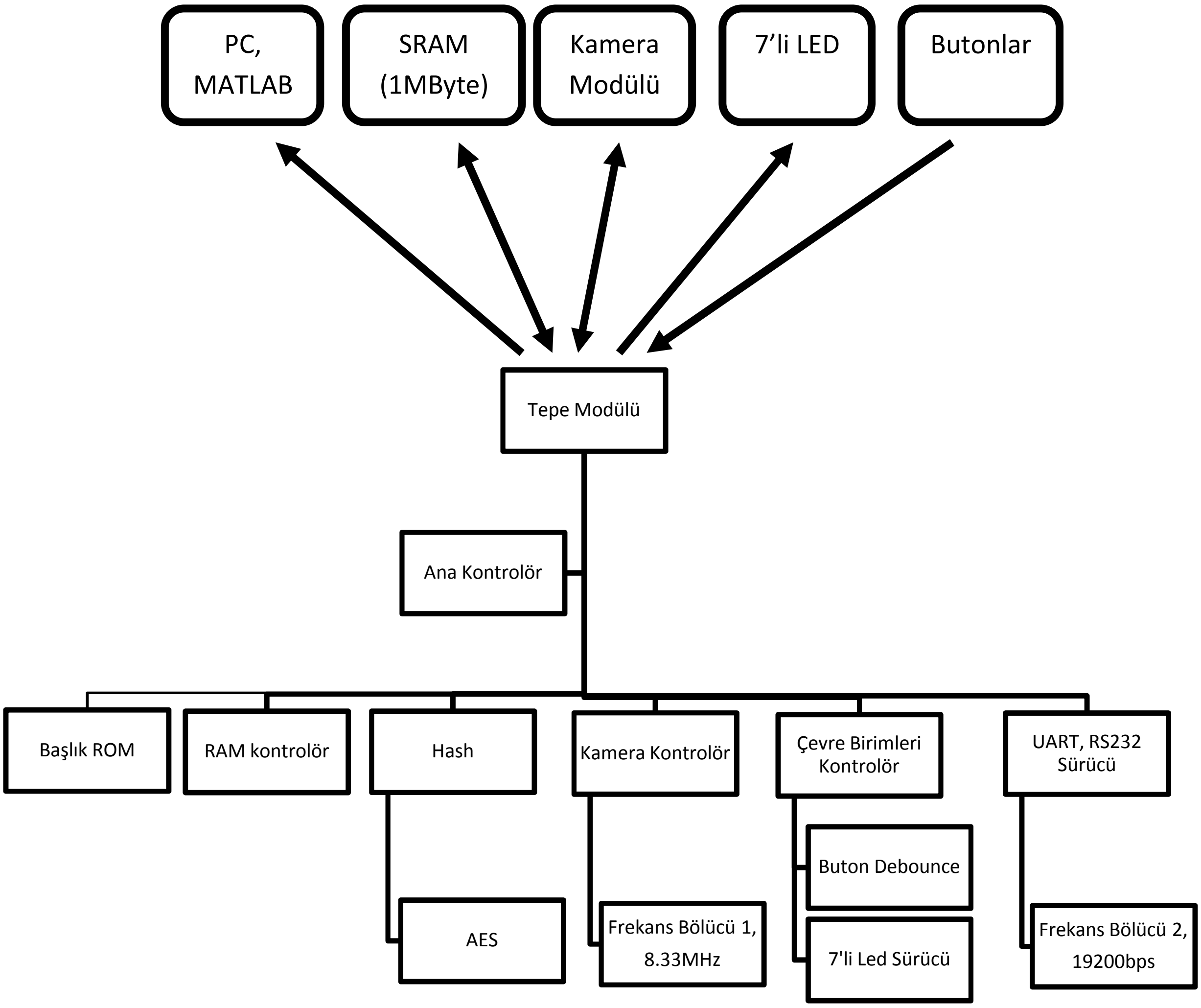
Fotoğraf makinesinin deklanşörüne yerleştirilecek bir parmak izi okuyucu sensor, fotoğrafı çeken kişi hakkında son derece değerli bir bilgi verebilir. Ayrıca fotoğraf makinesine yerleştirilecek bir küresel konum belirleme sistemi (GPS) fotoğrafın çekildiği yani olayın gerçekleştiği yer hakkında ipucu verebilir. Görüldüğü gibi tüm bu önerilerin ortak yanı olay anına dair mümkün olduğunca fazla bilgi edinilmesini sağlamaya yönelik olmalarıdır.

Projede başlangıç düzeyi bir FPGA ile çalışılmış ve kapsamlı bir sayısal sistem tasarımı yapılmıştır. Bu FPGA üzerinde 66 MHz çalışma frekansı limitine ve FPGA'nın %70 doluluk oranına erişilmiştir.

Sistem tasarımı sırasında ana kontrol bloğundaki sonlu durum makinesi omurga görevi görmüş ve tüm esas durumlar burada yer almıştır. Toplamda 6 durum içeren bu makinede durumlar arası geçişler gerektiğinde kullanıcı arabirimi olan butonlar sayesinde gerçekleştirilmiştir.

Ana kontrol bloğunun dışında kalan; kamera kontrolörü, RAM kontrolörü, Hash modülü, RS232 kontrolörü, yedi parçalı led ve butonlar için kontrol blokları hep modüler yapıda tasarlanmış ve kodlanmış bu sayede ileriki çalışmalar için bir kütüphane oluşturulmuştur.

Bu noktadan sonra sistem üzerinde yapılacak olan olası geliştirmelerde geriye dönük ek bir çaba sarf edilmeden doğrudan yeni blok alt modül olarak sisteme eklenecek ve ana kontrol bloğundaki durum makinesine eklenecek yeni bir durum ile devreye alınacaktır. Şekil 8.1'de tasarlanan sistemin genel çerçevesi görülmektedir.



Şekil 8.1: Tasarlanan Sistem Çerçevesi

KAYNAKLAR

[1] **Maxfield, C.**, 2004, The Design Warrior's Guide to FPGA: devices, tools and flows, Elsevier, Amsterdam

[2] **Ashenden,Peter J.**, 2002, The Designer's Guide to VHDL, Morgan Kaufmann, San Francisco

[3] **Yeniçeri,R.**, 2007, CMOS Görüntü Sensörü ve FPGA ile Sayısal Fotoğraf Makinesi Gerçeklenmesi, *Lisans Tezi*, İ.T.Ü. Elektrik-Elektronik Fakültesi

[4] **Stinson, D.**, 2002, Cryptography: Theory and Practice, Chapman & Hall/CRC, Boca Raton

[5] **Federal Information Processing Standards Publication**, 2001, Advanced Encryption Standard (AES)

[6] **Bellare,M., Kilian,J., Rogaway,P.**, 1999. The Security of the Cipher Block Chaining Message Authentication Code, *Advances in Cryptography – Crypto 94Proceedings*, Springer-Verlag.

ÖZGEÇMİŞ

Oğuz ŞEN, 1986 yılında İzmir'de doğdu. Ortaokulu Bornova Anadolu Lisesi, liseyi İzmir Fen Lisesi'nde tamamladıktan sonra 2004 yılında İstanbul Teknik Üniversitesi Elektronik Mühendisliği programında lisans eğitimine başladı. Haziran 2008'de lisans eğitimi sona erdikten sonra Almanya'da, Münih Teknik Üniversitesi'nde Haberleşme Elektroniği üzerine yüksek lisans düzeyinde eğitimine devam edecektir.