Yapay Sinir Ağları ile Kriptoloji Uygulamaları

Thesis · June 2013

DOI: 10.13140/RG.2.2.29938.61125

2 authors:

Apdullah Yayık
Kara Harp Okulu
29 PUBLICATIONS **73** CITATIONS
SEE PROFILE

Yakup Kutlu
Iskenderun Technical University, Hatay, Turkey
99 PUBLICATIONS **506** CITATIONS
SEE PROFILE

MUSTAFA KEMAK ÜNİVERSTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

ENFORMATİK ANA BİLİM DALI

YAPAY SİNİR AĞI İLE KRİPTOLOJİ UYGULAMALARI

Apdullah YAYIK

Yüksek Lisans Tezi

Antakya/HATAY

Haziran 2013

MUSTAFA KEMAL ÜNİVERSTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

YAPAY SİNİR AĞI İLE KRİPTOLOJİ UYGULAMALARI

APDULLAH YAYIK

YÜKSEK LİSANS TEZİ

ENFORMATİK ANA BİLİM DALI

Yrd.Doç.Dr. Yakup KUTLU danışmanlığında hazırlanan bu tez 05/06/2013 tarihinde aşağıdaki juri üyeleri tarafından oybirliği/oyçokluğu ile kabul edilmiştir.

Yrd.Doç.Dr. Yakup KUTLU Başkan	Yrd.Doç.Dr.Esen YILIDIRM Üye	Yrd.Doç.Dr.Ahmet GÖKÇEN Üye

Bu tezEnstitümüzEnformatikAnabilimDalındahazırlanmıştır.

KodNo :

Doç. Dr. İsmail Hakkı KARAHAN

EnstitüMüdürü

İmzaveMühür

Bu çalışma 8702 numaralı Bilimsel Araştırma Projesi tarafından desteklenmiştir**.**

Proje No:

İÇİNDEKİLER

ÖZET

YAPAY SİNİR AĞLARI İLE KRİPTOLOJİ UYGULAMASI

Bu çalışmada, Yapay Sinir Ağlarının (YSA) kriptoloji biliminin 3 farklı uygulama alanında kullanılabilirliği araştırılmıştır. İlk olarak; YSA tabanlı sözde rastsal sayı üreteci tasarlanarak NIST (Ulusal Teknoloji Standartları Enstitüsü) istatistiksel testleri ile rastsallığı test edilmiş ve 7 adet test başarı ile geçilmiştir. Ardından; YSA modellemesi ile ağırlıkları, nöron sayıları ve transfer fonksiyonları gizli anahtar olarak kullanan açık anahtarlama altyapılı kripto-sistem uygulaması yapılmıştır. YSA ile modellenen bir kripto-sistemin, şifreleme algoritmasına bağlı kalınmaksızın, deşifre edilebileceği öğrenilmiştir. Daha sonra; dijital imza işlemi için kullanılabilecek YSA tabanlı görüntü ve metin Hash Fonksiyonu uygulamaları yapılmış ve Hash değerlerinin duyarlılıklarının resim ve metin için istatistiksel olarak ortalama %90 civarında olduğu hesaplanmıştır.

2013-72

Anahtar Kelimeler : Açık Anahtarlama Altyapısı, Yapay Sinir Ağı Tabanlı Sözde Rastsal Sayı Üreteci, NIST Rastsallık Testleri, Hash Fonksiyonu.

ABSTRACT

CRYPTOLOGY APPLICATION USING ARTIFICIAL NEURAL NETWORK

In this study, the usage of Artificial Neural Network (ANN) in three different implementation of Cryptology Science is investigated. Firstly, ANN based pseudo-random numbers are generated and tested for randomness using seven NIST (National Institute of Standard Technology) Random Tests and resulted successfully. Secondly, a non-linear image and text crypto-system is modeled using ANN and weights, bias, neuron number and transfer function are used as secret key in ANN based asymmetric crypto-system. It is learned that any modeled crypto-system is able to be decrypted regardless of knowing encryption algorithm. Thirdly, ANN based image and text hash algorithm, which can be used for digital signature, is designed and plain text sensitivity of hash value is calculated as approximately %90 statistically for both image and text.

2013-72

Key Words: Asymmetric Crypto-System, ANN Based Pseudo-Random Number Generation, NIST Random Tests, Hash Function.

ŞEKİLLER DİZİNİ

ÇİZELGELER DİZİNİ

1 GİRİŞ

Günümüz bilgi teknolojileri dünyasında bilginin her geçen gün öneminin ve yaygınlığının artması, bilgiye her noktada erişilebilme isteklerinin artışa geçmesi ile beraber bu hususlara izin verecek olan teknolojik imkânlar her geçen gün hızla gelişmektedir. Eski çağlardan bu yana bilginin korunması beraberinde birçok çözümü getirmiş, kriptoloji ise bunlardan günümüze kadar en efektif olan ve kabul görmüş çözüm yolu olarak kendini ispatlamayı başarabilmiştir. Kriptoloji bilginin korunmasında doğal bir antikor görevi görmüş, bilginiz nerede olursa olsun bunun kontrolünüz dışındaki kişiler tarafından erişilebilmesini engellemeyi başarmıştır. Bilgiye artan saldırılar karşısında anlık koruma sağlayan çözümler yetersiz kalmış, özellikle büyük kurumların sahip olduğu verilerin korunması için bilgilerin şifrelenmesi vazgeçilmez bir çözüm olmuştur (Gülyurt, 2013).

Kriptolojide bilgi güvenliğini sağlamak maksadıyla matematiksel teknikler kullanılır. Bilgi güvenliği askeri haberleşmede, ticari ve sosyal medya uygulamalarında art niyeti kişilerden korunmak için günümüzde zorunlu hale gelmiştir. Bilgi sistemlerini tehdit eden birçok bilgisayar korsanı, siber terörist, yazılım hırsızı ve sosyal medya casusu bulunmaktadır (Munukur ve Gnanam, 2007). Dolayısıyla, kriptoloji haberleşme sisteminin en hayati unsurudur. Bir kripto sisteminin kullanılması için; güvenilirlik, kimlik doğrulama, bütünlük ve reddedilemezlik prensiplerini içeriyor olması gerekmektedir.

- Güvenilirlilik

İki kişi arasında gönderilen bilgilerin farklı kişiler tarafından okunmamasını sağlama durumudur. Örnek olarak, gönderilen bir mektubun, alıcıya giderken yolda herhangi bir kişi tarafından okunmasını (örneğin postacı) engelleme amacı güder. Normalde yazılan mektup açık metin şeklindedir ve herhangi bir kişi tarafından zarfın açılması halinde, gönderilmiş mektup okunabilir. Şifreleme bu açık metnin, şifrelenerek yazılması işlemini gerçekleştirir. Bu sayede mektubun yolda giderken herhangi bir kişi tarafından açılması halinde yazı açık metin olmadığı için okunması engellenecektir. Gizlilik, fiziksel ortamlarda güvenlikten,

matematiksel algoritmalara kadar varan birçok yaklaşımla sağlanır ve şifrelemede simetrik ve asimetrik yöntemler kullanılır.

- Kimlik doğrulama

İki merkez arasında gönderilen verinin, alıcı tarafında belirtilen gönderici tarafından gönderildiğinden emin olunması durumudur (*Sayısal İmza*). Kişiye ulaşan bir mektubun üzerinde bulunan gönderici ismi her zaman doğru olmayabilir. Kötü niyetli kişiler tarafından gönderici isimleri farklı yazılarak kişilere mektup yollanabilir (spam mailler gibi). Şifreleme, bilim olarak bu mektuplar üzerine özel imzalar ekleyerek, mektubu gönderen kişinin gerçekten mektubu gönderen kişi olduğundan emin olmayı sağlayabilir.

Gönderilen zaman dilimine göre özel algoritmalarla oluşturulan bu imzalar, alıcı kişi tarafından belirli yöntemlerle doğrulanabilir. Bu imza oluşturma ve doğrulama işlemi dijital imza olarak adlandırılır.

- Bütünlük

İki merkez arasında gönderilen verinin üçüncü kişiler tarafından değiştirilmesini engelleme durumudur. Normal yoldan gönderilen mektup yine üçüncü kişiler tarafından yolda orijinal şeklin dışında başka bir şekle dönüştürülerek yolculuğuna devam ettirilebilir. Yazılan mektup açık metin şeklindedir ve içerik okunabilmektedir. Okunabilen bu açık metin kötü niyetli kişiler tarafından yolda değiştirilerek, alıcıya farklı içerikle gönderilebilir. Şifreleme gönderilen bu düz metin üzerinde işlem yaparak sayısal bir sonuç oluşturur. Bu sonuç gönderilen yazının üzerinde en ufak bir değişiklik yapıldığında, algoritma aynı olduğundan değişecektir.

Gönderici ve alıcı tarafından aynı yazı üzerinde aynı algoritmayla oluşturulan sayısal sonuçlar birbirinin aynı olmak zorundadır. Eğer sayısal sonuçlar birbirini tutmuyorsa gönderilen metin yolda değiştirilmiştir şeklinde düşünülebilir. Çünkü aynı metin üzerinde yapılacak bir değişiklik aynı sayısal sonucu çıkarmayacaktır. Kullanılan algoritma sayesinde farklı metinler üzerinde aynı sayısal sonucun çıkartılması neredeyse imkânsızdır.

- *Reddedilemezlik*

Bilgiyi oluşturan ya da gönderen, daha sonra bilgiyi kendisinin oluşturduğunu veya gönderdiğini inkâr edememelidir. Bir gönderici daha sonrasında bir ileti göndermiş olduğunu yanlışlıkla reddetmemelidir.(Sağıroğlu ve Özkaya, 2007).

2 ÖNCEKİ ÇALIŞMALAR

Bugüne kadar haberleşmede kullanmak maksadıyla güçlü kripto sistemi geliştirmek için birçok çalışma yapılmıştır. Yakın geçmişe dikkatle bakıldığında yapay sinir ağları ile şifreleme teknikleri sıklıkla kullanılmakta olduğunu görmekteyiz. 1993 yılında yapay sinir ağlarının ağırlıkları kriptolojide anahtar olarak kullanılmıştır. Çok katmanlı perseptronların kripto çözmedeki performansının ümit verici olduğu, fakat performansın ağın topolojisi ve girdi uzayındaki gereksiz girdilere oldukça bağımlı olduğu gözlenmiştir. Yapay sinir ağlarının güçlü ve zayıf yönleri dizi şifreleri ve bazı klasik şifreleme tekniklerinde gösterilmiştir. (Tanrıverdi, 1993). 1994 yılında nöral kriptoloji uygulamaları yapılmış ve akıllı kart uygulamalarında kullanılabileceği iddia edilmiştir. (Pointcheval, 1994). Ardından kriptoloji protokolleri ile ilgili yayınlanan kitaplarda bahsedilmiştir. (Scheinder, 1996). Yapay sinir ağlarının kaotik davranmalarına dayanan ve nöronların yapısı simetrik anahtar olarak kullanılan kripto modeli 1999 yılında geliştirilmiştir (Guo ve ark. , 1999). Kaotik bir sistem tarafında üretilen binary sayılara göre değişen ağırlıkları olan yapay sinir ağı ile şifreleme ve deşifreleme çalışması 2000 yılında yapılmıştır (Lin ve Jui-Cheng, 2000). 2002 yılında, L.P.Yee tarafından çok katmanlı yapay sinir ağlarının tek yönlü hash fonksiyon özelliği kripto uygulamasında kullanılmıştır (Yee ve De Silva, 2002). 2003 yılında, IDEA ve ANS X.9 gibi 3DES algoritmalara dayanan klasik kripto sistemleri sözde rastsal sayı üreteçleri tabanlı yapay sinir ağları ile güçlendirmiştir (Karras ve Zorkadis, 2003). 2003 yılında FIPS 140-2 rastsallık testlerini başarı ile geçen eliptik eğri algoritması tabanlı rastsal sayı üreteci tasarlanmıştır (Lee ve Wong, 2004). 2004 yılında C++ programlama dili ile eliptik eğri şifreleme algoritması geliştirilmiştir. Eliptik eğri şifreleme algoritmasının işlemsel gücün, veri saklama kapasitesinin, bant genişliğinin ve güç tüketiminin sınırlı olduğu smart kartları, cep telefonları ve PDA' lar gibi ortamlarda kullanımının tam uygun

olduğunu belirtilmiştir (Yerlikaya, 2004). 2004 yılında kripto analiz aşamasında hangi şifreleme tekniğinin kullanıldığı ve hatta hangi dil ile şifreleme yapıldığı hakkında fikir veren kripto sistemin kimliğinin ve sınıfının nasıl belirleneceği incelenmiştir. Türkçenin yapısal özellikleri temel alınarak kripto analitik bir çalışma yapılmıştır (Derya ve ark., 2004). 2005 yılında, senkronize olan iki yapay sinir ağının ağırlıklarını DES algoritmasında gizli anahtar olarak kullanmıştır (Godhavari ve ark., 2005). 2006 yılında, ağaç paritesi yapılı iki yapay sinir ağının herbian öğrenme kuramı ile ortak çıkış değerinde senkronize olmasını sağlayarak, ağırlıkları ortak gizli anahtar üretmeyi başarılmıştır (Ruttor, 2006). Aynı yıl, YSA tabanlı simetrik şifreleme sistemi dizayn edilmiştir (Arvandi ve ark, 2006). 2007 yılında, yapay sinir ağının bazı verilerini gizli anahtar olarak kullanan algoritma ile elektronik haberleşmede yapay sinir ağı güvenliğini tanıtılmıştır (Sağıroğlu ve Özkaya, 2007). Aynı yıl, şifrelemenin çözülebilmesi için bir kurala dayanması gerektiği prensibini yapay sinir ağları kullanarak kaldırmıştır. Ayrıca, şifrelemenin herhangi bir kurala dayanmadan yapıldığında, yapay sinir ağlarının öğrenme özelliği ile deşifre edilebileceğinin mümkün olduğu iddia edilmiştir. (Munukur ve Gnanam, 2007). 2010 yılında, kaotik kriptolojiyi güçlendirmek için Matlab da yapay sinir ağı tabanlı kaotik sayı üreteci tasarlamıştır. Bayesian Regularization (BR) eğitim fonksiyonu ile eğitilen ve katmanlarındaki farklı boyutlarda olan ve 4 katmanlı yapay sinir ağı ile en az hata veren kripto sistemi tasarlandığını iddia edilmiştir (Dalkıran ve Danışman, 2010). Aynı yıl, Vigenere, Playfair ve Hill Chipper ile şifrelenen metinlerin tekrarlanan verilerinin frekans dağılımından oluşan öznitelikleri yapay sinir ağlarının örüntü tanıma özelliğini kullanarak sınıflandırılmıştır (Sivagurunathan ve ark., 2010). Yapay sinir ağı tabanlı Hash fonksiyonu uygulaması yapılarak istatistiksel testler ile sınanmıştır. Test sonuçları yapay sinir ağlarının sayısal imza uygulamalarında kullanımı için ümit vericidir.(Kulkarni ve ark., 2010) Ayrıca yapay sinir ağı tabanlı S-kutu kullanarak bir kripto sistem geliştirilmiştir (Noughabi ve Sadeghiyan, 2010). 2011 yılında, Matlab ile yapay sinir ağının ezberleme (aşırı öğrenme) özelliğini kullanarak sözde rastsal sayı üreteci yazılımı ve FPGA kullanarak gerekli donanımı geliştirmiş ve geliştirilen donanım ve yazılım bir takım istatistiksel testler (frekans testi, poker testi, seri testi ve otomatik korelâsyon testi) ile sınanmıştır ve sonuç olarak testlerden başarı elde edilmiştir (Othman ve Al Jammas, 2011). SHA-2 güvenli hash

fonksiyonunu ve yapay sinir ağı tabanlı hash fonksiyonu istatistiksel testlerden geçirilmiş ve neredeyse aynı sonuçlar elde edilmiştir (Sumangala ve ark., 2011). 2012 yılında çok katmanlı yapay sinir ağının belirli giriş ve çıkış değerlerinin eğitiminden sonra elde edilen ağırlık matrisleri rastsal sayı olarak değerlendirilmiştir. Üretilen rastsal sayılar NIST testlerine tabi tutulmuş ancak bazı testlerde başarısız olmuştur (Desai ve ark., 2012) .

Bu çalışmada;

Yapay sinir ağı tabanlı sözde rastsal sayı üretimi yapılarak bazı istatistiksel testler ile sınanmış ve sonuçların olumlu olduğu gözlemlenmiştir.

Doğrusal olmayan bir şifreleme yöntemi ile şifrelenen açık metin ve şifreli metin yapay sinir ağı ile modellenmiş ve ağırlıklar, bias ve transfer fonksiyonu bilgisi YSA tabanlı kripto sistem uygulamasının gizli anahtarı olarak kullanılmıştır.

E- imza işlemi için kullanılabilecek YSA tabanlı metin ve resim Hash Fonksiyonu uygulamaları yapılmış ve Hash değerlerinin duyarlılıklarının istatistiksel olarak olumlu olduğu hesaplanmıştır.

Kripto Sistem uygulamanın güvenli oturum açma, çevirim içi güvenli mesajlaşma, güvenli dosya paylaşma ve mesaj özeti (hash değeri) ara yüzleri Matlab ortamında geliştirilmiştir.

3 MATERYAL VE YÖNTEMLER

Bu çalışmada biyolojik sinir ağlarından esinlenerek geliştirilen çok katmanlı yapay sinir ağları kullanılmıştır. Yapay sinir ağları veri madenciliği, optik karakter tanıma ve çok okuma, ürünün pazardaki performansını tahmin etme, kredi kartı hilelerini saptama, zeki araçlar ve robotlar için uygun rota belirleme, güvenlik sistemlerinde konuşma ve parmak izi tanıma gibi birçok çalışma alanında kullanılmaktadır.

Eğer üretilen anahtarların periyodik davranışı kripto analist tarafından tespit edilir ise şifreleme algoritmasının bir güvenliği kalmayacaktır ve kullanılması gereksiz bir yazılım durumuna düşmüş demektir. Bu nedenle herhangi bir kripto sistemde anahtar olarak kullanılacak olan sözde rastsal sayıların mutlak surette rastsallık testlerine tabi tutulması gerekmektedir. Bu çalışmada NIST (Ulusal Standartlar Enstitüsü Teknolojisi) in 2010 yılında yayımladığı rastsallık testleri kullanılmıştır.

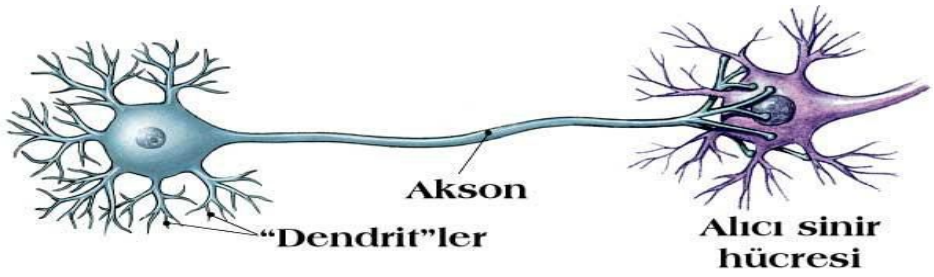
3.1 Biyolojik Sinir Ağları

Biyolojik sinir ağları beynimizde bulunan birçok sayıda sinir hücresinin bir koleksiyonudur. Bir sinir ağı milyonlarca sinir hücresinin bir araya gelmesi ile oluşmaktadır. Sinir hücreleri birbirleri ile bağlanarak fonksiyonlarını yerine getirirler. Beynimizde 10^{10} adet sinir hücresi ve bunlarında 6x 10^{13} ′ den fazla sayıda bağlantısının olduğu bilinmektedir. İnsan beyni, çok hızlı çalışabilen mükemmel bir bilgisayar gibi görünebilir. Biyolojik sinir ağlarının performansları küçümsenmeyecek kadar yüksek ve karmaşık olayları işleyebilecek yetenektedir. Bir grup insan resmi içinden tanıdık bir resmi 100-200 ms gibi kısa bir sürede fark edebilir. Hâlbuki geleneksel bilgisayarları böyle bir tanıma işlemi yapması çok uzun zaman alabilir. Bugün insan beyninin kapasitesinin çok küçük bir oranında kapasiteye sahip ve çalışabilen bir makine yapılsa olağanüstü bilgi işleme ve kontrol edebilme mekanizmaları geliştirmek ve mükemmel sonuçlar elde etmek mümkün olabilir. Yapay sinir ağları ile bu yeteneğin bilgisayara kazandırılması amaçlanmaktadır.

3.1.1 Biyolojik Sinir Hücresinin Yapısı

Biyolojik sinir hücresi insan beyninin çalışmasını sağlayan en temel taşlardan birisidir. İnsanın bütün davranışlarını ve çevresini anlamasını sağlarlar. Biyolojik sinir ağları beş duyu organından gelen bilgiler ışığında geliştirdiği algılama ve anlama mekanizmalarını çalıştırarak olaylar arasındaki ilişkileri öğrenir. (Önal 2009; Öztemel, 2003).

Biyolojik sinir sisteminin temel yapı taşı olan nöronların yapısı dendrit, akson, çekirdek ve bağlantılar olmak üzere dört ana bölümden oluşmaktadır (Şekil 3-1). Dendritlerin sinir hücresinin ucunda bulunan ve ağaç kökü görünümüne sahip bir yapıya sahiptir. Dendritlerin görevi bağlı olduğu diğer nöronlardan veya duyu organlarından gelen sinyalleri çekirdeğe iletmektir. Çekirdek dendrit tarafından gelen sinyalleri bir araya toplayarak ve aksona iletir. Toplanan bu sinyaller akson tarafından işlenerek nöronun diğer ucunda bulunan bağlantılara gönderilir. Bağlantılar ise yeni üretilen sinyalleri diğer nöronlara iletir.



Şekil 3-1 Biyolojik Sinir Hücresi

3.1.2 Biyolojik Sinir Ağlarının Yapısı

Bir insanın beyninde yaklaşık olarak 10 milyar sinir hücresi ve bu nöronların birbirleriyle yaptığı bağlantı sayısının ise 60 trilyon olduğu tahmin edilmektedir. Bu sinirler girdi bilgilerini duyu organlarından alırlar. Daha sonra alıcı (taşıyıcı) sinirler bu sinyalleri işleyip bir sonraki sinire aktararak sinyalin merkezi sinir sistemine kadar ulaşmasını sağlar. Merkezi sinir sistemi bu sinyalleri alıp yorumladıktan sonra tepki sinyallerini üretir. Bu sinyaller de tepkilerin oluşacağı organlara tepki sinirleri vasıtasıyla iletilir. Bu sayede duyu organlarından gelen bilgilere karşı tepki organlarına uygun işaretler Şekil 3-2' de gösterildiği gibi sinir sistemi vasıtasıyla yollanır.

Şekil 3-2 Biyolojik Sinir Ağı Yapısı

3.2 Yapay Sinir Ağları

Yapay sinir ağları (YSA) insan beyninin çalışma sisteminin yapay olarak benzetimi çabalarının bir sonucu olarak ortaya çıkmıştır. En genel anlamda bir YSA insan beynindeki birçok nöronun (sinir hücresinin), ya da yapay olarak basit işlemcilerin birbirlerine değişik etki seviyeleri ile bağlanması sonucu oluşan karmaşık bir sistem olarak düşünülebilir. Önceleri temel tıp birimlerinde insan beynindeki nöronların matematiksel modelleme çabaları ile başlayan çalışmalar, geçtiğimiz on sene içerisinde, disipline bir şekil almıştır. YSA bugün fizik, matematik, elektrik ve bilgisayar mühendisliği gibi çok farklı bilim dallarında araştırma konusu haline gelmiştir (Hamzaçelebi ve Kutay, 2004).

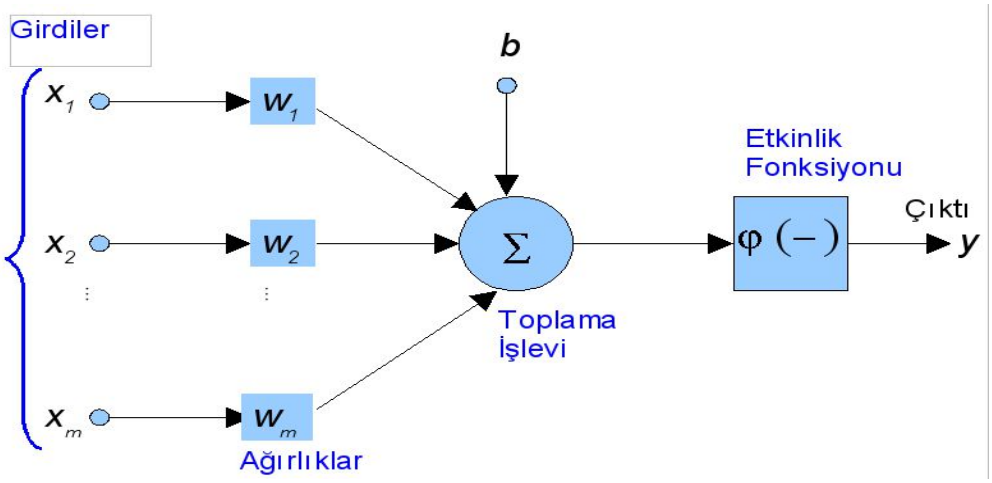
3.2.1 Yapay Sinir Hücresinin Yapısı

Yapay sinir hücreleri de biyolojik sinir hücrelerine benzer yapıdadır. Yapay nöronlar da aralarında bağ kurarak yapay sinir ağlarını oluştururlar.

Bir yapay sinir hücresi Şekil **3-3**'de gösterildiği gibi 6 bölümden oluşmaktadır;

- *Girdi Katmanı*
- *Ağırlıklar*

- *Ara Katman*
- *Toplama fonksiyonu*
- *Aktivasyon fonksiyonu*
- *Çıktılar*



Şekil 3-3 Yapay Sinir Hücresi

Girdi Katmanı

Girdiler nöronlara gelen verilerdir. Girdiler yapay sinir hücresine bir diğer hücreden gelebileceği gibi direk olarak dış dünyadan da gelebilir. Bu girdilerden gelen veriler biyolojik sinir hücrelerinde olduğu gibi toplanmak üzere toplayıcıya gönderilir. Bu katmandaki işlem elemanları dış dünyadan bilgileri alarak ara katmanlara transfer ederler. Bazı ağlarda girdi katmanında herhangi bir bilgi işleme olmaz.

Ağırlıklar

Yapay sinir hücresine gelen bilgiler girdiler üzerinden çekirdeğe ulaşmadan önce geldikleri bağlantıların ağırlığıyla çarpılarak çekirdeğe iletilir. Bu sayede girdilerin üretilecek çıktı üzerindeki etkisi ayarlanabilinmektedir. Bu ağırlıkların değerleri pozitif, negatif veya sıfır olabilir. Ağırlığı sıfır olan girdilerin çıktı üzerinde herhangi bir etkisi olmamaktadır. Bir ağırlığın değerinin büyük olması, o girişin yapay sinire güçlü bağlanması ya da önemli

olması, küçük olması zayıf bağlanması ya da önemli olmaması anlamına gelir (Elmas, 2011).

Ara Katman

Girdi katmanından gelen bilgiler işlenerek çıktı katmanına gönderilirler. Bu bilgilerin işlenmesi ara katmanlarda gerçekleştirilir. Bir ağ içinde birden fazla ara katman olabilir.

Toplama Fonksiyonu

Toplama fonksiyonu, bir hücreye gelen net girdiyi hesaplayan bir fonksiyondur ve genellikle net girdi, girişlerin ilgili ağırlıkla çarpımlarının toplamıdır (3.1). Toplama fonksiyonu, ağ yapısına göre maksimum alan, minimum alan ya da çarpım fonksiyonu olabilir.

$v=f(X_i.Y_i)$ $y=\mathbf{F}(v)$ (3.1)

w: Hücrenin ağırlıklar matrisini

x: Hücrenin giriş vektörünü

v: Hücrenin net girişini

y: Hücre çıkışını

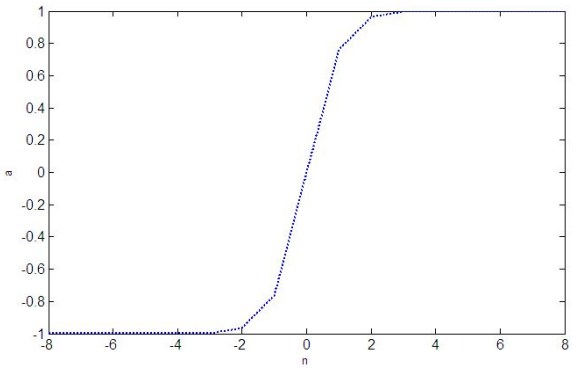
Aktivasyon Fonksiyonu

Toplama fonksiyonundan çıkan NET toplam hücrenin çıktısını oluşturmak üzere aktivasyon fonksiyonuna iletilir. Aktivasyon fonksiyonu genellikle doğrusal olmayan bir fonksiyon seçilir. Kullanılan aktivasyon fonksiyonları aşağıda belirtilmiştir.

- *Tansig*

Bu aktivasyon fonksiyonu için nöron giriş- çıkış ifadesi 3.2'de ve fonksiyonun değişimi Şekil 3-4'de verilmiştir. Fonksiyonun dinamik değişim aralığı [-1 1] aralığıdır ve

fonksiyon nöron toplam girişe olarak bu aralıkta lineer olmayan bir değişim gösterir. Bu fonksiyon hiperbolik-tangent fonksiyonu olarak da isimlendirilmektedir.

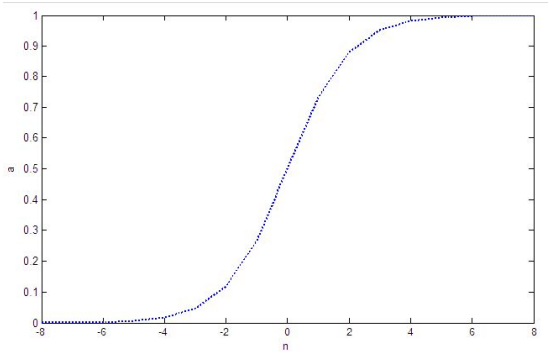


Şekil 3-4 Tangent-Sigmoid fonksiyonu giriş-çıkış eğrisi

$$\text{Tansig(n)}=\frac{2}{1+e^{(-2n)}}-1 \qquad (3.2)$$

❖ *Logsig*

Sigmoid fonksiyonu olarak da isimlendirilen bu aktivasyon fonksiyonunun giriş-çıkış ifadesi ve fonksiyonun girişe göre değişimi 3.3 ifadesinde ve Şekil 3-5'de belirtilmiştir. Fonksiyonun dinamik değişim aralığı [0 1] aralığıdır ve fonksiyon bu aralıkta lineer olmayan bir değişim sergiler.

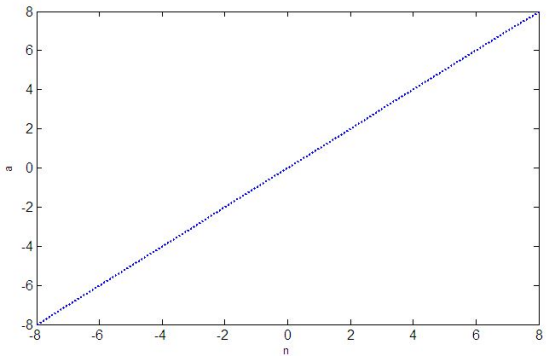


Şekil 3-5 Logaritmik Sigmoid fonksiyonu giriş-çıkış eğrisi

$$\text{Logsig(n)}=\frac{1}{1+e^{n}} \qquad (3.3)$$

❖ *Purelin*

Bu aktivasyon fonksiyonunda nöron girişlerinin değişimine göre nöron çıkışı lineer olarak değişmektedir. Dinamik değişim aralığı [-1 1] aralığıdır. Fonksiyona ait giriş-çıkış karakteristiği Şekil 3-6 ve fonksiyon tanımı 3.4' de aşağıda verilmiştir.



Şekil 3-6 Purelin fonksiyonu çıkış eğrisi

$$\text{Purelin}(n) = n \tag{3.4}$$

Yapay sinir ağlarının bir özelliği olan "doğrusal olmama" aktivasyon fonksiyonlarının doğrusal olmama özelliğinden gelmektedir.

Aktivasyon fonksiyonu seçilirken dikkat edilmesi gereken bir diğer nokta ise fonksiyonun türevinin kolay hesaplanabilir olmasıdır. Geri beslemeli ağlarda aktivasyon fonksiyonunun türevi de kullanıldığı için hesaplamanın yavaşlamaması için türevi kolay hesaplanır bir fonksiyon seçilir (Altun ve Eminoğlu, 2006)

Çıktılar

Bu katmandaki işlem elemanları ara katmandan gelen bilgileri işleyerek ağın girdi katmanından sunulan girdi seti için üretmesi gereken çıktıyı üretirler. Üretilen çıktı dış dünyaya gönderilir.

3.2.2 Yapay Sinir Ağlarının Yapısı

Mühendislik uygulamalarında YSA' nın geniş çaplı kullanımının en önemli nedeni, klasik tekniklerle çözümü zor problemler için etkin bir alternatif oluşturmasıdır. Çünkü bilgisayarlar insanın beyinsel yeteneğinin en zayıf olduğu çarpma, bölme gibi matematiksel ve algoritmik hesaplama işlemlerinde hız ve doğruluk açısından yüzlerce kat başarılı olmalarına rağmen insan beyninin öğrenme ve tanıma gibi işlevlerini hala yeteri kadar gerçekleştirememektedirler.

İnsan vücudu, sinir sistemi sayesinde yaşadığı olaylardan meydana gelen her türlü fiziksel, biyolojik ve kimyasal değişim karşısında, değişimlere alışabilmek maksadıyla kendisini yenilemekte ve çeşitli reaksiyonlar üretmektedir. Bütün sistemleri uyumlu çalışan bu sistem birçok araştırmacıya çalışmalarında esin kaynağı olmuştur. Etrafımızda meydana gelen değişimler, vücuttaki sinirler tarafından algılanmakta, beyne iletilmekte ve karar mekanizması olarak çalışan beyin, algıya karşılık en uygun tepkiyi üretmek için vücuttaki gerekli alt sistemleri uyarmaktadır. Yani, insan vücudundaki sinir sistemi, Algılama-Karar Verme-İcra Etme fonksiyonlarını yürüten harika bir yapıdır (Dalkıran, 2003).

Yapay sinir ağları, insanlar tarafından gerçekleştirilmiş örnekleri (gerçek beyin fonksiyonlarının ürünü olan örnekleri) kullanarak olayları öğrenebilen, çevreden gelen olaylara karşı nasıl tepkiler üretileceğini belirleyen bilgisayar sistemleridir. İnsan beyninin fonksiyonel özelliklerine benzer şekilde,

- *Öğrenme*
- *İlişkilendirme*
- *Sınıflandırma*
- *Genelleme*
- *Özellik belirleme*
- *Optimizasyon*

gibi konular da başarılı bir şekilde uygulanmaktadır (Önal, 2009).

Bugün dahi insan beyninin yetenekleri, kapasitesi ve sınırları hala tam anlamıyla çözülememiştir. Bu konuda; biyologlar beynin biyolojik yapısını incelemek ve gizemlerini çözmek için, matematikçiler matematiksel modelini ortaya koymak için çalışmaktadırlar. Yapay sinir ağların (YSA) temeli ilk olarak 1943 yılında ortaya atılmıştır. Bir nörobiyolog olan Warren McCulloch ve bir matematikçi olan Walter Pitts ile başlayan, Von Neumann ve Minsky ile devam eden çalışmalar, yapay nöronlardan oluşan ağların hesaplama yapabileceğini göstererek bu alanda atılan önemli adımlardır. 1970'lerde öğrenme algoritmalarının, uygulamadaki problemlerin çözümünde yetersiz kalması ve mevcut teknik imkânların kısıtlı olması nedeniyle yapay sinir ağları ile ilgili çalışmalar yavaşlamıştır. 1980'li yılların ikinci yarısından itibaren bilgisayar teknolojisindeki gelişmelere paralel olarak yapay sinir ağlarındaki gelişmeler de tekrar hız kazanmıştır. 1986 yılında geri yayılım öğrenme algoritmasının geliştirilmesiyle karmaşık problemlerin çözümünde eğitilen çok katmanlı ağ sistemlerinin kullanılabileceği gösterilmiştir (Dalkıran, 2003).

Doğada olduğu gibi yapay sinir ağlarında da elementler arasındaki bağlantı ağ fonksiyonunu belirtmektedir. Elementler arasındaki bağlantıları (ağırlıkları) değiştirilerek yeni bir yapay sinir ağı geliştirilebilmektedir. Yapay sinir ağlarının ağırlıkları belirli giriş değerleri ile belirli çıkış değerleri elde edene kadar değiştirilir, yani eğitilir. Yapay sinir ağlarının eğitimi hedeflenen çıkış değeri ile mevcut çıkış değeri aynı olana kadar (veya çok yakın) olana kadar devam eder (Demuth ve ark., 2004).

Yapay sinir ağları yapay nöronların ağırlıklandırılmış grafiğidir (Scheinder, 1996). Yapay sinir ağlarının avantajlarından bazıları; bilinen durumlardaki sonuçları kullanarak bilinmeyen durumlar hakkında karar verilebilmesi, işletiminde hızlı tepki verilebilmesi ve güvenilirlik ile verimlilik derecesinin yüksek olmasıdır (Dalkıran ve Danışman, 2010).

İlk katmanına giriş bilgisinin uygulandığı, en son katmanından ise çıkış bilgisinin alındığı ileri beslemeli bir yapıda ara katmalar, giriş ve çıkış katmaları arasındaki bağlantıyı sağlamakta olup dış ortam ile herhangi bir bilgi alış-verişinde bulunmazlar. İleri beslemeli ağ modelinde herhangi bir katmanın içerisinde veya katmanlar arasında, çıkıştan girişe doğru bir geri besleme olmayıp bütün bağlantılar girişten çıkışa doğru veri akışını

sağlayacak şekilde yapılmıştır. Bu öğrenme algoritmaları kullanılarak eğitilebilecek ileri beslemeli ağ modellerine Çok Katmanlı Perceptron (Multi Layer Perceptron, MLP) ve LVQ (Learning Vector Quantization) ağları örnek olarak verilebilir (Dalkıran, 2003).

MLP ağları giriş, bir veya daha fazla sayıda ara ve çıkış katlarına sahip olup mimari açıdan ileri beslemeli, öğrenme algoritması bakımından danışmanlı öğrenen ağlar sınıfındadır. Çok sayıda öğrenme algoritması kullanılarak eğitilebilen bu ağ yapısında; giriş, çıkış ve ara katlarda bulunan nöron sayısı problemin karmaşıklığı ile ilgili olup bu sayı tecrübeye dayalı olarak belirlenir. MLP ağlarında, uygulanan girişe karşılık üretilen çıkış ile hedef çıkış arasındaki hata, kullanılan öğrenme algoritmasına göre tekrar değerlendirilerek; hata değeri en aza düşürülünceye veya belirlenen iterasyon sayısına ulaşılıncaya kadar ağın ağırlıkları değiştirilir. Ayrıca ağ içerisinde ara bağlantılar girişten çıkışa doğru olduğu için herhangi bir andaki çıkış sadece o andaki girişin bir fonksiyonu olarak ifade edilir. Bundan dolayı bu tür ağlar statik ağlar olarak da bilinmektedir (Dalkıran, 2003).

3.2.3 Yapay Sinir Ağlarının Genel Özellikleri

Yapay sinir ağlarının karakteristik özellikleri uygulanan ağ modeline göre değişmektedir. Burada bütün modeller için geçerli olan genel karakteristik özellikler aşağıdaki gibi sıralanmıştır.

- Yapay sinir ağları makine öğrenmesi gerçekleştirirler.
- Programları çalışma stili bilinen programlama yöntemlerine benzememektedir.
- Bilginin saklanması sağlanmaktadır.
- Yapay sinir ağları örnekleri kullanarak öğrenirler.
- Yapay sinir ağlarının güvenle çalıştırılabilmesi için önce eğitilmeleri ve performanslarının test edilmesi gerekir.
- Görülmemiş örnekler hakkında bilgi üretilebilirler.
- Algılamaya yönelik olaylarda kullanılabilirler.
- Şekil (örüntü) ilişkilendirme ve sınıflandırma yapabilirler.
- Örüntü tamamlama gerçekleştirebilirler.
- Kendi kendini organize etme ve öğrenebilme yetenekleri vardır.

- Eksik bilgi ile çalışabilmektedirler.
- Hata toleransına sahiptirler.
- Belirsiz, tam olmayan bilgileri işleyebilirler.
- Dereceli bozulma gösterirler.
- Dağıtık belleğe sahiptirler.
- Sadece nümerik bilgiler ile çalışabilmektedirler.

Yukarıda belirtilen özelliklere ek olarak geliştirilmiş olan her modelin kendisine özgü özellikleri olabilmektedir (Önal 2009; Öztemel 2003).

YSA' nın hesaplama ve bilgi işleme gücünü, paralel dağılmış yapısından, öğrenebilme ve genelleme yeteneğinden aldığı söylenebilir. Genelleme, eğitim ya da öğrenme sürecinde karşılaşılmayan girişler için de YSA' nın uygun tepkileri üretmesi olarak tanımlanır. Bu üstün özellikleri, YSA' nın karmaşık problemleri çözebilme yeteneğini gösterir. Günümüzde birçok bilim alanında YSA, aşağıdaki özellikleri nedeniyle etkin olmuş ve uygulama yeri bulmuştur. Yapay sinir ağlarının üstün özellikleri aşağıda açıklanmıştır.

Doğrusallık

YSA' ların yapıları gereği doğrusal ağlar olduğu gibi, daha çok doğrusal olmayan yönleriyle öne çıkmıştır. Ağın ya da temel işlem elemanı olan hücrenin, doğrusallığı *aktivasyon fonksiyonu* ile belirlenir. Bu özelliği ile YSA, özelikle doğrusal olmayan karmaşık problemlerin çözümünde en önemli araç durumuna gelmiştir.

Öğrenme

YSA' nın arzu edilen davranışı gösterebilmesi için amaca uygun olarak tasarlanması gerekir. Bu durum, hücreler arasında doğru bağlantıların yapılması ve bağlantıların uygun ağırlıklara sahip olması gerektiğini ifade eder. YSA' nın karmaşık yapısı nedeniyle bağlantılar ve ağırlıklar önceden ayarlı olarak verilemez ya da tasarlanamaz. Genellikle ağırlıklar, rastgele ya da sabit bir değerde seçilir. YSA, istenen davranışı gösterecek şekilde ilgilendiği problemden aldığı eğitim örneklerini kullanarak problemi öğrenmelidir. Belli bir

hata kriterine ve öğrenme algoritmasına göre, ağırlıkların yenilenerek, artık değişmediği durumda öğrenmenin gerçekleştiği söylenebilir.

Genelleme

YSA, ilgilendiği problemi öğrendikten sonra eğitim sırasında karşılaşmadığı test örnekleri için de arzu edilen tepkiyi üretebilir. Örneğin, karakter tanıma amacıyla eğitilmiş bir YSA, bozuk karakter girişlerinde de doğru karakterleri verebilir ya da bir sistemin eğitilmiş YSA modeli, eğitim sürecinde verilmeyen giriş sinyalleri için de sistemle aynı davranışı gösterebilir.

Uyarlanabilirlik

YSA, ilgilendiği problemdeki değişikliklere göre ağırlıklarını ayarlar. Yani, belirli bir problemi çözmek amacıyla eğitilen YSA, problemdeki değişimlere göre tekrar eğitilebilir, değişimler devamlı ise gerçek zamanda da eğitime devam edilebilir. Bu özelliği ile YSA, sinyal işleme, uyarlamalı sistem tanıma ve denetim gibi alanlarda etkin olarak kullanılır.

Hata Toleransı

YSA, çok sayıda hücrenin çeşitli şekillerde bağlanmasından oluştuğundan paralel dağılmış bir yapıya sahiptir ve ağın sahip olduğu bilgi, ağdaki bütün bağlantılar üzerine dağılmış durumdadır. Bu nedenle, eğitilmiş bir YSA' nın bazı bağlantılarının hatta bazı hücrelerinin etkisiz hale gelmesi, ağın doğru bilgi üretmesini önemli ölçüde etkilemez. Bu nedenle, geleneksel yöntemlere göre hatayı indirgeme yetenekleri son derece yüksektir.

Donanım ve Hız

YSA, paralel yapısı nedeniyle büyük ölçekli bütünleşmiş devre teknolojisi ile gerçeklenebilir. Bu özellik, YSA' nın hızlı bilgi işleme yeteneğini artırır ve gerçek zamanlı uygulamalarda kullanılabilmesini mümkün kılar.

Analiz ve Tasarım Kolaylığı

YSA' nın temel işlem elemanı olan hücrenin yapısı ve modeli, bütün YSA yapılarında yaklaşık aynıdır. Dolayısıyla, YSA' nın farklı uygulama alanlarındaki yapıları da standart yapıdaki bu hücrelerden oluşacaktır. Bu nedenle, farklı uygulama alanlarında kullanılan farklı mimarilerdeki YSA' lar, benzer öğrenme algoritmalarını ve teorilerini paylaşabilirler. Bu özellik, problemlerin YSA ile çözümünde önemli bir kolaylık getirecektir.

Yazılım yardımıyla daha kolay kurulabilen yapay sinir ağları, yine yazılımsal olarak çalıştırılabilmesi de rahat olabilecek modellerdir. Ancak elektronik devrelerle kurulan yapay sinir ağı modelleri doğal olarak yazılım ile kurulan modellere kıyasla daha hızlı sonuca ulaşabilecektir. Bu sebepten dolayı, yapay sinir ağları günümüzde yazılımsal olarak kurulup, çalıştırılıp, test edilmekte ve gerekli tüm değişiklikler ve dinamik güncellemeler yapılmakta, ardından sonuçlara göre karar verilmektedir. Eğer elde edilen sonuçların başarısı %99'lar ifade edilebiliniyorsa, o zaman gerekli görüldüğü takdirde model elektronik devreler üzerine aktarılmaya çalışmaktadır. Böylece yapay sinir ağ modelleri, gerçek yasama uygulanmak üzere fiziksel bir platform üzerinde hazır hale getirilmiş olmaktadır.

3.3 Kriptoloji

Kriptoloji, Yunanca krypto's (saklı) ve lo'gos (kelime) kelimelerinin birleştirilmesinden oluşturulmuştur ve iletişimde gizlilik bilimi olarak değerlendirilmektedir. Ticari ilişkilerde, devlet işlerinde, askeri işlerde ve personel ilişkilerinde güvenli iş çalışması yapmak büyük bir sorundur. Sistemler arası bağlantılarda ya da herhangi iki nokta arasındaki haberleşmede verinin güvenli bir şekilde gittiğinden emin olmak gerekir. Bunun sağlanması ise gönderilen verinin şifrelenmesi ile olur. Böylece açık haberleşme kanalları kullanılarak verinin güvenli bir şekilde ulaştırılması sağlanır. İletişimde, açık bir haberleşme kanalı kullanılıyorsa gizli tutulmak istenen bilginin yetkisiz bir kişi tarafından dinlenebileceği veya haberleşme kanalına girip veriyi bozabileceği ya da değiştirebileceği düşüncesi her zaman için önemli bir problem oluşturur. Şifreleme işlevinin en geleneksel kullanımı bilgilerin belirli kişilerden saklanması amacını güden kullanımdır. Bu fikir ister istemez,

rakip ya da düşman kavramına da referansta bulunur. Bu bağlamda bilginin gizlenmesi genellikle bir mesajın şifrelenmesini yani rakibin eline geçse dahi rakip tarafından kolayca anlaşılamayacak, çözülemeyecek bir şekle dönüştürülmesi anlamına gelir (Şekil 3-7).

Şekil 3-7 Şifreleme ve Şifre Çözme

Gizleme yani dönüştürme işleminin sahip olması gereken bir diğer önemli özellik de, mesajı alması beklenen yetkili kişinin şifrelenmiş mesajı kolayca ve kısa sürede çözebilmesidir.

Klasik şifre elektronik bilgisayarların ortaya çıkmasından önce geliştirilen veya kullanılan şifre kast edilmektedir. ENIGMA ve II. Dünya Savaşı esnasında kullanılan benzerleri elektronik-öncesi kriptografi alanının doruktaki temsilcileridir.

Kriptoloji esas olarak iki bölüme ayrılır: Kriptografi (şifreleme) ve kripto analiz (şifre çözme). Gönderilmek istenen orijinal mesaj açık mesaj ve bu mesajın şifrelenmiş halinin adı şifreli mesaj olarak adlan uzun yıldır kullanılmaktadır. Sağlık hizmetleri, finansal işler gibi konularda bilgisayarlar arasındaki haberleşmede açık kanallar kullanılarak yapılmaktadır. Bu açık kanalların kullanılması sırasında yukarıda sayılan işlerin güvenli ve gizli bir şekilde yapılabilmesi için şifrelemeye gerek duyulmaktadır (Yerlikaya, 2003).

Kriptografi bilimi anahtar kullanım özelliklerine bağlı olarak iki farklı algoritma sistemi ortaya koyulmuştur.

3.3.1 Gizli Anahtarlama Altyapılı (Simetrik) Şifreleme Algoritmaları

Simetrik şifreleme algoritmaları şifreleme ve deşifreleme işlemleri için Şekil 3-8 'de gösterildiği gibi tek bir gizli anahtar kullanmaktadır. Şifreleme işlemlerini gerçekleştirdikten sonra şifreli metni alıcıya gönderirken şifreli metinle birlikte gizli anahtarı da alıcıya güvenli bir şekilde göndermesi gerekmektedir. Simetrik şifreleme algoritmaları çok hızlı şifreleme ve deşifreleme işlemleri gerçekleştirilebildiğinden dolayı günümüzde çok yaygın olarak kullanılmaktadır.

Şekil 3-8 Gizli Anahtarlama Altyapısı

Simetrik şifre, şifreleme için kullanılan anahtarın şifreyi çözmek için kullanılan anahtara denk olduğu şifredir. Şifreleme ve şifre çözme için kullanılan anahtarlar birbirinin aynısıdır yani gönderici ve alıcı *aynı gizi* paylaşırlar.

Alıcı ve göndericinin simetrik şifreleme kullanarak güvenli bir şekilde haberleşmesi için, bir anahtar üzerinde anlaşmaları ve bu anahtarı gizli tutmaları gerekmektedir. Eğer bu kişiler ayrı konumlarda bulunuyorsa, taşıyıcının, telefon sisteminin ya da diğer tasıma ortamlarının özel anahtarın saklanabilmesi açısından yeterli güvenilirlikte olması gerekmektedir. Çünkü anahtarı ele geçirecek her kişi, şifreyi çözebilir. Anahtarların üretimi, iletimi ve saklanması anahtar yönetimi olarak adlandırılır ve tüm şifreleme sistemleri anahtar yönetimi sorunlarıyla uğraşmak durumundadır. Anahtarların gizli

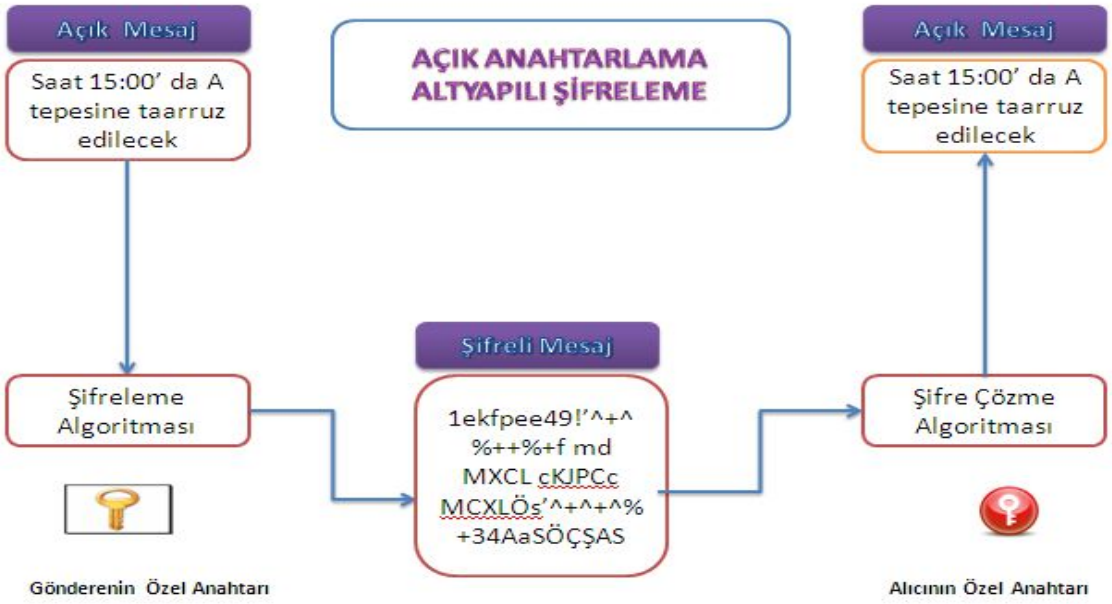
kalmasını gerektirdiğinden dolayı, simetrik şifreleme, özel anahtar yönetiminde oldukça sıkıntı yasamaktadır. (Yavuz, 2006)

3.3.2 Açık Anahtarlama Altyapılı (Asimetrik) Şifreleme Algoritmaları

Esasen, 1975 yılına dek simetrik türden farklı bir şifreleme tekniği tasarlanabileceği düşünülmüyordu. 1975Simetrik şifrelemedeki anahtar paylaşım sorununu çözmek için, 1976 yılında Whitfield Diffie ve Martin Hellman tarafından asimetrik şifreleme tekniği geliştirilmiştir. Bu yöntemde, bilindiği gibi iki ayrı anahtar kullanılması ve herhangi bir anahtar transferinin gerekmemesi güvenliği artırmaktadır. Kullanılan anahtar ilgili şahıstan başka kimseyi ilgilendirmez. Bu modele göre şifreleme anahtarı (aynı zamanda açık anahtar olarak anılır ve kamuoyuna açıktır), şifreyi çözme anahtarına (aynı zamanda gizli anahtar olarak anılır ve sadece şifreyi çözmeye yetkili kişinin bilgisi dâhilindedir) dair çok az bilgi verir ve tersi de doğrudur. Şifreleme ve çözme işlemi birbirinin simetriği olmayan algoritmalarla gerçekleştirildiğinden dolayı da asimetrik şifreleme sistemi olarak bilinir.

Asimetrik şifreler aynı zamanda matematiksel analiz bakımından da oldukça ilginçtirler çünkü bu şifrelerin çözümünün zorluğu doğrudan bazı önemli matematiksel problemlerin çözümünün zorluğu ile bağlantılıdır. Simetrik şifreler, matematiksel bakımından, asimetrik şifrelere kıyasla daha basittirler.

Simetrik şifreleme tekniğinde bulunan anahtar dağıtım problemini çözmek için Şekil 3-9' da gösterildiği gibi şifreleme ve çözme işlemlerinin her birisi için ayrı anahtar kullanma prensibine dayanan bir şifreleme sistemi geliştirilmiştir. Bu sistemde şifreleme işlemi herkes tarafından bilinen açık anahtarla yapılır (Şekil 3-9).



Şekil 3-9 Açık Anahtarlama Altyapısı

Açık anahtarlı şifrelemede, özel anahtar her zaman matematiksel olarak açık anahtara bağlıdır. Bu yüzden, açık anahtardan özel anahtar üretilerek açık anahtarlı bir sistemin şifresinin kırılması her zaman için mümkündür. Bu duruma önlem olarak, açık anahtardan özel anahtar türetilmesinin mümkün olduğunca çok zor gerçekleşmesi sağlanmalıdır.

Açık anahtarlama alt yapılı kripto sistemlerde bilgiler yetkisiz kişiler tarafından ele geçirildiğinde ülke savunmasını riske sokacak kadar özel ya da bir bankayı batırabilecek kadar ön değerli ise şifreli metin ile alıcının özel anahtarı farklı kanallardan gönderilebilir. Örneğin şifreli metin elektronik ortamdan iletilirken anahtar güvenli bir kurye ile iletilebilir.

3.3.3 Yapay Sinir Ağlarının Kriptolojide Hash Fonksiyonu Olarak Kullanılmasının Avantajları

Eğer ulaşılması hedeflenen değer (y_k) giriş değerine (x_k) göre çok farklılık gösteriyor ise, giriş değeri kullanılarak ulaşılması hedeflenen değere ulaşmak çok zor olurken (3.5), hedeflenen değerden giriş değerini hesaplamak kolay olmaktadır. Yapay sinir ağları bu özelliğinden dolayı hash fonksiyonlarında kullanılmaktadır. Yapay sinir ağlarında paralel

uygulama önemli bir özelliktir. Her katman paraleldir. Böylece her katmanda bağımsız fonksiyon uygulanabilir. Bu yüzden veri işleme uygulamaları için uygundur.

$$y_k = Ø\left(\sum_{j=1}^{m} w_{k,} x_j + b_k\right) \tag{3.5}$$

Karmaşıklık, yapay sinir ağlarının doğrusal olmayan yapısından kaynaklanan özel bir özelliğidir. Bu özellik hedeflenen değer ile giriş değerleri arasında doğrusal olmayan ve karmaşık bir bağ kurulmasını sağlar. Yani, çıkış değerlerinin her biri giriş değerlerinin her birine karmaşık bir bağ ile bağlıdır. Bundan dolayı, giriş değerlerinin tam olarak belirlenmesi çok zordur. Karmaşıklık özelliği yapay sinir ağlarını kriptoloji uygulamalarında bir adım taşımaktadır.

Sayısal İmza

Açık anahtarlı şifrelemenin bir diğer yararı da, sayısal imzayı sağlayacak metotlar sunmasıdır. Günlük hayatta kullanılan imzalarda olduğu gibi, sayısal imzalar da elektronik ortamda gönderilen bilginin veya e-mail'in kime ait olduğunu göstermek için kullanılır. Açık Anahtar Altyapı çatısının kullanılmaya başlanması ile yaygınlaşan sayısal imza, bir anahtar çifti (açık ve özel anahtarlar) ile elektronik ortamda iletilen veriye vurulan bir mühürdür. Karmaşık algoritmaların meydana getirdiği şifreleme teknolojisini kullanarak oluşturulmuş sayılar serisidir. Yani belgenin içeriğinin şifrelenerek saklanmasıdır. Sayısal imzalar göndericinin kimliğinin kesin bir biçimde teyit edilmesini ve elektronik dokümanın bütünlüğünün kontrolünü mümkün kıla, inkar edilemez özelliktedir. Sayısal bir imza, kişinin el yazısı ile attığı imzaya eş değerdir. Aynı amaçla kullanılır. Ancak, el yazısı ile atılan imzanın taklit edilmesi kolaydır. Buna karsın, sayısal imzanın taklit edilmesi nerdeyse imkânsızdır. Sayısal imzaların oluşturulmasında ve doğrulanmasında sayısal sertifikalar kullanılır. Gönderilen verinin imzalanması için, gönderen kişiye ait bir sayısal sertifika olması gerekmektedir (Yavuz, 2006).

3.3.4 Hash Fonksiyonları

Kriptografik hash fonksiyonları modern kriptografide temel bir rol oynar. Hash fonksiyonları ile büyük tanım bölgeleri küçük değer bölgelerine dönüştürülür. Hash fonksiyonu girdi olarak bir mesajı alır ve hash kodu, hash sonucu, hash değeri, mesaj özeti veya kısaca hash ile belirtilen bir çıktı üretir. Daha kesin bir ifadeyle bir hash fonksiyonu keyfi sonlu boyutlu bit şeritlerini n-bit diyebileceğimiz sabit uzunluklu şeritlere dönüştürür. En iyi bilinen hash fonksiyonları MD-2, MD-4, MD-5, SHA-1, SHA-2 ve SHA-3' dür. Hash fonksiyonları veri bütünlüğü ile dijital imza tasarıları için kullanılırlar. Açık anahtarlı bir algoritmayla hazırlanan dijital imza, gönderilen bilginin sayısal içeriğinin değiştirilmediğinin ve gönderen tarafın kimliğinin ispatı için atılır. Teknik olarak dijital imza, imzalanmış belgenin özünü, özetini (hash) içeren, elektronik mesaja eklenmiş bilgidir. İçerikte yapılacak bir değişiklik hash' ı geçersiz kılacaktır.

Başka bir ifadeyle hash fonksiyonu gönderilecek mesajdan matematiksel yollarla sabit uzunlukta sayısal bilgi üretme işlemidir. Üretilen sayısal bilgi "mesaj özeti" olarak bilinir. Mesaj özeti anlamsız bir bilgidir. Hash fonksiyonu geri dönüşümü olmayan bir fonksiyondur; yani mesaj özetine bakarak mesajın kendisini elde etmek mümkün değildir. Aynı özeti veren iki farklı mesaj bulmak da imkânsız olmalıdır. Her mesajın farklı özetinin olması, mesajda yapılacak en ufak bir değişiklikte imzanın geçersiz kalmasını sağlayacaktır. Kriptografinin böyle fonksiyonlara ihtiyacı vardır. Çünkü bu fonksiyonların ana özellikleri tersinin hesaplanmasının güç olmasıdır (Soyalıç, 2005).

Ayrıca, kullanıcı yetkileri sunucu üzerinde kayıt edilirken kullanılmaktadır. Kullanıcı, programa önceden kayıt edilmemişse uygulamayı kullanamamaktadır. Bu kayıt girişinde kullanıcı, bir şifre girer. Bu şifre doğrudan veri tabanına kaydedilmez. Bu şifre, hash fonksiyonları ile geri dönüşümü olmayan başka bir veri haline dönüştürülerek veri tabanına kaydedilir. Bu yöntemle veri tabanına erişen kötü niyetli kişilerin bu şifreleri ele geçirmeleri zorlaştırılmış olur (Dülgerler ve Sarısakal, 2003).

Bir mesaj ilk olarak özetlenir ve sonra hash değeri mesajın bir temsilcisi gibi orijinal mesaj yerine imzalanır. Örneğin bir mesajının orijinal mesaj ile aynı olup olmadığına

bakılırken hash değeri hesaplanır ve korunan orijinal hash değeri ile kıyaslanır. Değerler eşitse girdilerinde eşit olduğu kabul edilir. Bu durumda mesaj değiştirilmemiş demektir (Şekil 3-10).

Şekil 3-10 Hash Fonksiyonun Sayısal İmza olarak kullanılması

5070 sayılı Elektronik İmza Kanunu'nda yer alan şekliyle elektronik imza; başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veriyi tanımlar.

Elektronik İmza Kanunu'nda; güvenli elektronik imza, elle atılan imzaya eşdeğer kabul edilmiş ve elektronik imza ile oluşturulmuş verilerin senet hükmünde olacağı belirtilmiştir.

Hash Fonksiyonunun Özellikleri;

- *Ön Görüntü Direnci*

x, x' girdi; y, y' çıktı ve h hash fonksiyonu olmak üzere; önceden belirtilmiş bütün çıktılar için hash değeri bu çıktı olan herhangi bir x girdisi hesaplanabilir olmamalıdır. Yani;

karşılık geldiği girdi bilinmeyen herhangi bir y verildiğinde h(x')=y olacak şekilde herhangi bir x' ön görüntüsü bulmak kolay olmamalıdır.

- *İkinci Ön Görüntü Direnci*

Belirlenen herhangi bir girdi ile aynı çıktıya sahip ikinci bir girdinin bulunması hesaplanabilir olmamalıdır. Yani bir x verildiğinde h(x)=h(x1) olacak şekilde x ≠x1 olmak üzere ikinci bir x1 ön görüntüsü bulmak kolay olmamalıdır.

- *Çakışma Direnci*

Aynı çıktıya sahip farklı iki x, x' girdileri bulmak kolay hesaplanabilir olmamalıdır. Yani girdilerin seçimi serbest olmak üzere h(x)=h(x') olacak şekilde herhangi iki x, x' girdisi bulmak kolay olmamalıdır (Soyalıç, 2005).

Hash Fonksiyonu Türleri

- *Tek Yol Hash Fonksiyonu (TYHF)*

Bir hash fonksiyonu ön görüntü ve ikinci ön görüntü özelliklerini sağlarsa bu fonksiyona tek yol hash fonksiyonu denir. Yani;

i. Keyfi sonlu boyutlu x girdisini n sabit uzunluğundaki h(x) çıktısına dönüştürür.
ii. Bir x girdisi verildiğinde h(x) i hesaplamak kolaydır.
iii. h(x)=y olacak şekildeki x i bulmak kolay olmamalıdır. (Ön Görüntü Direnci)
iv. Bir x girdisi verildiğinde h(x) =h(y) özelliğini sağlayan y bulmak kolay olmamalıdır. (İkinci Ön Görüntü Direnci)

- *Çakışma Dirençli Hash Fonksiyonu (ÇDHF)*

İkinci ön görüntü direnci ve çakışma direnci özelliklerini sağlayan hash fonksiyonlarıdır.

Alışılmış Hash Fonksiyonları

Alışılmış hash fonksiyonları özetlemenin açık amaçları için özel olarak düzenlenmiştir. Bu fonksiyonlar mesaj özet ailesinden yararlanılarak oluşturulurlar. Uygulamada çok iyi ilgi

alan bu fonksiyonlar MD-4 hash fonksiyonuna dayanırlar. MD-4, 32-bitlik makinelerin bilgisayar yazılım uygulamalarına özgü olarak tasarlanmıştır.

- *MD (Mesaj-Özeti Algoritması)-2*

1989 yılında tanımı verilen mesaj özet algoritması 128-bitlik blok boyutuna sahiptir. Algoritma kırılmış olup, yeni uygulamalar için kullanılmamaktadır. Mesaj özeti 128 □bit uzunluğundadır. (B.Kaliski, 1992)

- *MD-4*

1990 yılında Ron Rivest tarafından geliştirilmiştir. MD-4, 128 □bitlik bir hash değeri üretir. Mesaj 512-bitlik bloklarda tekrarlı yapı içinde ve her blok üç farklı döngüde işlemden geçirilir. Aynı hash değerine sahip iki mesaj bulmak yaklaşık 2^{64} uygulama gerektirirken; önceden belirlenmiş bir hash değerini sağlayan bir mesaj bulmak yaklaşık 2^{128}uygulama gerektirir (Rivest, 1990)

MD-4 için sıkıştırma fonksiyonu uygulamasında çakışmalar bulunmuştur. Bu sebeple MD-4 ün çakışma dirençli hash fonksiyonu olarak kullanımı tavsiye edilmez (Soyalıç, 2005).

- *MD-5*

MD-5, Ron Rivest tarafından 1991'de geliştirilmiştir. MD-4 ün güçlendirilmiş versiyonu gibi düzenlenmiştir. Mesaj 512-bitlik bloklarda 16x32 bitlik alt bloklar halinde işlemden geçirilir. Algoritma dört farklı döngüden oluşur. Çıktı 4 tane 32-bitlik blok olup 128- bitlik hash değeri verir (Rivest, 1991).

- *SHA (Güvenli Hash Algoritması)-0*

1993 yılında NIST tarafından FIPS PUB 180 standartlarına göre yapılan ilk sürüm bugün SHA-0 olarak adlandırılmaktadır. Bu sürüm 1995 yılında yerini FIPS PUB 180-1 standartlarına uygun olarak yeniden geliştirilen SHA-1 algoritmasına bıraktı. SHA-0 algoritması SHA-2 algoritmasının aksine SHA-1 algoritmasıyla büyük benzerlikler taşır. SHA-1 algoritmasının farkı mesajın sıkıştırma fonksiyonuna bit bit dönüşümünün

yapılmasıdır. Böylelikle SHA-0 algoritmasındaki güvenlik açığının kapatılabileceği düşünülmüş, ancak bu çalışmalar yeterli olmamıştır.

- *SHA -1*

1995 yılında SHA-1 algoritması geliştirilmiştir. SHA-1 bir mesaj özet algoritması ve bir kriptografik hash fonksiyonu olup NSA (Birleşmiş Milletler Ulusal Güvenlik Ajansı) tarafından düzenlenip, NIST (Ulusal Standartlar Enstitüsü Teknolojisi) tarafından yayımlanmıştır. Algoritmanın orijinal tanımlaması Güvenli Hash Standardı olarak 1995'de yayımlandı (Secure Hash Standard, 1995).

- *SHA-2*

SHA-1 algoritmasının verdiği kırılma tedirginliği ile SHA-2 algoritmaları geliştirilmiştir. SHA-2 algoritmaları 2001 yılında FIPS PUB 180-2 standartlarına uygun olarak tasarlanmışlardır. SHA özet fonksiyon kapsamında veri özeti uzunluğu daha uzun olan ve aralarında ufak farklar içeren ve SHA-2 ailesi olarak adlandırılan dört farklı algoritma (SHA-224, SHA-256, SHA-384 ve SHA-512) bulunur. SHA-256, SHA-384, ve SHA-512 algoritmaları 2001 yılında, SHA-224 algoritması ise 2004 yılında geliştirilmiştir. SHA-224 algoritması anahtar uzunluklarını eşleştirilmesiyle Triple DES standartlarına da uyum sağlamıştır. SHA- 2 versiyonu US 6829355 patentine de sahiptir. SHA-0 ve SHA-1 için geliştirilmiş ataklar SHA-2 versiyonları için herhangi bir zayıflık belirtmemiştir. Ancak SHA-2 algoritmasının yapısı SHA-1'e benzediğinden bu algoritmaların da yakın zamanda kırılma ihtimallerine karşı araştırmacılar yeni bir algoritma tasarlamaya karar vermişlerdir ve SHA-3 algoritması gündeme gelmiştir.

Ülkemizde kullanılan elektronik imzalar 30.01.2013 tarihine kadar SHA-1 alogritmasına göre şifrelenmekteydi. Bilgi Teknolojileri İletişim Kurumu tarafından 30.01.2013 tarihli, 28544 sayılı "ELEKTRONİK İMZA İLE İLGİLİ SÜREÇLERE VE TEKNİK KRİTERLERE İLİŞKİN TEBLİĞDE DEĞİŞİKLİK YAPILMASINA DAİR TEBLİĞ" de

SHA-2 algoritmasının kullanılması tüm kamu kurum ve kuruluşlarına bildirilmiştir (Resmi Gazete, 30.01.2013).

- *SHA-3*

SHA-1 algoritmasındaki güvenlik açıklarından sonra, temeli aynı olduğu için, SHA-2 algoritmasının da güvenlik sorunu olacağını düşünen ABD Ulusal Standartlar ve Teknolojiler Enstitüsü (NIST), 2007 Kasım'ında yayımladığı genelge ile yeni bir özet fonksiyonu için uluslar arası bir yarışma açtığını duyurmuştur. Bu genelgede SHA-0, MD4 ve MD5 algoritmalarının çakışma nedeniyle artık güvenli olmadığını ve o gün itibarıyla SHA-1 algoritmasında henüz bir çakışma olmadığını ancak olabileceğini öngördüklerini belirttiler. Nitekim, günümüzde SHA-1 algoritmasında çakışma sayısı güvenli denecek sayıların altına kadar gerilemiştir. Bu gelişmeler çerçevesinde SHA-3 için bu yarışma düzenlenmiştir.

Dijital İmzanın Faydaları

- Güvenilir kimliklendirme ve onay mekanizmasıyla güvenli olarak elektronik ortamlarda işlemlerin yapılabilmesine katkılar sağlayacaktır.
- İş ve işlemler hızlıca yapılabilecektir. (Çeşitli protokoller ortadan kalkacak ve sonuç odaklı işlemler internet üzerinden hızlıca gerçekleştirilecektir)
- İş maliyetleri düşecek, verimlilik artacaktır. (e-imza ile birlikte noter, kırtasiye, yol vb. giderler neredeyse yok denecek kadar azalacaktır.)
- İş takipleri kolaylaşabilecektir. (yapılan işlemleri elektronik ortamda an be an izleyebilmek ve işlemin hangi düzeyde olduğunu görebilmek mümkün olacaktır)
- Elektronik ortamlarda meydana gelebilecek güvenlik zafiyetleri ve açıklar ortadan kaldırılabilecektir.
- Elektronik ortamlara güven artacak dolayısıyla elektronik ortamlarda yapılabilecek iş ve işlemlerde artışlar meydana gelecektir.
- E-ticaret hacimleri artacaktır *(E-imza, 2013)*.

3.4 Sözde Rastsal Sayılar ve İstatistik

Rastgelelik

Rastgele üretilen sayılar, istatistiksel örneklemelerde, şans oyunlarında ve benzetim uygulamalarında sıkça kullanılır. Benzetim uygulamalarından Monte Carlo Benzetimi deney girdileri belirli olmayan, kesin olmayan rastsal bir şekilde gelmesi bekleniyorsa ve dağılım bir fonksiyonla hesaplanabilecekse kullanılır. Monte Carlo, rastgele sayıları temel alarak tahmini sistemleri modeller. Hücre Simülasyonu, Borsa Modelleri, Dağılım Fonksiyonları, Sayısal Analiz, Doğal olayların simülasyonu, Atom ve Molekül Fiziği, Nükleer Fizik ve Yüksek Enerji Fiziği modellerini test eden simülasyonlar, deneylerde kullanılan aletlerin simülasyonu örneğin bir madde içerisinde x ışınlarının dağılımı (Mooney, 1997)

Bir rastgele bit sırası tarafları “0” ve “1” olarak etiketlenmiş bir hilesiz bozuk paranın yazı/tura sonuçları gibi yorumlanabilir. Her bir yazı/tura atışı bir “0” veya “1” üretiminin tam olarak ½ olasılığına sahiptir. Bundan başka, yazı/tura atışlarının her biri diğerlerinden bağımsızdır: herhangi bir yazı/tura atışının kendinden önce gelen sonucu, sonraki yazı/tura atışlarını etkilemez. Hilesiz para böylece mükemmel rastgele bir akış üreteci olur. Çünkü “0” ve “1” değerleri rastgele olarak dağıtılmış olacaktır. Sıranın tüm öğeleri diğerlerinden bağımsız olarak üretilir ve sıradaki bir sonraki öğenin değeri önceden tahmin edilemez, kaç eleman olduğuna da bakılmaksızın üretilmektedir. Gerçek bir rastgele sıranın idealleştirilmiş bir üretecinin kuramsal çıkışı, rastgele ve sözde rastgele sayı üreteçlerinin tespiti için bir kriter vazifesi görür.

3.4.1 Kriptolojide Rastgelelik

Rastgele sayı üreteçleri anahtarın üretim işlemlerinin güçlendirilmesi maksadıyla kriptoloji çalışmalarında kullanılmaktadır. Bilgi güvenliğinin sağlanması için, kriptoloji uygulamalarında kullanılan rastsal sayı üreteçleri, farklı uygulama alanlarına nazaran çok daha güçlü ve tahmin edilebilmesi zor olmalıdır. Üreteçlerin ürettiği sayıların belirli bir sayı dizisine dayandırılmaması veya çok uzun sayı dizilerine dayandırılması gerekmektedir.

Rastgeleliğin en önemli özelliği, sonuçların ortaya çıkmasından tamamen şans olayının rol oynaması ve gerekliliği öngörülerin ve tahminlerin kesin bir doğrulukla önceden yapılamamasıdır.

Sözde Rastsal Sayı Üreteçleri

Sözde Rastsal Sayı Üreteçlerinin (SRSÜ) çıktıları gerçek anlamda rastsal değildir, bu tür algoritmalar gerçek rastsal sayı dizilerinin bazı özelliklerini yaklaşık olarak taşır. John Von Neumann' ın da belirttiği gibi "Aritmetik yöntemlerle rastsal sayılar üretmeye çalışan biri büyük günah işliyordur." (Neumann, 1951). Her ne kadar rastsal sayılar donanımsal rastsal sayı üreteçleri ile üretiliyor olsa da, sözde rastsal sayılar modern bilgi işlemenin önemli bir bölümünü kapsamaktadır ve bunlar kriptolojiden tutun fiziksel sistemleri benzetimine yarayan Monte Carlo (Mooney, 1997) yöntemlerine dek pek çok yerde kullanılmaktadır. Oak Ridge National Laboratory' den Robert R. Coveyou' nun "Rastsal sayıların üretimi rastgele gerçekleştirilemeyecek kadar önemlidir" (Coveyou, 1998) cümlesinde belirttiği gibi üretilmiş olan sayıların rastsallığı ciddi ve dikkatli bir matematik analiz gerektirmektedir.

Sözde rastsal sayı üreteçleri deterministik bir bilgisayarda çalıştıkları için deterministik algoritmalardır ve bu tür bir algoritma ile üretilen sayı dizisinin gerçek bir rastsal dizide olmayan periyodiklik özelliği olacaktır. Eğer üreteç sabit miktarda hafıza kullanıyorsa yeterli sayıda döngü adımından sonra aynı içsel duruma ikinci kez gelecektir ve ondan sonra da sonsuza dek tekrar edecektir. Periyodik olmayan bir üreteç tasarlanabilir ancak bu tür bir sistemin ihtiyaç duyduğu hafıza miktarı sistem çalıştıkça büyüyecektir. Buna ek olarak bir sözde rastsal sayı üreteci keyfi bir başlama noktasından, ya da çekirdek durumundan, başlatılabilir ve o andan itibaren özdeş bir sayı dizisi üretir. Periyodikliğin pratik önemi sınırlıdır. Eklenen her bir hafıza biti ile maksimum periyot iki katına çıkar. Herhangi bir bilgisayarın evrenin beklenen yaşam süresi boyunca hesaplayamayacağı kadar uzun periyoda sahip sözde rastsal sayı üreteçleri inşa etmek mümkündür. Şifre bilimdeki cevaplanmamış sorulardan biri de iyi tasarlanmış bir sözde rastsal sayı üretecinin çıktısını, çekirdeğini (başlangıç parametrelerini) bilmeden, gerçek rastsal gürültüden ayırt etmenin

mümkün olup olmayacağıdır. Şifre bilimdeki pek çok uygulama uygun bir sözde rastsal sayı üretecinin çıktısının gürültüden ayırt edilmeyeceği varsayımına dayanır. En basit örneği akış şifresidir. Bu algoritma gizli bir mesajı, rastsal sayı üretecinin çıktısı ile şifreleme işlemine tabi tutar. Bu tür rastsal sayı üreteçlerinin tasarımı bir hayli zordur ve çoğu program çok daha basit üreteçler kullanır.

Sözde rastsal sayı üretecin geliştirilmesinin uzun tarihsel süreci vardır. Vernam (1971) rastsal olarak sıralanan sayı dizisi ile tek zamanlı şifrelemeyi bulmuştur. SRSÜ kullanılarak tasarlanan kripto sistemlerinin güvenlilik ölçüsü, SRSÜ' nün gerçek rastsal sıralı sayı dizisinden ayırt edilemeyeceği varsayımına dayanmaktadır. SRSÜ kripto uygulamalarının güvenilirliğinde hayati önem taşımaktadır.

Bu çalışmada Modified subtract with borrow generator (Marsaglia ve Zaman, 1993) algoritması ile sözde rastsal sayılar ileriki bölümlerde kullanmak amacıyla üretilmiştir.

İstatistiksel Testler

Rastgele sayı üreteçlerini test etmek için istatistiksel testler kullanılır. İstatistiksel çıkarım yapmak için istatistiksel hipotez testleri kullanılır. Bu testlerde bir hipotez (yokluk hipotezi, H0) öne sürülür, bu hipotezin tersi de alternatif hipotez, Ha olarak kabul edilir. İstatistiksel test sonucunda varılabilecek iki farklı temel karar vardır: - H0' ı reddet. - H0' ı reddetme. Birinci karar, H0 aleyhine güçlü bir kanıt elde edildiğinde verilir. Bu güçlü kanıt bulunamadığında ise ikinci karar verilir. Bütün istatistiksel testlerde kaçınılmaz hata yapma payı vardır. Test sonucunda iki farklı hata, birinci tip (alfa) ve ikinci tip (beta) yapılabilir. Birinci tip hata hipotezimiz doğruyken, kararımız H0'ı reddetmek olarak gerçekleşir. İkinci tip hata ise hipotezimiz yanlışken, kararımız H0'ı reddetme olduğunda gerçekleşir. Hipotez testinde birinci tip hata yapma olasılığını sınırlamak gerekir. Test sonucunda birinci tip hata yapma olasılığımız, testimizin anlam seviyesini verir. Bu değer genellikle 0.01- 0.05 olarak seçilir. İstatistiksel bir testin gücü, ikinci tip hatayı yapmama olasılığına eşittir. Testin gücü daha çok örneklem ile artırılabilir (Rukhin ve ark., 2010).

3.4.2 Ulusal Teknoloji Standartları Enstitüsü (National Institute of Standard Technology, NIST) Rastsallık Testleri

İstatistiksel bir test yapılacağında ilk olarak, H0 ve Ha belirlenir. Daha sonra testin anlam seviyesine karar verilir. Kitleden alınan rastgele örneklemden test istatistiğinin değeri ve teste ilişkin ret bölgesinin olasılığı olan p-değeri elde edilir. p değeri, birinci tip hata yapma olasılığını kontrol etmek yerine, H0'ın doğru olduğu varsayımı altında test istatistiğinin değeri veya daha uç bir değer olması olasılığına karşılık gelir. Bu tanıma uygun olarak hesaplanan olasılık p-değerini verir. Eğer bu değer seçilen anlamlılık değerinden küçükse H0 hipotezi reddedilir.

Bir sayı dizisi eğer rastsallık testlerini başarı ile geçiyorsa, sayı dizisinde bir sonraki rakamın ne olacağını hesaplamanın imkânsız olduğu değerlendirilmektedir. Üretilen sayıları bu şekilde olan üreteç, SRSÜ olma şartını sağlıyor demektir ve kripto sisteminde kullanılması doğru bir karardır.

Rastsal sayı üreteçlerinin geçerliliğini ölçmek maksadıyla DIEHARD (Marsaglia, 1995) test paketi, ENT Test paketi (Walker, 1998), NIST Test Paketi(Rukhin ve ark., 2010) gibi birçok rastsallık test paketi kullanılmaktadır. Bu çalışmada; içlerinden en popüleri olan ve birçok çalışmada tercih edilen(Sulak, 2011; Yayik ve Kutlu, 2013; Fidan ve Gerek, 2008) NIST Test paketi kullanılmıştır. NIST paket programı LİNUX ortamında derlenmiş C kodları kullanılarak yapılmıştır.

- *Frekans Testi*

Testin faaliyet merkezi, parçalanmamış sıra (Kriptolojide devamlı olarak kullanılan sembollerin (harfler, rakamlar v.s.) sıralanmış terkibidir) (Sulak, 2011). Bu testin amacı, bir sırada bulunan sıfır ve birlerin miktarının tamamen rastgele bir sıra için beklenen ile yaklaşık olarak aynı olup olmadığının belirlenmesidir.

- *Blok İçinde Frekans Testi*

Testin faaliyet merkezi, M-bit bloklarda birlerin en uzun tekrar sayısıdır. M-bitlik bloklarda bulunan en uzun birler grubu üzerinde odaklaşır. Bu testin amacı, test edilen sıradaki birlerin en uzun tekrar sayısı ile rastgele bir sıradaki birlerin beklenen en uzun tekrar sayısının uyumlu olup olmadığını belirlemektir (Sulak, 2011). Testin faaliyet merkezi, M-bit blokları içindeki birlerin oranıdır. Verilen bir sırada bulunan 0 ve 1'lerin oranını M bitlik bloklar içinde kontrol eder. Her bir bloktaki 1'lerin beklenen oranı M/2'dir. Bu testin amacı, bir M-bit bloktaki birlerin frekansının bir rastgelelik varsayımı altında beklenen gibi yaklaşık olarak M/2 olup olmadığının belirlenmesidir. Blok uzunluğu M=1 olarak alındığında blok frekans testi, frekans testine dönüşür.

- *Runs Testi*

Bu testin amacı; farklı uzunluklardaki 0 ve 1'lerin tekrarının rastgele bir dizi için beklendiği gibi olup olmadığının belirlenmesidir. Özellikle, bu test 0 ve 1'ler arasındaki değişimin çok hızlı veya çok yavaş olup olmadığını belirler (Sulak, 2011).

Blok Frekans Testi: Testin faaliyet merkezi, M-bit blokları içindeki birlerin oranıdır. Verilen bir sırada bulunan 0 ve 1'lerin oranını M bitlik bloklar içinde kontrol eder. Her bir bloktaki 1'lerin beklenen oranı M/2'dir. Bu testin amacı, bir M-bit bloktaki birlerin frekansının bir rastgelelik varsayımı altında beklenen gibi yaklaşık olarak M/2 olup olmadığının belirlenmesidir. Blok uzunluğu M=1 olarak alındığında blok frekans testi, frekans testine dönüşür (Sulak, 2011).

- *Bloktaki En Uzun Runs Testi*

Testin faaliyet merkezi, M-bit bloklarda birlerin en uzun tekrar sayısıdır. M bitlik bloklarda bulunan en uzun birler grubu üzerinde odaklaşır. Bu testin amacı, test edilen sıradaki birlerin en uzun tekrar sayısı ile rastgele bir sıradaki birlerin beklenen en uzun tekrar sayısının uyumlu olup olmadığını belirlemektir. Sıra M-bitlik n tane bloğa bölünür ve her blok içerisindeki en uzun birler grubunun uzunluğuna bakılır. Bu değerlerin frekansları beklenen değerlerle kıyaslanır ve ciddi bir sapma olup olmadığı kontrol edilir. Birlerin

beklenen en uzun tekrar sayılarında bir düzensizlik olması, sıfırların beklenen en uzun tekrar sayılarında da bir düzensizlik olduğu anlamına gelir. Bu nedenle, birlerin testi zorunludur.

- *Kümülâtif Toplamlar Testi*

Bu testin amacı; dizinin değişik parçalarının kümülâtif toplamın beklenen değerlere göre ne kadar farklılık gösterdiğinin belirlenmesidir. Kümülâtif toplamlar da rastsal bir ilişki içerisinde olabilirler. Bu test sonucunda dizinin rastsal kabul edilebilmesi için kümülâtif toplamının 0 (sıfır) ' a yakın olması gerekmektedir (Sulak, 2011).

- *Ayrık Fourier Testi*

Bu testin faaliyet merkezi sıranın Ayrık Fourier Dönüşümündeki tepe noktalarıdır. Bu testin amacı rastgelelik varsayımından bir sapma gösteren, test edilen sıradaki periyodik özellikleri (yani, birbirine yakın olan tekrarlı kalıpları)tespit etmektir. Bu amaç, %95 barajını önemli ölçüde %5 den farklı olarak aşan tepelerin sayısını tespit etmek içindir.

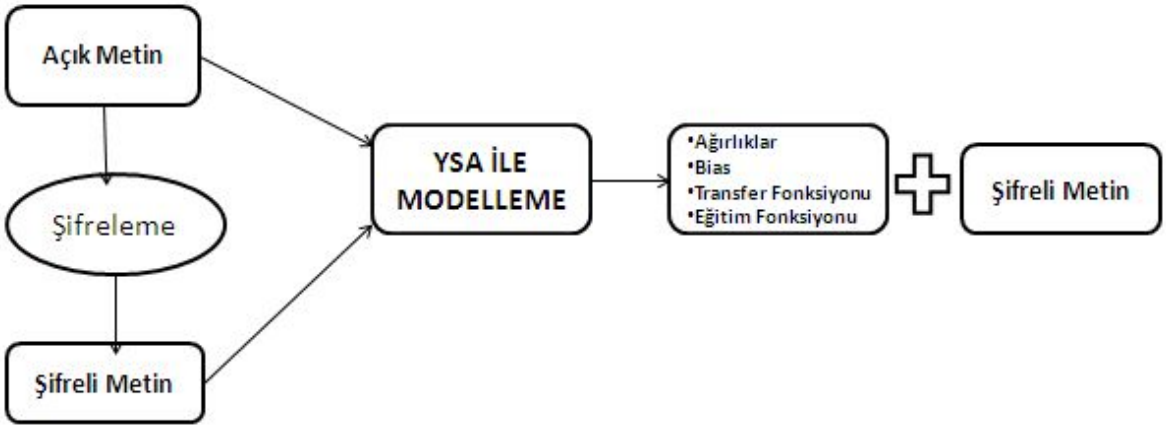
Burada açıklanan test ayrık fourier dönüşümüne dayanır. Bu, spektral metotları olarak bilinen prosedürler sınıfının bir üyesidir. Fourier Testi rastgelelik varsayımından gelen sapmayı belirleyecek bit serilerindeki periyodik özellikleri denetler.

- *Rank Testi*

Testin faaliyet merkezi, parçalanmamış sıranın alt matrislerinin sıralı ranklarıdır. Bu testin amacı, orijinal sıranın alt sıralarının sabit uzunlukları arasındaki lineer bağımlılığını kontrol etmektir. Test içerisinde sıra MxM-bitlik matrisler halinde parçalanır ve oluşturulan her bir matrisin rankı hesaplanır. Sıradan oluşturulan matrislerin ranklarının frekansları hesaplanır, beklenen frekansla kıyaslanır ve ciddi bir sapma olup olmadığı kontrol edilir.

4 ARAŞTIRMA BULGULARI VE TARTIŞMA

Yapılan açık anahtarlama altyapılı kripto sistem uygulamasında; yapay sinir ağı ile üretilen sözde rastsal sayılar *şifreleme anahtarı (açık anahtar)*olarak doğrusal olmayan şifrelemede kullanılmıştır. Yapay Sinir ağı ile elde edilen şifreli metin ile açık metnin modellemesi yapılmış ve modellemede kullanılan yapay sinir ağı yapısı ve tüm parametreleri *şifre çözme anahtarı (özel anahtar)* olarak şifreli metnin içerisine gömülerek alıcıya gönderilmiştir (Şekil 4-1). Alıcı şifre çözme anahtarını kullanarak yapay sinir ağı modelini tasarlamış ve açık metni elde etmiştir.



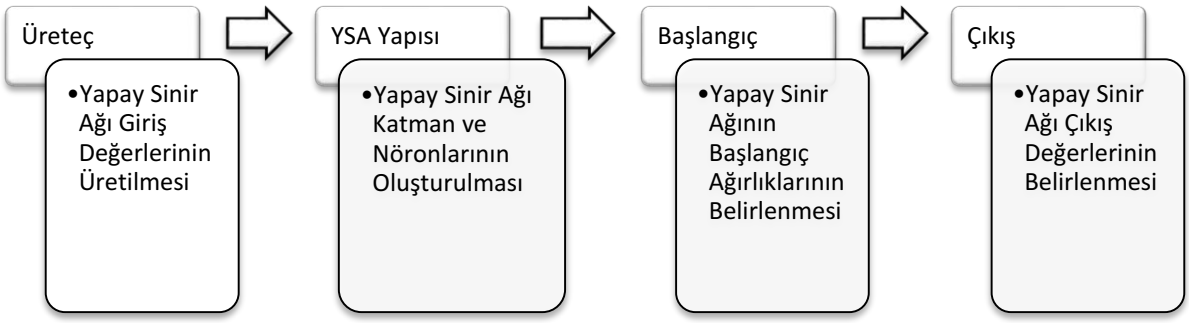
Şekil 4-1 Yapay Sinir Ağı tabanlı Açık Anahtarlama Altyapılı Kripto Sistem

Yukarıda anlatılan açık anahtarlama sistemi aşağıdaki maddelerde ayrıntılı olarak açıklanmıştır.

4.1 Yapay Sinir Ağı Tabanlı Sözde Rastsal Sayı Üreteçleri

Yapay sinir ağları karmaşık yapıları itibariyle kriptolojide anahtar üretiminde kullanılmaktadır. Aşırı öğrenme (ezberleme) sonucunda girdisinden bağımsız olarak çok farklı çıkışlar elde edebilen Çok Katmanlı Yapay Sinir Ağları bir rastsal sayı üreteciymiş gibi değerlendirilerek kriptolojide anahtar dağıtımı konusunda yeni fikirlerin ortaya çıkmasına sebep olmuştur (Karras ve Zorkadis, 2003). Bu çalışmada çok katmanlı yapay sinir ağlarının özelliklerinden esinlenerek YSA tabanlı bir Sözde Rastsal Sayı Üreteci

tasarlanmıştır (Şekil 4-2). Kullanılan YSA' nın girdisi olarak uzun periyodu olan ve bir önceki bölümde anlatılan Modified Subtract with Barrow üreteci (Marsaglia ve Zaman, 1993) ile üretilen ikilik sayı sistemindeki sayılar kullanılmıştır. YSA' nın başlangıç ağırlıkları olarak ise Yapay Sinir Ağı tabanlı sözde rastsal sayılar rastsal değerler olarak kullanılmıştır. Başlangıç ağırlıkları her defasında rastsal olarak değişen Aktivasyon Fonksiyonları ile işleme sokularak çıktı değerleri hesaplanmıştır. Bu çıktılara YSA tabanlı rastsal sayılar denilmektedir.



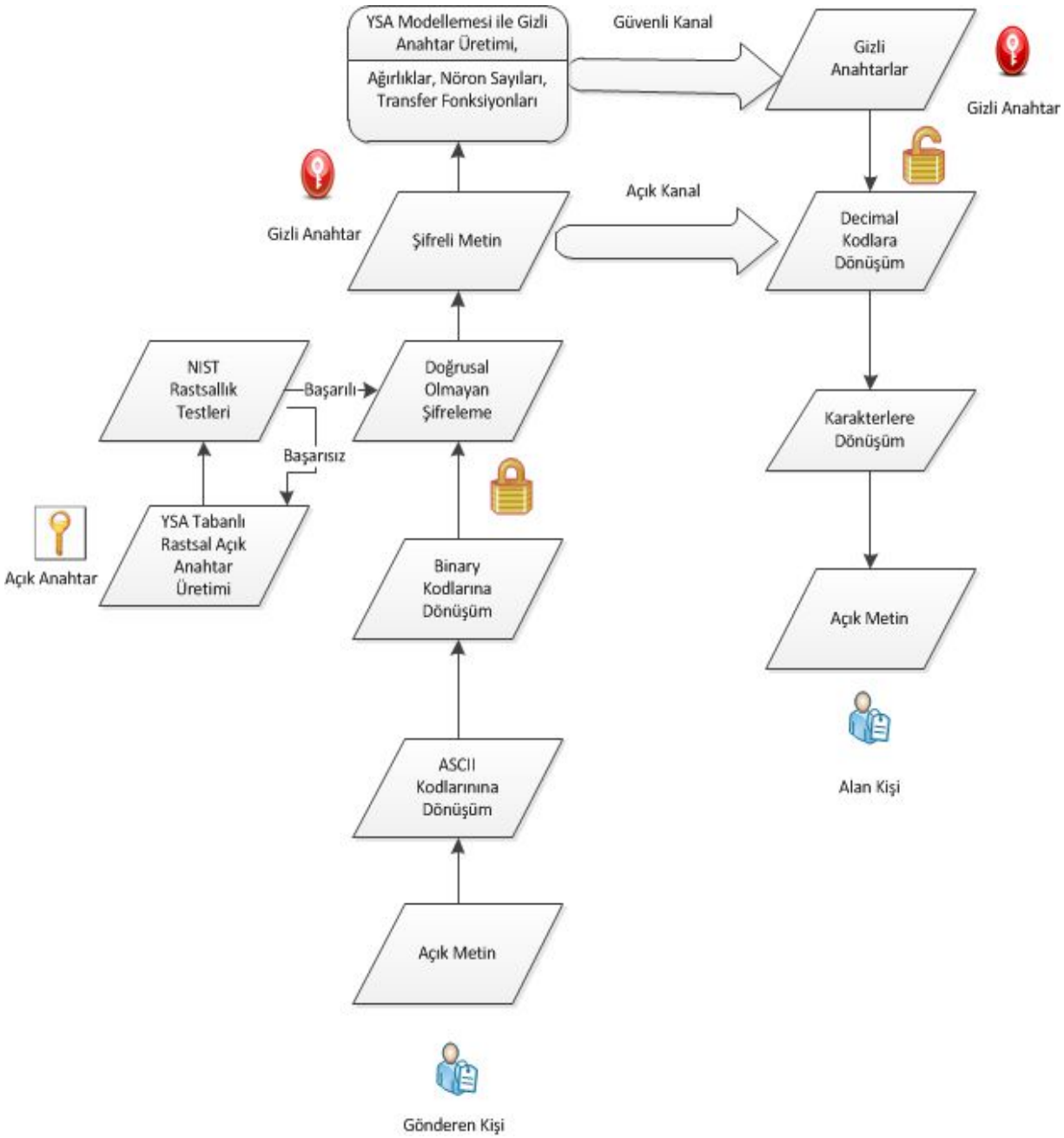
Şekil 4-2 Yapay Sinir Ağı Tabanlı Rastsal Sayı Üretimi

4.2 Yapay Sinir Ağı Tabalı Kriptoloji

Herhangi bir kurum tarafından bir kripto sistemin kullanılabilmesi için tüm veri formatlarını yüksek performansta ve güvenli olarak şifreleyebilmeli ve çözebilmelidir. Kurum içerisinde kullanılan tüm şifrelerin güvenli olarak veri tabanında tek yönlü şifrelenmiş (hash) olarak muhafaza edilebilmesi gerekmektedir. Elektronik ortamda yapılan tüm işlemler sayısal imza altına alınarak reddedilemez seviyede olmalıdır. Bu sebeple yapay sinir ağı tabanlı şifreleme uygulamasında; metin şifrelemesi, güvenli dosya uygulaması, resim şifrelemesi ve tek yönlü hash fonksiyonu uygulamaları yapılmıştır.

4.2.1 Metin Şifreleme

Tasarlanan kripto sistemin akış diyagramı Şekil 4-3'de gösterildiği gibidir. Açık metnin sistem tarafından alınarak geçirildiği işlemler madde madde açıklanmıştır.

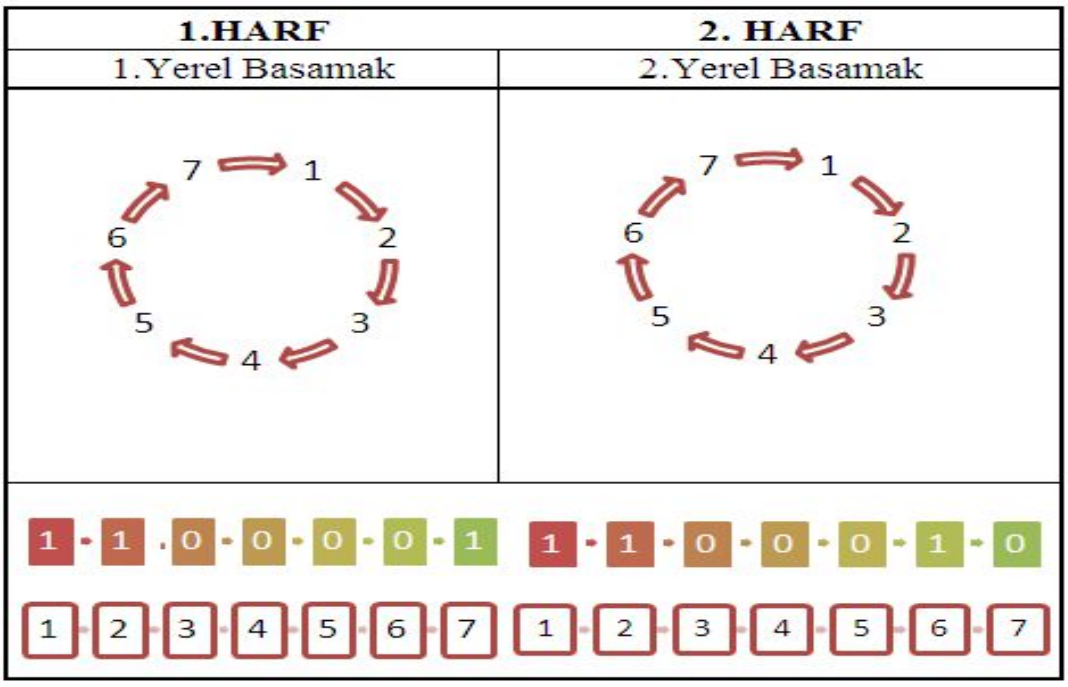


Şekil 4-3 Yapay Sinir Ağı Tabanlı Kripto Sistemin Aşamaları

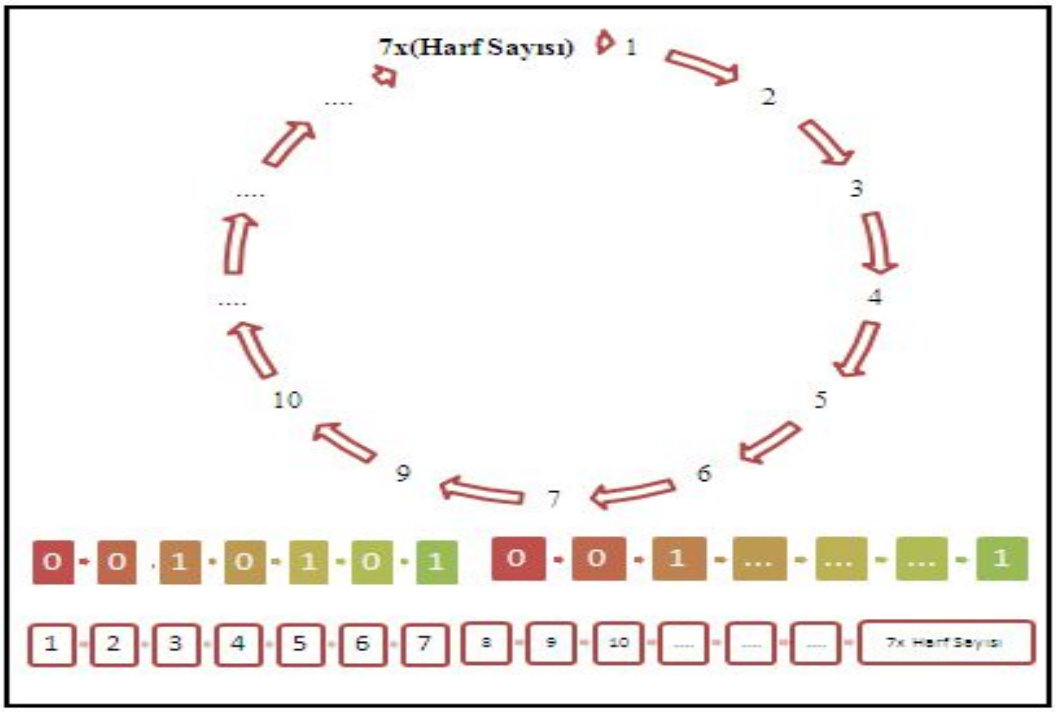
YSA tabanlı şifreleme anahtarı üretme ve Doğrusal Olmayan Yapı ile Şifreleme

Kripto algoritmalarında rastsallığın arttırılması güvenirliliği de beraberinde arttırarak sistemi kullanılabilir hale getirmektedir. Şifreli metnin rastsal yöntemlere dayanan verilerle her bir 7 bitini kendi içinde ve tamamını bir arada karıştırılması şüphesiz ki şifrelenme gücünü arttıracak ve bir kripto analistin müdahalesinde başarılı olmasını sağlayacaktır. Bahsedilen işlemlerin teknik olarak yapılışı sırasıyla aşağıda belirtilmiştir.

Öncelikle; açık metnin her harfi ASCI kodlarına dönüştürülmüştür. Daha sonra bu ASCI kodlar 7 bitlik binary kodlara dönüştürülmüştür. Ardından bir harfi temsil eden 7 bitlik binary kodlar kendi arasında yerel olarak ( ) ve bütün harfleri temsil eden binary kodlar ayrıca kendi arasında genel olarak (**Hata! Başvuru kaynağı bulunamadı.**) karıştırılmıştır. basamak değerlerinin yerleri değiştirilmiştir.) Bu karıştırma işlemi ise önceki bölümlerde anlatılan yapay sinir ağları tabanlı rastsal sayı üreteçleri ile yapılmıştır.



Şekil 4-4 Yerel Karıştırma

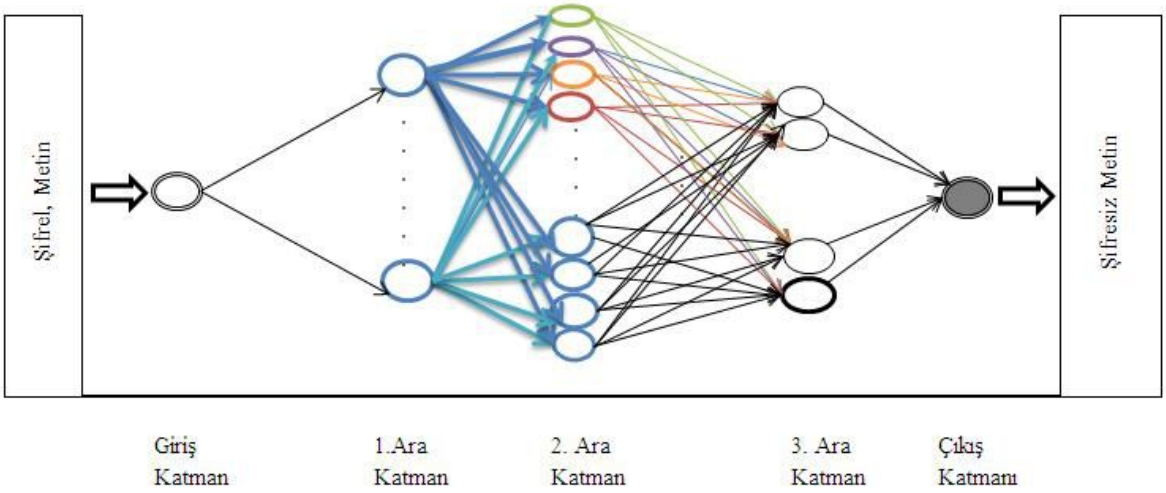


Şekil 4-5 Genel Karıştırma

. Başlangıç ağırlıkları kullanılarak elde edilen sayıları ise yapay sinir ağı tabanlı rastsal sayılardır. Dolayısıyla binary kodların basamaklarının yerleri güçlü bir şekilde karıştırılmış olmaktadır. Sonuçta elde edilen karıştırılmış binary kodlar şifreli metindir. Şifreleme işlemi herhangi bir doğrusal işleme dayanmadığından şifreleme algoritmasını tahmin etmek gayet zor, belki de imkânsızdır. Bu çalışmanın ilerleyen bölümlerinde şifreleme algoritması yapay sinir ağlarının öğrenme yeteneği kullanılarak belirlenmeye çalışılacaktır.

Yapay Sinir Ağı Modellemesi ile Şifre Çözme Anahtarı Üretilmesi

Alıcının tasarladığı yapay sinir ağı 4 adet nörona sahip giriş katmanı, Şekil 4-2' de belirtilen yapay sinir ağı tabanlı rastsal sayı üreteci ile üretilen rastsal değerlere sahip 3 adet ara katman ve 1 adet nörona sahip çıkış katmanı olmak üzere toplam 4 katmanlı olarak tasarlanmıştır.

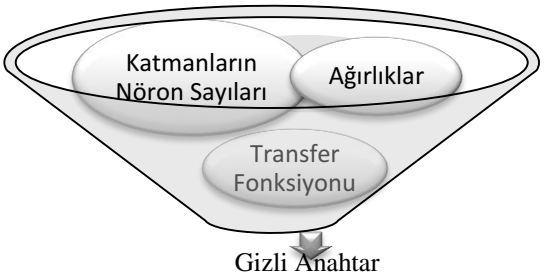


Şekil 4-6 Gönderenin Tasarladığı Yapay Sinir Ağı

Şekil 4-6' da gösterilen yapay sinir ağında giriş olarak, şifreli metin, istenilen hedef olarak ise açık metin kullanılmaktadır. Eğitim algoritması, Aktivasyon Fonksiyonu ve Ara Katmanların Nöron Sayıları Yapay Sinir Ağı Tabanlı Sözde Rastsal Sayı Üreteci ile her defasında değişecek şekilde tasarlanmıştır. Böylece rastsallık bir derece daha arttırılmıştır.

Alıcıya Yapay Sinir Ağı Topolojisinin Gönderilmesi

Yukarıda anlatılan uygulamalar şifreli bir metni herhangi bir kripto analistin saldırısına karşı güvenli iletişim sağlamak maksadıyla yapılmaktadır. Bunun için; giriş ağırlıkları, katmanların nöron sayıları, transfer fonksiyonları ve eğitim algoritması ve her defasında rastsal olarak belirlenen nöron sayıları bir veri içerisinde yalnızca alıcının anlayabileceği formatta karıştırılarak "gizli anahtar" (Şekil 4-7) olarak alıcıya güvenli bir kanaldan gönderilmektedir.



Şekil 4-7 YSA Tabanlı Gizli Anahtar

Ardından alıcı tarafında bu veriler kullanılarak önce ön işlemden geçirilir sonrasında yeni bir yapay sinir ağı tasarlamaktadır. Yeni network sayesinde şifreli metin çözülerek son işlemler gerçekleştirilir. Sırasıyla bütün harflerinin ASCI kodlarının binary haline ulaşır. Önce 7'lik binary değerleri ASCI kodlara, sonra ASCI kodları harflere dönüştürülmektedir. Harfler yan yana birleştirildiğinde alıcı açık metni elde etmiş olmaktadır.

Yukarıda anlatılan şifreleme ve şifre çözme algoritmaları kullanılarak

- *Çevirim içi yazışmalarda kullanılabilecek gerçek zamanlı metin şifreleme*
- *Güvenli dosya oluşturma*

Uygulamaları yapılmıştır.

4.2.2 Resim Şifreleme

Birçok geleneksel ya da modern kripto sistemler metin verilerini korumak için tasarlanmışlardır. Orijinal gizli açık metin, rastsal olarak anlamsız şifreli metne dönüştürülmektedir. Şifreli metin üretildiğinde ya saklanmakta ya da ağda iletilmektedir. Şifreli Metin alındığında deşifreleme algoritması kullanılarak orijinal haline dönüştürülmektedir.

Resimleri direk olarak şifrelemek için geleneksel kripto sistemlerini (RSA ve DES gibi) kullanabilmemize rağmen iki nedenden dolayı uygun değildir; birincisi resimlerin boyutları metinlere göre genellikle çok daha büyüktür. Bu nedenle geleneksel kripto sistemler resmi direk olarak şifrelemek için çok daha fazla zamana ihtiyaç duyarlar. İkincisi ise şifresi çözülen metnin orijinal metne eş olması zorunluluğudur. Ancak bu zorunluluk resim verisi için geçerli değildir. İnsan algısının karakteristiklerine göre resimdeki ufak bozulmalar genellikle kabul edilebilirdir.

Renkli resimler genellikle üç adet 2 boyutlu diziler olarak ifade edilirler. İki boyutlu dizileri kripto sistemleriyle koruyabilmek için öncelikle her boyutun bir diziye dönüştürülmesi gerekmektedir.

Resim şifrelemesini incelemek için öncelikle metin verisiyle resim verisinin arasındaki uygulama farklarını analiz etmemiz gerekir. Temel olarak resimle metin arasındaki farklar aşağıdaki gibidir,

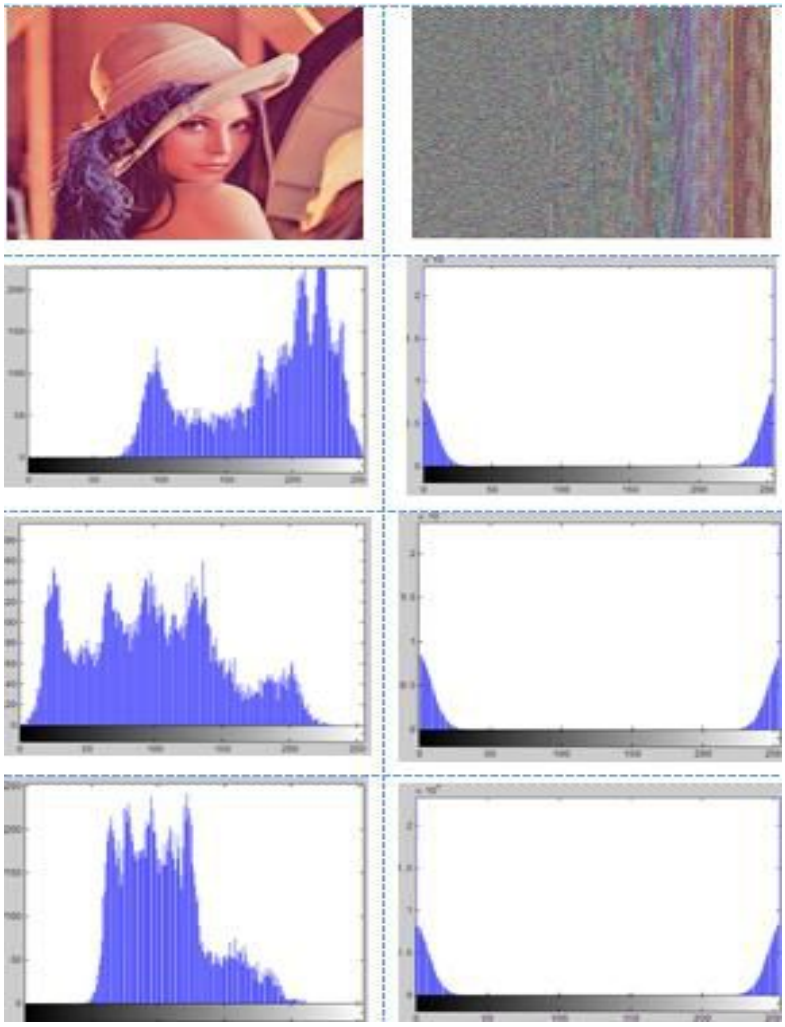
- Şifreli metin oluşturulduğunda, şifreli metin orijinal metine kayıpsız deşifre edilmelidir. Fakat şifreli resim orijinal resme çok az kayıpla deşifre edilebilir.
- Metin verisi kelime dizilerinden oluşur. Bu nedenle metin verisi direk olarak stream ya da block cipher' lerle şifrelenebilir. Ancak sayısal resim verileri genellikle iki boyutlu dizilerle ifade edilirler.

Sayısal İmza Kullanarak Resim Şifreleme Tekniği

Güvenli resim iletimi için yeni bir teknik önerilmektedir. Orijinal resmin sayısal imzası, orijinal resmin kodlanmış versiyonuna eklenmektedir. Resmin kodlanması BCH (Bose-Chaudhuri Hochquenghem) gibi uygun bir hata kontrol kodlaması yöntemiyle yapılmaktadır. Alıcı tarafında ise kod çözme işleminden sonra sayısal imza kullanılarak resmin doğruluğu onaylanabilir (Güvenoğlu, 2006).

Bu çalışmada metin şifreleme bölümünde anlatılan YSA tabanlı şifreleme işlemleri her boyutu dizilere dönüştürülen renkli resmi şifrelemek için kullanılmıştır. 128x128 boyutundaki üç adet resim 1x128x128 boyutundaki verilere dönüştürülmüş ve önceki sayfalarda anlatılan doğrusal olmayan şifreleme (, **Hata! Başvuru kaynağı ulunamadı.**) ile şifrelenmiştir. Şifreli dizi ile açık anahtar olarak her dizi için tasarlanan birer YSA ile eğitim yaptırılarak elde edilen ağırlıklar, 512x512 boyutunda resim verisi olarak alıcı tarafına gönderilmiştir. Alıcı tarafında tasarlanan benzer bir YSA ile şifreli değerler ve ağırlıklar kullanılarak orijinal resmin RGB kodları elde edilmiştir.

Şekil 4-8' de Orijinal Resmin renkli olarak şifrelenmiş halini ve RGB kodlarının her boyutunun orijinal ve şifreli halinin histogramı gösterilmiştir.



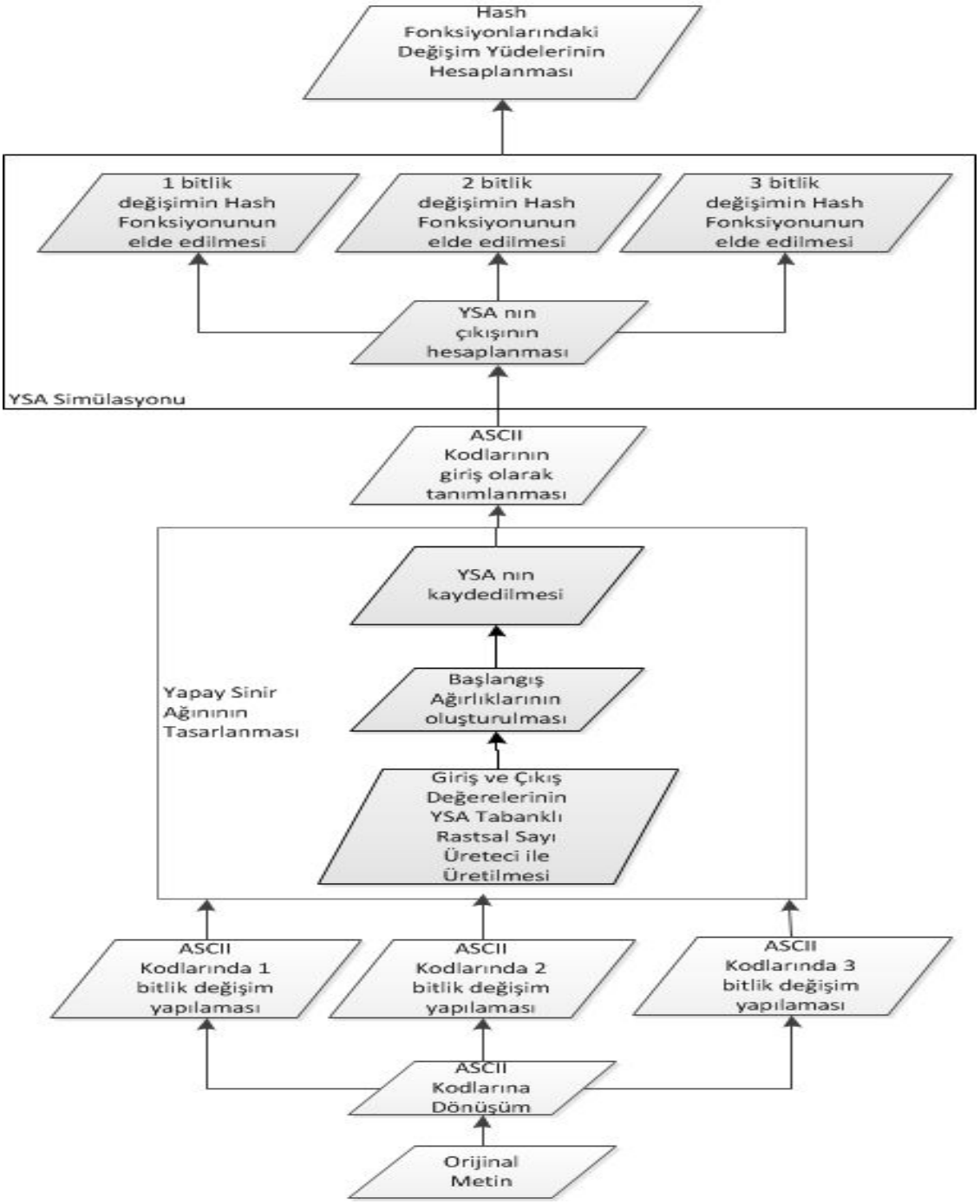
Şekil 4-8 1. sırada Orijinal Resim ve Şifreli Resim. 2.,3. ve 4. sıralarda sırasıyla resmin ilk üç boyutunun şifrelenmiş halini ve histogramını göstermektedir.

4.2.3 Hash Fonksiyonu

Kriptografik sistemlerin olmazsa olmaz özelliklerinden biri güvenirliktir. Sonraki aranan özellik ise mesajı başkalarının anlayamayacağı fakat alıcının anlayabileceği şekilde göndermektir. Bundan sonra gerekli olan ise mesajı okunaklı olmayan şekilde gönderen fonksiyonlardır. Herhangi biri mesajı duyarsa anlayamamalı ve onu çevirememelidir. Kriptografinin bu şekilde fonksiyonlara ihtiyacı vardır. Çünkü bu fonksiyonların ana özellikleri tersinin hesaplanmasının güç olmasıdır.

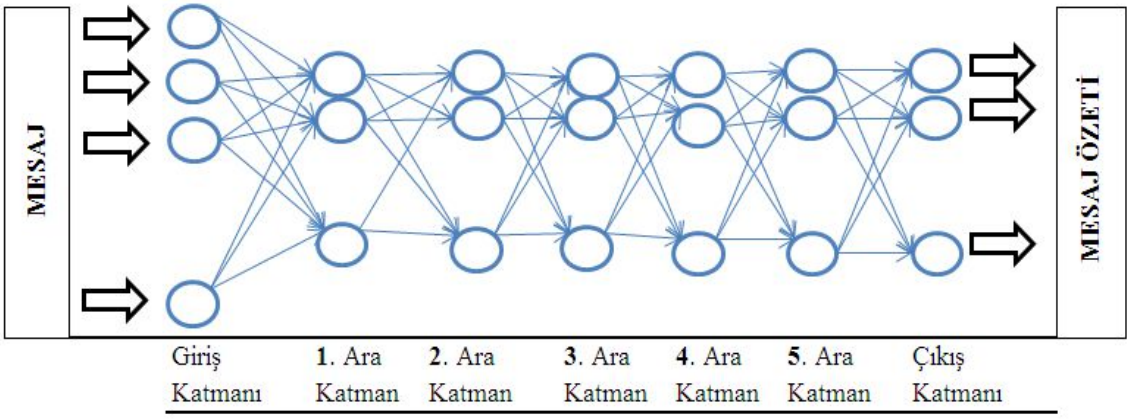
Hash Değeri Üretim Aşamaları

Bu uygulamada kullanılan YSA tabanlı hash fonksiyonu üretim aşamaları Şekil 4-9 'da belirtilmiştir.



Şekil 4-9 Yapay Sinir Ağı Tabanlı Hash Fonksiyonu

Girilen orijinal metin ASCII kodlarına dönüştürülür. Giriş ve çıkış değeri sözde rastsal sayı üreteci (Yayik and Kutlu , 2013) ile üretilen 5 ara katmanlı (33-45-6-17-11) Yapay Sinir Ağının geri yayılım algoritması ile eğitilerek kaydedilir. Kaydedilen YSA nın giriş değeri olarak orijinal metinin ASCII kodları kullanılır. Ağın 5. ara katmanının transfer fonksiyonu tansig (3.2) olduğundan çıkış değeri 0 ve +1 aralığında isteğe göre 1x32, 1x128, 1x256 veya 1x512 uzunluğunda vektör olarak elde edilir. Normalizasyon ve dönüşüm işlemleri sonunda 1x32 büyük ve küçük harflerden oluşan hash değeri elde edilmektedir. Kullanılan Yapay Sinir Ağının yapısı Şekil 4-10' da gösterilmiştir.



Şekil 4-10 Hash Fonksiyonu YSA Yapısı

Hash Değerinin Duyarlılığı

Hash fonksiyonunda amaç farklı mesajlar için farklı mesaj özetlerinin (hash değeri) elde edilmesidir. Buna hash fonksiyonunun açık metin duyarlılığı denilmektedir. Açık metindeki küçük değişimlerin hash değerinde büyük değişimlere neden olmalıdır (5.1).

Duyarlılık : (fark $(H_0,H_i)/S_b$)*100 (5.1)

$\boldsymbol{H_0}$ = Orijinal verinin Hash Değeri

$\boldsymbol{H_i}$ = % i kadar değişiklik yapılmış olan verinin Hash Değeri

S_b =Hash Değerinin karakter sayısı

Fark işlemi parantez içerisindeki değerlerin birbirlerine göre farklılık seviyesini belirlemektedir.

Böylelikle algoritma istatistiksel saldırılara karşı güvenlidir denilebilir (Sumangala ve ark., 2011). YSA tabanlı hash fonksiyonunun açık metin duyarlılığını test etmek maksadıyla açık metinin (orijinal metin) ASCII karakterlerinde küçük değişiklikler yapılarak hash değerindeki değişimler gözlemlenmiştir.

Metnin Hash Değerinin Duyarlılığı

Hash Fonksiyonu alınacak olan metin; "***Günümüz bilgi teknolojileri dünyasında bilginin her geçen gün öneminin ve yaygınlığının artması, bilgiye her noktada erişilebilme isteklerinin artışa geçmesi ile beraber bu hususlara izin verecek olan teknolojik imkânlar her geçen gün hızla gelişmektedir.***" dir. 256 karakterden oluşan bu metnin hash fonksiyonu;

"uJOYbbBfsDbcRQGTGKXCKFTChCVTKBij" dir.

Metinin ASCII kodlarında değişiklikler yaparak hash fonksiyonunun değişimi gözlemlenmiştir. Metnin ASCII kodlarında;

- *1 bitlik değişiklik yapıldığında 32-bit hash değeri*

"kNQYbnBklZnjGVIEIWVTKDRDsTPEGNxf " olmaktadır ve orijinal metnin hash fonksiyonuna göre %96,7 değişiklik göstermektedir.

- *2 bitlik değişiklik yapıldığında 32-bit hash değeri*

"rAVSdwAthLwuRBASEGEHIGXVtBMARVdy" olmaktadır ve orijinal metnin hash fonksiyonuna göre %90,9 değişiklik göstermektedir.

- *3 bitlik değişiklik yapıldığında 32-bit hash değeri*

"rMWLuiIxtUgbJETHDBCAGMUJjMTEWWyl" olmaktadır ve orijinal metnin hash fonksiyonuna göre %96 değişiklik göstermektedir.

Yukarıdaki örnek uygulamada hash değerinin 256 karakterlik orijinal metnin ASCII kodlarında yapılan 1, 2 ve 3 bitlik değişiklere karşı duyarlılığı gösterilmeye çalışılmıştır.

Resmin Hash Değerinin Duyarlılığı

Orijinal Resim

GtCgSZuQVLYCKBTIZXRTPROFW
CRQSGfZcMiROMSfEBeKIEraQSg
EUWpSnJAGRaOYQLHAIEWEWm
cVuYKVyzvIoHLrVWfbQTNXeIImV
yIrONTXVUNAHNBORvDsuMLSW
LXtgRCFiPDLQNRNOeYXLNJXEJ
MCSMSkTILHHtKDOFMPLncYQO
qPAEnVrJEqQJPLCZlLuNNNMmU
RpWJTsJYLNNzCFaFpNDXPNFHC
PgOrAumdldMPFGgTJRHMyVSEG
XIILNEc

256-bit hash Değeri

10 adet bit Değeri Değişen Resim

IrBfRDpJTMBCGYTKVBPQMUQ
FSWQTSZfZePhWSMVfHDhGGFt
dORdATZoTjMWFRuNARPEEEH
WHVjbRvYHDdbsGqFIuSWxuRQ
HYeHJsSaKtPJUXSWQCILYMQv
DooNGSCQBufOEEnPZMOKSMO
fWWMJIYFILATNPpREOFDvNCP
GIMGrbXMUnQZDnVqIFnTMPM
DDiNwJOQKnWQoWIOlHSGLNaB
JeFqLJUQOIFDTfPmAxrdidNREG
cVLRIGbVRIFXFJIOYf

256-bit Hash Değeri

Duyarlılık : % 58

60 adet pixel Değeri Değişen Resim

HsBfSCrLULABHYSIVAPQMSOETX
QTRCdYdNhVRMTfHDgHHFsdORe
BTZqTjNXEQvNYROFEFHXHVjdRu
YJCbztIpGKtTWaxQRIXeIJsTbItPKT
YTWOCJLAMRvDppNGRBPZvgPDF
nPZMPLSMOfWXMLIYFJKBTNQoR
FNFFwNDQFIMHraYOTnQAFnVqJ
EnSKOLDDiMxJOOLoXQoWIOmISH
MNaCJeGpNHVPPIFCShPoBxqdieNQ
EGdULSIHaVRHFXGIKOBf

256-bit hash Değeri

Duyarlılık = % 87

Yukarıdaki örnek uygulamada hash değerinin 327x293x3 boyutundaki parmak izinin 10 ve 60 adet pixelinde yapılan değişiklere karşı duyarlılığı gösterilmeye çalışılmıştır. (Parmak izinde az miktarda pixelin değeri değiştiğinden gözle herhangi bir değişiklik gözlemlenememektedir.)

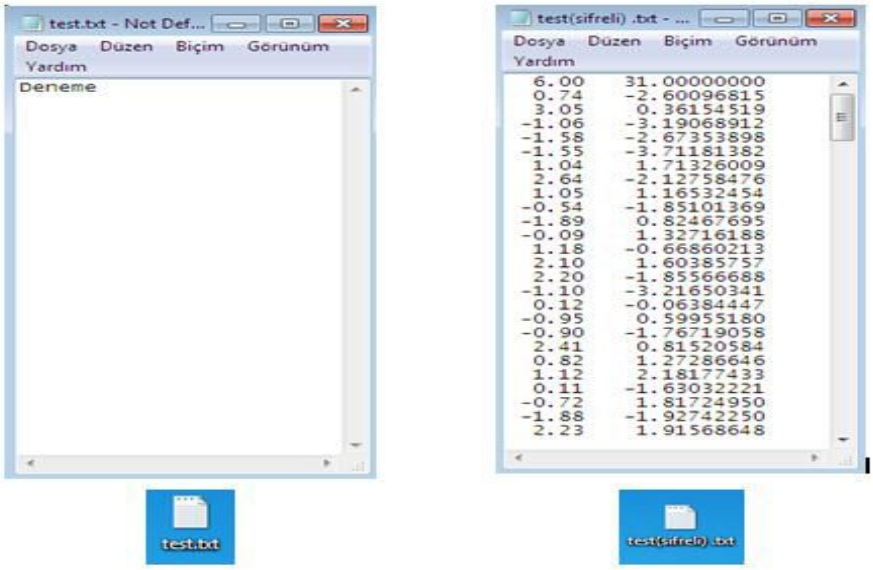
4.2.4 Geliştirilen Arayüzler

Matlab ile gerçekleştirilen kripto sistemi için bir ara yüzler oluşturulmuştur. Oluşturulan ara yüzde kullanıcı yetkilendirilmesi yapılarak yetkisine bağlı olarak kripto işlemleri yapması ve ayrıca oluşturulan YSA yapılarını görebilmesi sağlanmaktadır (Şekil 4-12). Arayüzler sayesinde; dosya şifreleme (

Şekil 4-16) ve gerçek zamanlı şifreleme (Şekil 4-14) olmak üzere 2 farklı şifreleme sisteminden herhangi birini seçme imkânını sağlamaktadır (Şekil 4-13). Gerçek zamanlı şifreleme arayüzü MSN, Facebook, Google+, Twitter gibi sosyal medyada güvenli yazışmalar için kullanılabilecek şekilde tasarlanmıştır. Dosya şifreleme işleminde kullanıcı bilgisayarında kayıtlı bir dosyayı seçerek şifrelenebilmektedir. Şifreleme sonrasında dosyanın isminin yanına parantez içerisine "şifreli" ifadesi otomatik olarak eklenmektedir (Şekil 4-11). Yetkili kullanıcılar tarafından YSA yapısı ve ağırlıkları görülebilmekte ve

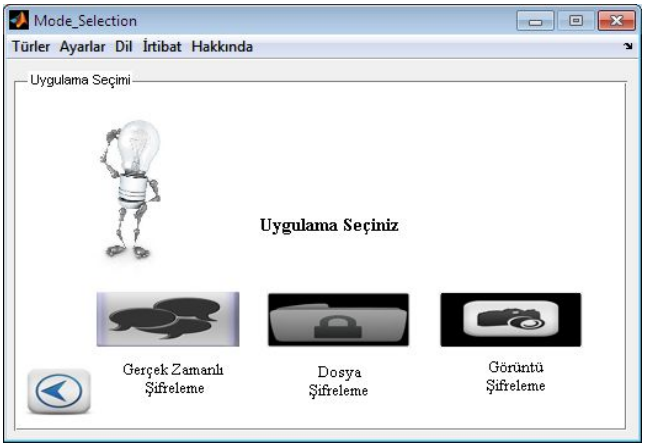
analizi yapılabilmektedir. Şifreleme işleminden sonra dosyalar IP adresi üzerinden Basit Posta Aktarım Protokolü(Simple Mail Transfer Protokol, SMTP) kullanılarak aktarılabilmektedir.

Hash Fonksiyonu Uygulamanın daha etkin görülebilmesi ve incelebilmesi maksadıyla Matlab ile metin (Şekil 4-19) ve resim (Şekil 4-20) için arayüzleri geliştirilmiştir

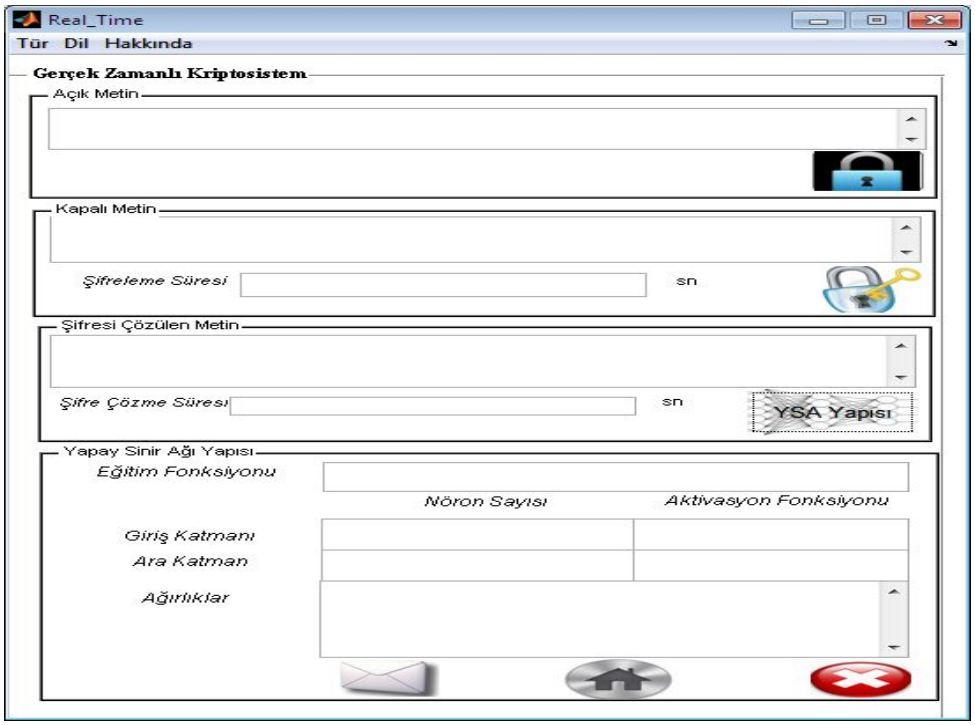


Şekil 4-11 Normal Dosya ve Şifreli Dosya

Şekil 4-12 Oturum Açılışı

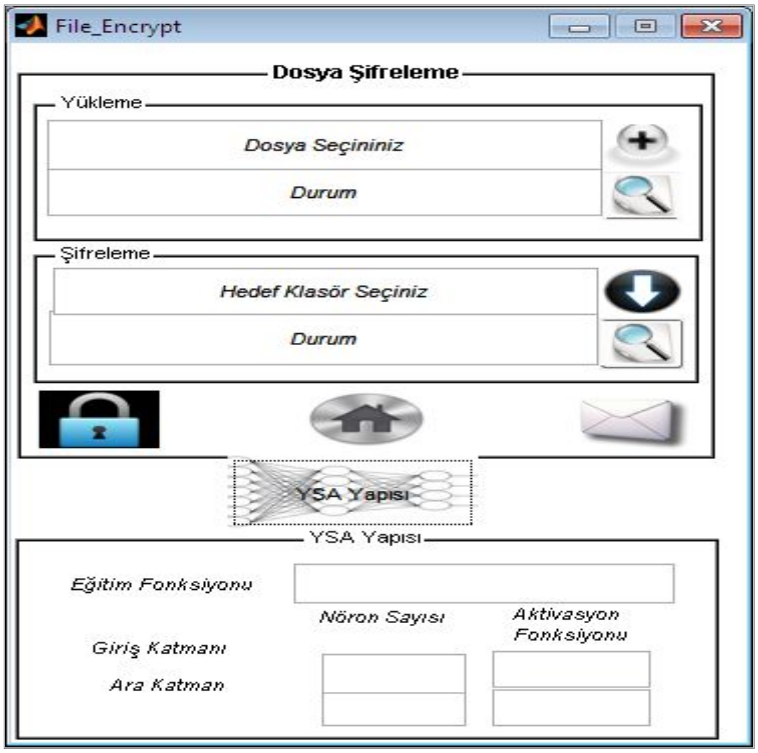


Şekil 4-13 Uygulama Seçimi



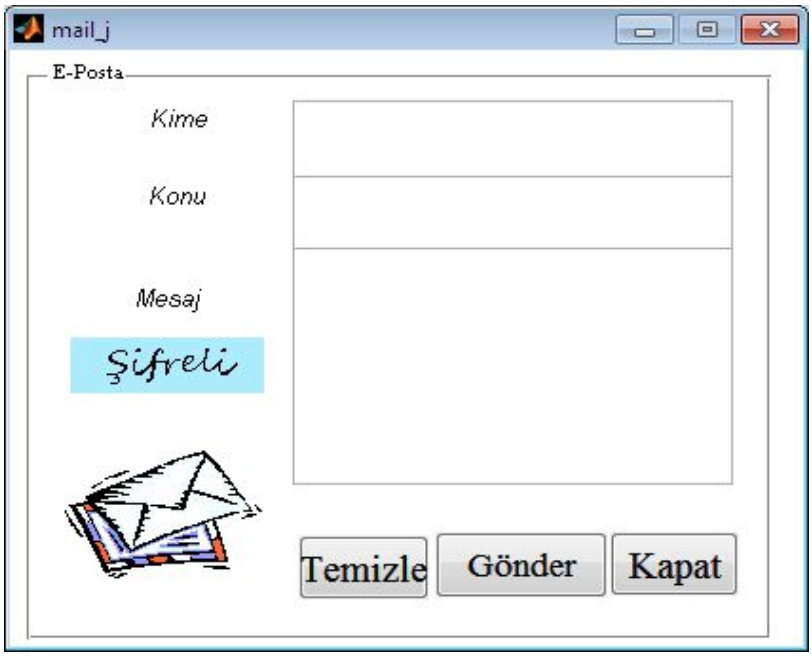
Şekil 4-14 Gerçek Zamanlı Kripto Sistem

Şekil 4-15 Güvenli Dosya Uygulaması Seçimi

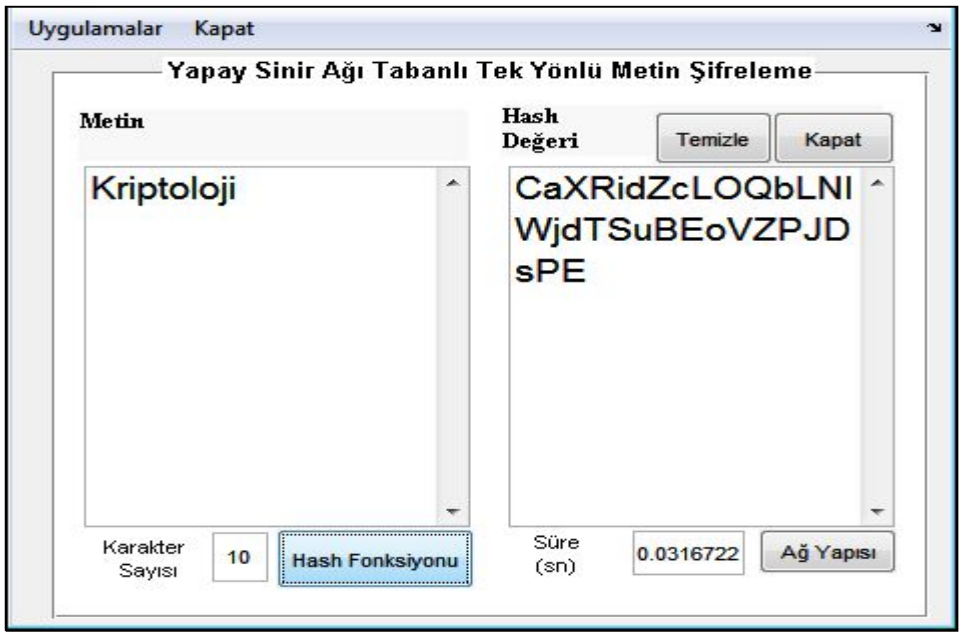


Şekil 4-16 Dosya Şifreleme

Şekil 4-17 Dosya Şifre Çözme



Şekil 4-18 E-Posta Modülü



Şekil 4-19 YSA Tabanlı Hash Fonksiyonu Arayüzü (Metin)

Şekil 4-20 YSA Tabanlı Hash Fonksiyonu Arayüzü (Resim)

5 SONUÇ VE ÖNERİLER

Gelişen bilgisayar teknoloji hızlı işlem yaparak 10 yıl öncesinde çözülmesi 300 yıl süreceği düşünülen klasik kripto sistemlerini dakikalar içinde çözebilecek duruma gelmiştir. Bu sebeple, klasik kripto yöntemlerinin günümüz bilişim teknolojisine ayak uydurması gerekmektedir. Günümüzde kripto sistemlerinin güvenirliğinin ileriye taşınması için mutlaka bilimin gelişen dallarından destek alınmalıdır. Kuantum mekaniği, yapay sinir ağları, kaotik sistemler bunlarda birkaçıdır. Yapay sinir ağları kripto sistemleri; kaotik başlatıcı (Lin ve Jui-Cheng, 2000; Dalkıran ve Danışman, 2010; Yavuz, 2006), sözde rastsal sayı üreteci (Karras ve Zorkadis, 2003; Munukur ve Gnanam, 2007; Othman ve ark., 2011), ezberleme (aşırı öğrenme) (Karras ve Zorkadis, 2003) ve S-kutusu (Noughabi ve Sadeghiyan, 2010) kullanılarak uygulanmaktadır. Bu çalışmada yapay sinir ağlarının sözde rastsal sayı üreteci ile kripto uygulamalarında kullanılmasında yeni bir yol çizilmeye çalışılmıştır. Eğitim yapılan yapay sinir ağının yapısının, YSA tabanlı sözde rastsal sayı üreteçleri ile belirlenmesi sistemin çözülmesini oldukça zorlaştırmaktadır. Bilindiği gibi ağırlık vektörlerinin değerleri eğitimin durumuna ve başlangıç ağırlıklarına göre rastsal olarak değişmektedir, bu çalışmada katmanların nöron sayıları rastsal olduğundan, ağırlık vektörlerinin boyutları da rastsal olarak değişmektedir.

Eğer bir kripto analist şifreyi çözmek isterse öncelikle, kullanılan yapay sinir ağının aynısını tasarlamak yani, bütün topolojiyi ayrıntıları ile bilmek zorundadır ve kripto analistin çok uzun yıllarını alacak gibi gözükmektedir. YSA kullanılarak modellenen herhangi bir kripto sisteminin (AES, 3DES, RSA…vs) şifreli dosyaları çözülebilecektir.

5.1 Rastsal Sayı Üreteci

YSA tabanlı sözde rastsal sayı üreteçleri ile sıradan sözde rastsal sayı üreteçlerinin verileri binary dizilerin rastsallığını ölçmede güvenilirliği kabul edilen (Rukhin and coworkers, 2010) NIST rastsallık testlerine tabii tutulmuştur. Çizelge 5-1 ve Çizelge 5-2’ ye dikkat edildiğinde YSA tabanlı sözde rastsal sayı üreteçlerinin sıradan olana (Modified Subtract with barrow) göre çok daha başarılı olduğu gözlemlenmektedir. Dolayısıyla YSA' nın rastsallığı arttırdığı söylenebilir.

Çizelge 5-1 Yapay Sinir Ağı Tabanlı Rastsal Sayıların Test Sonuçları

Rastsallık Testleri	*p* değeri	Sonuç
FREKANS TESTİ	0.14986	BAŞARILI
BLOK FREKANS TESTİ	0.91173	BAŞARILI
RUNS TESTİ	0.85160	BAŞARILI
BLOKTAKİ EN UZUB BİRLER TESTİ	0.09335	BAŞARILI
KÜMULATİF TOPLAMLAR TESTİ	0.91173	BAŞARILI
AYRIK FOURİER DÖNÜŞÜM TESTİ	0.64636	BAŞARILI
RANK TESTİ	0.74190	BAŞARILI

Çizelge 5-2 Modified Subtract With Borrow İle Üretilen Sözde Rastsal Sayıların Test Sonuçları

Rastsallık Testleri	*p* değeri	Sonuç
FREKANS TESTİ	0.00023	**BAŞARISIZ**
BLOK FREKANS TESTİ	0.23460	BAŞARILI
RUNS TESTİ	0.00021	**BAŞARISIZ**
BLOKTAKİ EN UZUB BİRLER TESTİ	0.00000	**BAŞARISIZ**
KÜMULATİF TOPLAMLAR TESTİ	0.00036	**BAŞARISIZ**
AYRIK FOURİER DÖNÜŞÜM TESTİ	0.40886	BAŞARILI
RANK TESTİ	0.74190	BAŞARILI

5.2 Metin Şifreleme

Eğitim örnek olarak 4 katmanlı 4-3-18-97-1, 4-132-91-86-1, 4-14-7-121-1, 4-196-13-4-1, 4-23-48-51-1 yapılarında yapılmış olup eğitimlerin performansı ile şifreleme ve şifre çözme süresi Çizelge 5-3'de belirtilmiştir.

Çizelge 5-3 Eğitim Bilgileri

KARAKTER SAYISI	NÖRON SAYISI	ŞİFRELEME SÜRESİ (sn)	ŞİFRE ÇÖZME SÜRESİ (sn)	PERFORMANS
200	4-3-18-97-1	0,3105	0.1215	2,14E-01
200	4-132-91-86-1	11.816	0.1111	3,60E-32
200	4-14-7-121-1	10.510	0.1618	1,36E-04
200	4-196-13-4-1,	13.147	0.1978	2,14E-01
200	4-23-48-51-1	6.114	0.1874	3,15E-12

5.3 Resim Şifreleme

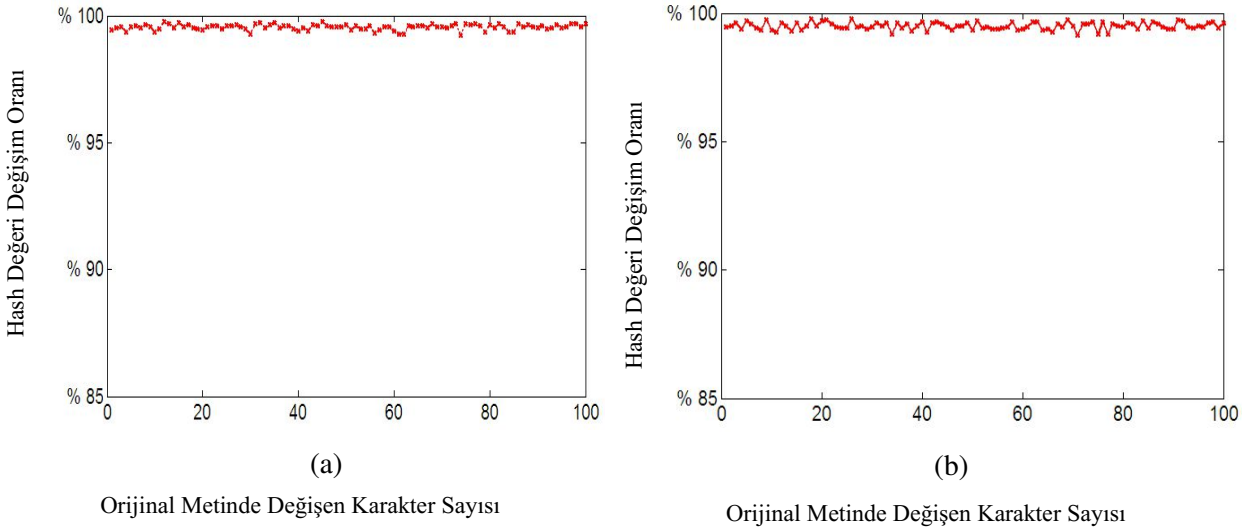
Yapılan çalışmada resim şifreleme işlemi metin şifreleme algoritması kullanılarak yapılmıştır. YSA nın verileri olarak metnin ASCII kodları yerine resmin pixel değerleri kıllanılmıştır. Ancak resmin pixel değerlerinin metne göre çok fazla biyüklükte olduğundan dolayı Lena' nın resmi 26 dk.da şifrelenmiş olup 14 dk.da şifresi çözülmüştür. YSA yapısı değiştirilerek işlem süresinin azaltılabileceği düşünülmektedir. Şifreli resmin histogramı ile orijinal resmin histogramının birbirlerinden tamamen farklı olması (Şekil 4-8) şifreleme işleminin başarılı olduğunu göstermektedir. Bu çalışmada resim şifrelemenin YSA tabanlı yapılabileceği gösterilmiştir.

5.4 Hash Fonksiyonu

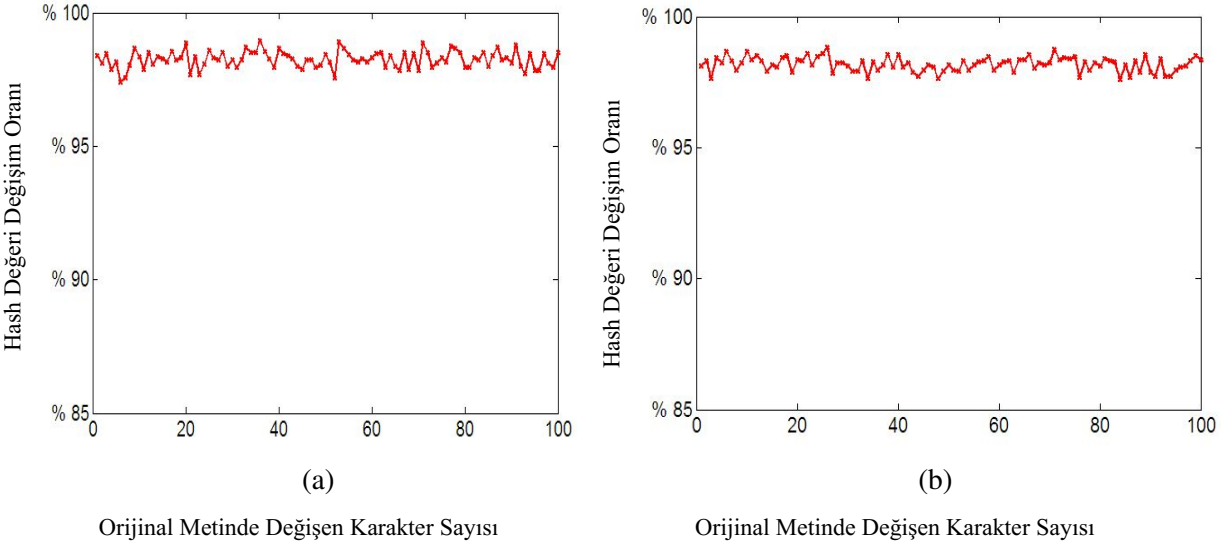
Bu çalışmada resim ve metnin has değeri YSA tabanlı hesaplanmıştır. Hash değeri bir çok çalışmada hexadecimal olarak hesaplanmıştır. Bu çalışmada ise hash değeri iki farlı şekilde; "yalnızca büyük harf, büyük ve küçük harflerden oluşan kombinasyon" şeklinde "32-bit, 128-bit, 256-bit ve 512-bit " uzunluklarında oluşturulmuştur.

Metnin Hash Değerinin Duyarlılığı

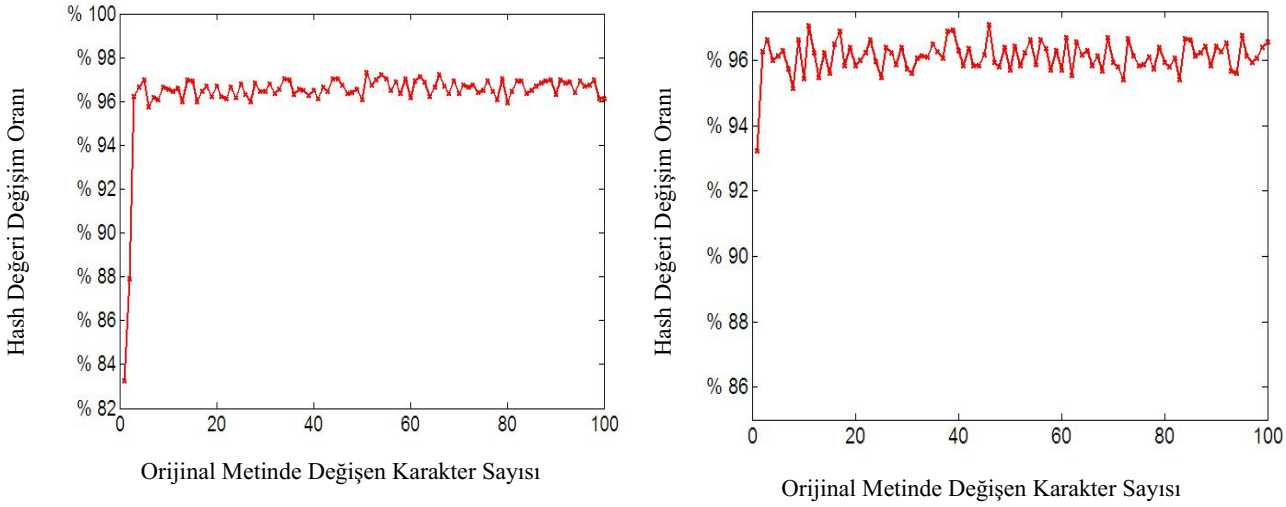
Metnin 256 ve 512 bitlik yalnızca büyük harflerden oluşan ve büyük ve küçük harf kombinasyonundan oluşan hash fonksiyonlarının açık metin duyarlılıkları, Şekil 5-3 ve Şekil 5-4 de gösterilmiştir.



Şekil 5-1 YSA Tabanlı (a) Yalnızca büyük harflerden oluşan, (b) Yalnızca büyük ve küçük harflerden oluşan 32 bit Hash Fonksiyonunun Açık Metin Duyarlılığı

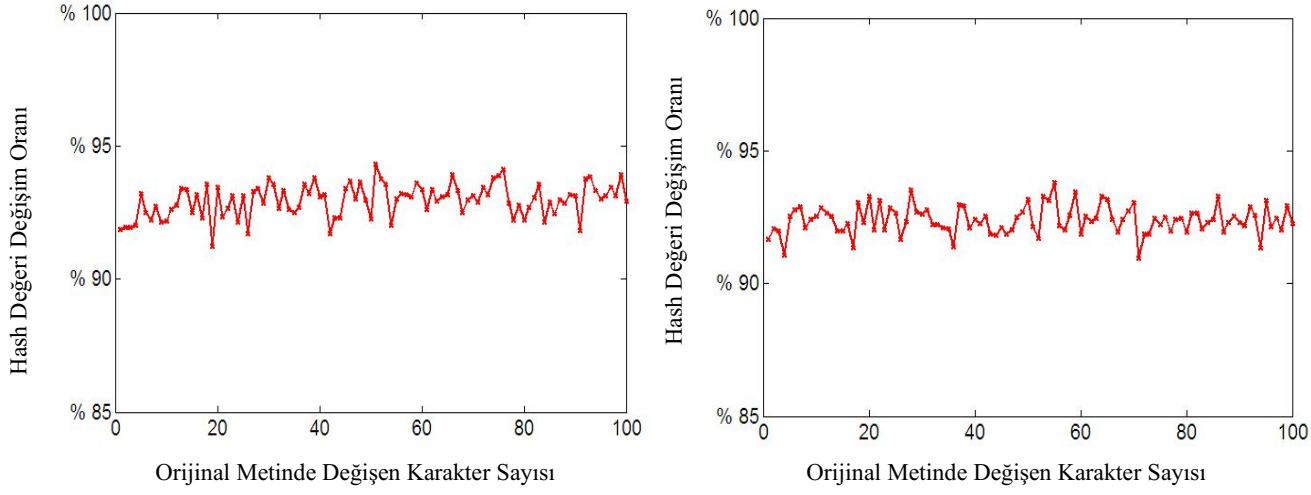


Şekil 5-2 YSA Tabanlı (a) Yalnızca büyük harflerden oluşan, (b) Yalnızca büyük ve küçük harflerden oluşan 128 bit Hash Fonksiyonunun Açık Metin Duyarlılığı



(a) (b)

Şekil 5-3 YSA Tabanlı (a) Yalnızca büyük harflerden oluşan, (b) Yalnızca büyük ve küçük harflerden oluşan 256 bit Hash Fonksiyonunun Açık Metin Duyarlılığı

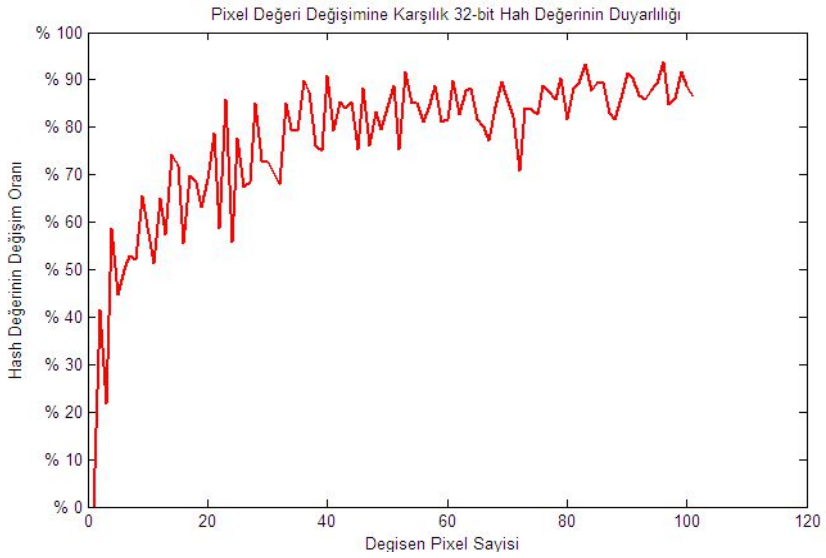


(a) (b)

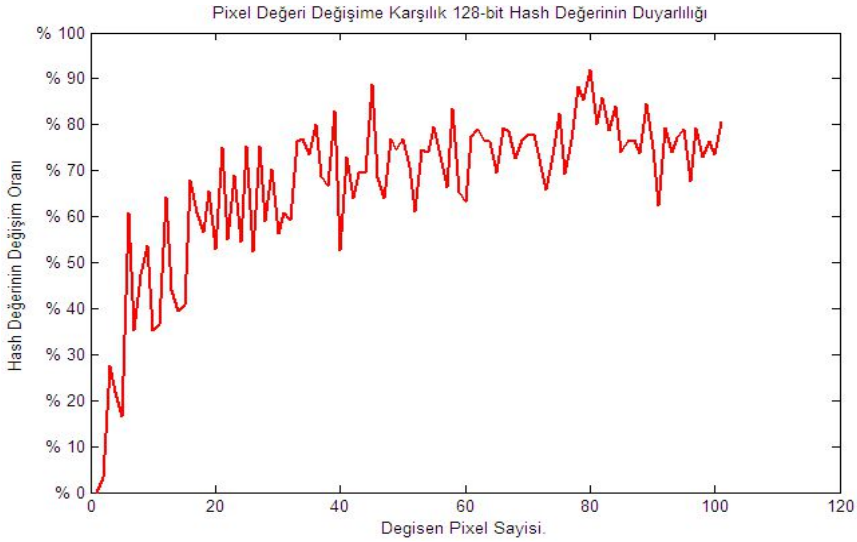
Şekil 5-4 YSA Tabanlı (a) Yalnızca büyük harflerden oluşan, (b) Yalnızca büyük ve küçük harflerden oluşan 512 bit Hash Fonksiyonunun Açık Metin Duyarlılığı

Resmin Hash Değerinin Duyarlılığı

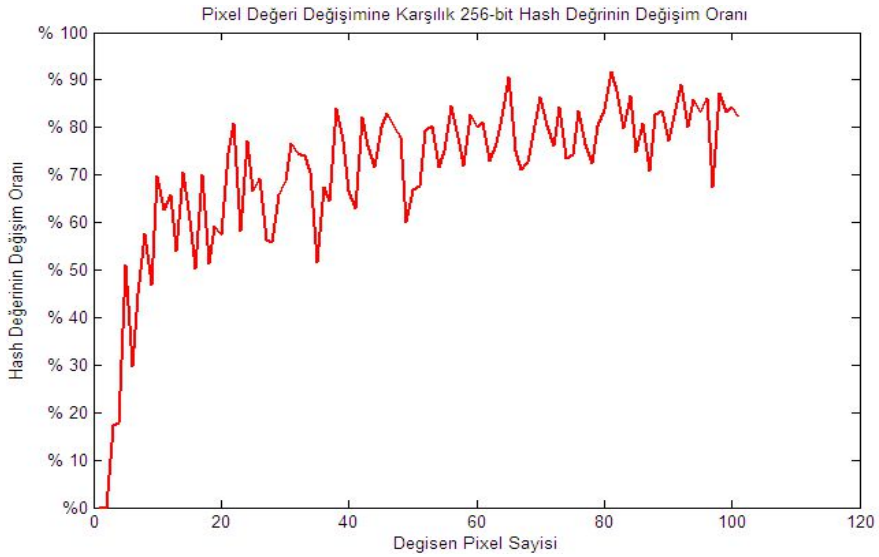
Resmin 32, 128, 256 ve 512 bitlik büyük ve küçük harflerden oluşan hash fonksiyonlarının duyarlılıkları Şekil 5-5, Şekil 5-6, Şekil 5-7 ve Şekil 5-8 ‘ da gösterilmiştir.



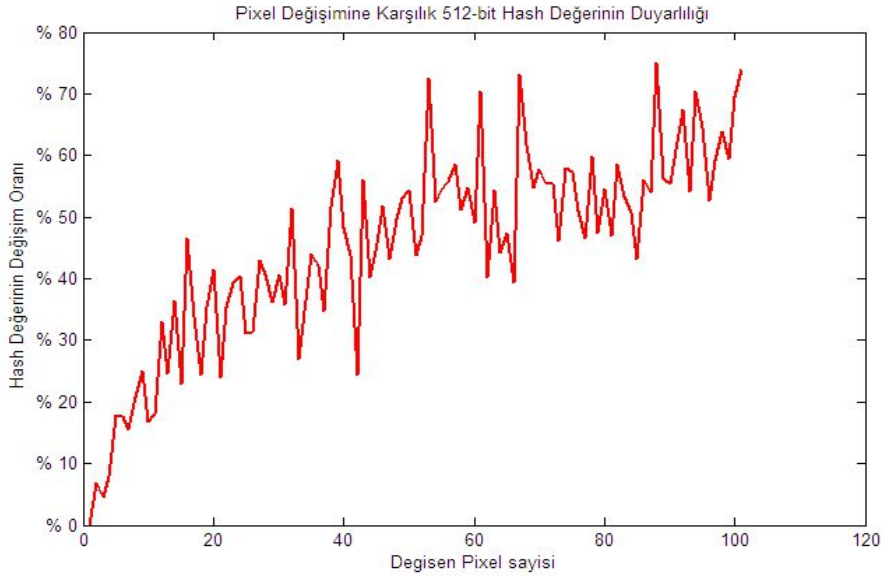
Şekil 5-5 YSA Tabanlı büyük ve küçük harflerden oluşan 32 bit Hash Fonksiyonunun (resim) Duyarlılığı



Şekil 5-6 YSA Tabanlı büyük ve küçük harflerden oluşan 128- bit Hash Fonksiyonunun (resim) Duyarlılığı.



Şekil 5-7 YSA Tabanlı büyük ve küçük harflerden oluşan 256- bit Hash Fonksiyonunun (resim) Duyarlılığı.



Şekil 5-8 YSA Tabanlı büyük ve küçük harflerden oluşan 512- bit Hash Fonksiyonunun (resim) Duyarlılığı.

2011 yılında, giriş katmanında 768, ara katmanda 64, çıkış katmanında 256 adet nöron bulunan ileri beslemeli YSA tabanlı hash fonksiyonunun açık metine karşı duyarlılığı %50 civarında (Sumangala ve ark., 2011) olarak rapor edilmiştir. Bu çalışmada ise; giriş katmanında 100, ara katmanlarında sırasıyla 33, 45, 6 ,17, 11, çıkış katmanında ise hash

değerinin bit sayısına karar veren 32, 128, 256 veya 512 adet nöron bulunan 2 adet geri beslemeli YSA tasarlanmıştır. Tasarlanan YSA' lar kayıt altına alınarak simülasyon ile hızlı bir şekilde metin ve resmin hash değerleri hesaplanmıştır. Farklı bit sayılarının kullanılarak hash değerinin bit sayısına göre ne gibi farklılıklar gösterdiğini incelenmiştir.

Metin ve resmin hash değerinin duyarlılığını anlayabilmek için metnin karakterlerinin ASCII kodlarına ve resmin pixellerine +1 değeri eklenerek hash değerlerindeki değişimler gözlemlenmiştir. Hash fonksiyonu eğer doğru işlem yapıyor ise hash değerlerindeki duyarlılık değeri kesinlikle düz çizgi olmamalıdır sürekli salınım yapmalıdır ve %100 'e yakın olmalıdır.

Şekil 5-1, Şekil 5-2, Şekil 5-3 ve Şekil 5-4' de 256 karaktere sahip bölüm 4.2.3'deki metnin n=1:100 olmak üzere n karakterinin ASCII kodlarına +1 değeri eklenen 32, 128, 256 ve 512 bit hash değerlerinin duyarlılığı gösterilmektedir. Metnin üzerindeki değişikliklerin 32, 128, 256 ve 512 bit hash değerindeki değişim %90 ile %100 arasındadır. Dolayısıyla YSA tabanlı hash fonksiyonu metnin ASCII kodlarının en ufak değişikliğine karşı yüksek derecede duyarlıdır denilebilir.

Şekil 5-5, Şekil 5-6, Şekil 5-7 ve Şekil 5-8' de her defasında rastsal olarak belirlenen farklı pixellerine +1 değeri gürültü olarak eklenen 327x293x3 boyutlu parmak izi resminin sırasıyla 32, 128, 256 ve 512 bitlik hash değerlerinin duyarlılığı gösterilmektedir. Parmak izi resimde +1 değeri eklenen pixel sayısı 32-bit lik hash değeri için 30' u geçtikten sonra, 128-bitlik hash değeri için 45' i geçtikten sonra, 256-bit hash değerinde 60' ı geçtikten sonra, 512-bitlik hash değerinde ise 65' i geçtikten sonra hash değerinde %80' lere varan anlamlı değişiklikler meydana getirdiği gözlemlenmektedir (Şekil 5-5, Şekil 5-6, Şekil 5-7 ve Şekil 5-8). Ortalama değer etrafındaki saçılımların sayısal ölçütü olarak çoğu zaman standart sapma kullanılır. Duyarlılıkların standart sapmaları Çizelge 5-4'de gösterilmiştir. Standart sapma değerlerinin düşük olması tüm değerlerin ortalama değerlere yakın olduğunu yani büyük değişimlerin olmadığını gösterrnektedir.

Dolayısıyla YSA' nın hash fonksiyonu uygulamalarında doğru bir etkili tercih olduğunu söylenebilir.

Ayrıca, YSA tabanlı Hash fonksiyonunun hash değerini üretme süresi de incelenmiştir. Resmin ve metnin hash değeri 1sn in altında oluşturulabilmektedir. Dolayısıyla kullanım etkinliğinin gayet uygun olduğu değerlendirilmektedir.

Çizelge 5-4 Çizelge 5 4 Hash Fonksiyonu Duyarlılığının Standart Sapma Bilgileri

32-Bit			128-Bit			256-Bit			512-Bit		
Pixel Değişim Miktarı	**Ortalama**	**Standart Sapma**	**Pixel Değişim Miktarı**	**Ortalama**	**Standart Sapma**	**Pixel Değişim Miktarı**	**Ortalama**	**Standart Sapma**	**Pixel Değişim Miktarı**	**Ortalama**	**Standart Sapma**
1	35,4	3,1	1	4,0	9,6	1	59,9	5,5	1	4,1	3,0
2	18,8	14,4	2	30,6	13,5	2	14,6	12,6	2	15,4	7,3
3	67,4	11,8	3	39,4	10,0	3	16,2	16,6	3	29,2	3,3
4	31,9	14,8	4	49,8	14,0	4	60,8	16,9	4	14,0	6,1
5	49,3	28,5	5	34,5	15,9	5	40,7	19,1	5	26,0	7,4
6	61,1	18,2	6	48,4	13,1	6	47,8	21,4	6	22,8	7,2
7	50,0	18,6	7	38,9	22,4	7	56,8	17,4	7	18,1	10,3
8	44,4	24,4	8	47,9	15,6	8	70,5	7,5	8	23,6	10,3
9	58,3	19,2	9	56,9	14,5	9	38,9	20,3	9	40,6	11,6
10	67,7	27,8	10	72,1	10,1	10	38,8	19,7	10	30,7	7,2
11	64,9	19,9	11	47,9	21,8	11	60,9	15,0	11	30,5	10,2
12	56,6	16,3	12	50,1	18,7	12	44,2	20,9	12	41,4	16,1
13	77,8	11,3	13	37,8	16,5	13	69,0	10,4	13	29,1	7,4
14	70,5	11,5	14	74,5	14,0	14	61,3	18,5	14	27,1	15,2
15	77,4	9,5	15	42,4	13,1	15	49,5	23,2	15	31,5	18,6
16	75,3	15,7	16	66,1	13,1	16	79,5	7,4	16	25,4	17,6
17	66,0	15,8	17	52,7	16,5	17	61,8	12,5	17	59,3	4,6
18	76,7	12,8	18	64,6	14,7	18	46,7	18,2	18	23,4	10,7
19	84,0	10,3	19	61,7	17,0	19	77,3	11,1	19	53,9	16,7
20	77,1	6,6	20	59,5	13,2	20	78,7	6,6	20	24,3	10,8
21	76,4	14,0	21	58,3	17,9	21	77,5	5,7	21	20,3	9,9
22	81,3	12,4	22	53,0	9,7	22	56,9	18,9	22	33,8	12,0
23	83,0	13,5	23	63,6	19,4	23	75,6	7,2	23	54,8	10,9
24	70,5	13,1	24	72,7	13,3	24	50,4	16,8	24	40,6	16,6
25	72,2	13,2	25	50,7	21,3	25	57,2	17,3	25	30,9	14,8
26	76,7	8,6	26	51,6	22,9	26	68,8	8,1	26	28,0	12,0
27	70,8	20,0	27	51,3	20,2	27	54,6	21,0	27	35,1	11,3
28	83,0	13,5	28	38,1	15,7	28	55,6	15,0	28	36,4	16,4
29	83,7	11,0	29	57,7	22,7	29	62,7	11,0	29	34,8	20,4
30	77,8	14,2	30	54,8	21,8	30	76,4	7,5	30	42,7	22,9
31	70,8	26,0	31	59,5	18,9	31	67,8	16,8	31	42,3	20,8
32	77,1	11,5	32	56,8	15,6	32	72,5	8,4	32	29,8	11,3
33	76,4	16,5	33	59,1	23,6	33	77,2	8,6	33	47,6	12,7
34	73,3	16,9	34	74,7	19,1	34	68,2	19,8	34	33,3	16,2
35	70,5	20,0	35	75,3	4,9	35	73,4	8,2	35	29,4	17,5
36	84,0	11,3	36	51,9	22,1	36	73,0	7,8	36	62,8	7,3
37	83,7	12,3	37	76,0	13,9	37	69,7	7,1	37	45,6	12,9
38	71,9	19,4	38	69,8	16,5	38	74,3	14,8	38	33,0	20,1
39	81,3	8,7	39	68,9	14,2	39	71,7	11,7	39	68,7	5,2
40	92,7	5,2	40	80,7	9,4	40	83,6	4,5	40	46,0	7,0
41	77,4	10,5	41	65,7	8,7	41	73,2	25,3	41	35,5	14,8
42	84,7	6,5	42	69,4	17,8	42	59,8	16,0	42	63,8	10,4
43	84,0	12,1	43	69,4	15,8	43	73,0	12,6	43	45,9	11,8
44	89,6	4,1	44	62,3	25,0	44	63,0	17,8	44	42,5	13,8
45	88,2	9,2	45	73,3	9,7	45	84,5	8,2	45	61,4	17,4
46	78,5	14,7	46	74,0	17,5	46	81,5	9,0	46	55,2	9,3
47	79,9	8,7	47	69,4	13,4	47	84,2	7,5	47	48,5	15,6
48	84,0	8,0	48	79,9	3,2	48	79,2	7,4	48	48,6	12,5
49	80,6	6,9	49	62,5	19,5	49	88,7	4,2	49	57,0	18,1
50	89,2	5,7	50	54,4	12,2	50	73,2	12,1	50	31,2	14,8

32-Bit			128-Bit			256-Bit			512-Bit		
Pixel Değişim Miktarı	**Ortalama**	**Standart Sapma**	**Pixel Değişim Miktarı**	**Ortalama**	**Standart Sapma**	**Pixel Değişim Miktarı**	**Ortalama**	**Standart Sapma**	**Pixel Değişim Miktarı**	**Ortalama**	**Standart Sapma**
51	71,5	16,6	51	68,1	17,4	51	72,3	19,9	51	50,5	12,3
52	88,9	11,8	52	77,3	7,5	52	68,9	16,1	52	35,9	13,6
53	84,0	4,5	53	75,0	7,9	53	68,0	18,5	53	44,3	16,4
54	78,5	15,7	54	84,2	6,9	54	73,7	5,9	54	43,8	13,8
55	89,9	5,4	55	62,2	19,7	55	78,6	8,9	55	43,4	19,7
56	87,8	9,3	56	78,2	12,0	56	86,5	7,2	56	62,7	15,7
57	84,4	7,2	57	90,9	3,4	57	79,9	6,0	57	44,8	13,5
58	69,4	20,7	58	73,2	19,8	58	90,0	4,1	58	44,6	15,8
59	74,3	15,7	59	79,0	10,6	59	78,0	5,7	59	46,7	22,4
60	76,7	19,3	60	83,7	6,6	60	90,7	4,7	60	68,3	9,2
61	70,5	10,9	61	75,7	12,3	61	83,5	8,2	61	64,4	16,3
62	95,1	2,3	62	69,0	27,0	62	90,4	3,3	62	43,8	21,7
63	79,9	14,3	63	75,7	14,8	63	71,8	18,1	63	58,6	18,8
64	81,3	10,6	64	83,3	13,2	64	73,2	13,6	64	58,7	16,3
65	87,2	10,1	65	66,1	21,5	65	78,8	12,7	65	57,6	14,8
66	83,3	9,1	66	75,6	11,8	66	80,6	10,0	66	56,7	17,3
67	87,5	11,8	67	81,3	13,1	67	90,4	3,4	67	80,8	6,2
68	83,3	13,4	68	87,8	3,7	68	65,1	24,2	68	49,6	19,0
69	92,7	5,2	69	78,8	11,4	69	77,6	12,4	69	54,7	8,0
70	85,8	11,4	70	83,5	6,6	70	92,2	1,6	70	54,3	21,2
71	85,1	11,7	71	76,0	13,9	71	77,3	14,0	71	63,1	22,4
72	85,4	15,9	72	72,7	13,1	72	75,5	5,2	72	63,7	9,7
73	90,3	8,2	73	74,9	14,3	73	68,1	15,7	73	61,0	11,2
74	84,4	14,1	74	80,8	11,1	74	71,7	21,1	74	57,5	14,7
75	81,6	12,9	75	90,1	4,2	75	85,2	5,5	75	63,7	16,9
76	90,3	9,4	76	76,0	12,5	76	77,1	13,3	76	63,7	12,4
77	87,8	11,2	77	86,8	6,3	77	79,9	13,7	77	49,9	14,4
78	79,9	9,4	78	70,8	12,7	78	78,0	12,5	78	64,1	8,2
79	87,8	7,7	79	81,8	8,5	79	83,1	6,1	79	59,5	15,4
80	85,4	8,3	80	72,3	17,1	80	79,3	8,0	80	64,4	12,1
81	89,2	6,5	81	88,5	10,5	81	90,0	3,7	81	77,5	7,3
82	85,8	10,7	82	69,0	19,9	82	70,7	20,6	82	79,8	5,0
83	92,0	9,0	83	74,4	16,2	83	77,0	11,6	83	70,7	19,1
84	85,1	12,2	84	70,9	17,7	84	85,5	6,3	84	66,0	16,6
85	89,2	14,8	85	66,3	22,7	85	86,9	4,1	85	47,7	12,0
86	88,2	10,6	86	87,7	5,5	86	92,8	3,3	86	62,7	15,6
87	85,8	12,6	87	83,9	7,9	87	79,1	23,6	87	62,9	12,7
88	84,4	8,0	88	83,5	4,5	88	88,9	8,3	88	51,1	18,0
89	86,5	16,9	89	78,8	9,9	89	80,2	10,8	89	70,7	10,2
90	86,1	6,6	90	73,3	21,7	90	86,6	6,8	90	65,8	8,9
91	87,5	5,4	91	84,6	11,9	91	75,4	16,0	91	65,2	14,3
92	87,8	7,4	92	82,1	6,2	92	86,6	4,7	92	60,9	14,9
93	87,2	9,9	93	87,5	3,6	93	84,5	8,5	93	52,8	11,4
94	86,8	8,2	94	88,9	7,0	94	88,0	3,7	94	68,9	8,6
95	92,7	6,1	95	78,6	12,4	95	79,6	10,1	95	51,2	15,7
96	89,2	6,5	96	69,3	16,9	96	72,1	22,1	96	64,9	14,5
97	93,4	5,5	97	83,1	9,2	97	78,2	11,6	97	50,7	15,6
98	91,0	7,2	98	71,2	12,9	98	74,3	11,9	98	64,6	11,1
99	87,5	10,1	99	82,9	10,8	99	73,7	12,7	99	58,0	15,0
100	84,0	10,2	100	85,1	4,7	100	86,7	5,6	100	54,1	16,7

6 KAYNAKÇA

Rukhin A., Soto J., Nechvatal J., Smid M., Barker E., Leigh S., Levenson M., Vangel M., Banks D., Hackert A., Dray J. ve Vo S. (2010). **A Statical Test For Random and Pseudorandom Number Generators For Cryptographic Algorithms**. Special Publication National Instite of Standart Technology .

Altun, H., ve Eminoğlu, Y. (2006). **MLP Yapay Sinir Ağlarında Öğrenme Sürecinin Aktivasyon Fonksiyonu Ve İstatiksel Değişim Gösteren Giriş Verilerine Bağımlılığı** . Niğde Üniversitesi, Mühendislik-Mimarlık Fakültesi Elektrik-Elektronik Mühendisliği Bölümü Dergisi .

Arvand, M. I., Wu, S., Sadeghian, A., Melek, W. W., ve Woungang, I. (2006). **Symmetric Chipper Design Using Recurrent Neural Networks.** International Joint Conferance on Neural Networks .

B.Kaliski. (1992). **The MD-2 Message Digest Algorithm**. RSA Labratuarı.

Coveyou, R. (1998). **A Mathematic Safari**. The Jungles of Randomness , 178.

Dalkıran, İ. (2003). **Yapay Zeka Tekniği Kullanan Bilgisayar Tabanlı Yüksek Hassasiyetli Sıcaklık Ölçme Birimi Tasarımı.** Yüksek Lisans Tezi, Erciğes Üniverstesi Fen Bilimleri Enstirüsü Kayseri .

Dalkıran, İ., ve Danışman, K. (2010). **Artificial Neural Network Based Choatic Generator For Crytography.** TUBİTAK Eng&Comp.Sci. , 12 (18).

Demuth, H., Beale, M., ve Hagan, M. (2004). **MATLAB Neural Network User's Guide**. The Matworks.

Derya, A., Yerlikaya, T., ve Buluş, E. (2004). **Simetrik Kriptosistemlerden Çok Alfabeli Yerine Koyma Metodunun Türkiye Türkçsinin Yapısal Özelliklerini Kullanarak Kripto Analitik İncelenmesi.** Trakya Üniverstesi .

Desai V., Patil R.veDandine R. (2012). **Using Layer Recurrent Neural Network to Generate Pseudorandom Number Sequences.** International Journal of Computer Science Issues , 1 (9).

Dülgerler, M., ve Sarısakal, N. (2003). **Elgamal Şifreleme Algoritmasını Kullanan Güvenli Bir E-Posta Uygulaması: Md Message Controller**. İstanbul Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü .

E-imza. (2013). **E-Tuğra Nitelikli Elekronik İmza Sertifikası**: http://www.e-tugra.com.tr/ adresinden alınmıştır

Elmas, Ç. (2011). **Yapay Zeka Uygulamaları**. Ankara: Seçkin Yayımcılık.

Fidan, M., ve Gerek, Ö. N. (2008). **Antı-Mycıelskı Sayı Uretecinin Rastsallık Analizi**. Sınyal İşleme ve İletişim Uygulamaları .

Godhavari, T., Alainelu, R., ve Soundararajan, R. (2005). **Cryptography Using Neural Network.** IEEE Indian 2005 Conferance .

Guo, D., Cheng, L., ve Cheng, L. (1999). **A New Symmetric Probablistic Encryption Scheme Based on Chaotic Attractors of Neural Networks.** Applied Intelligence , 1 (10), 71-84.

Gülyurt, M. (2013). **Kurumsal Şifreleme Anahtarı Yönetimi**. Starling Me .

Güvenoğlu, E. (2006). **Görüntü Şifreleme Algoritmaları ve Performans Analizleri**. Trakya Üniverstesi Yüksek Lisans Tezi .

Hamzaçelebi, C., ve Kutay, F. (2004). **Yapay Sinir Ağları ile Türkiye Elektrik Enerjisi Üretiminin 2010 Yılına Kadar Tahmini**. Gazi Üniverstesi Mühendislik-Mimarlık Fakültesi Dergisi , 227-233.

Hughes, J. M., ve College, K. (2007). **Pseudorandom Number Generator Using Binary Recurrent Neural Networks.** A Technical Report submitted to Kalamazoo College .

Karras, D., ve Zorkadis, P. V. (2003). **On Neural Network Techiques in Secure Managment of Communication Systems Through Improving and Quality Assesing Pseudo-Random Stream Generators.** Journal Of Pergamum .

Kulkarni,V. R. and coworkers. (2010). **Hash Functıon Implementatıon Usıng Artıfıcıal Neural Network.** International Journal on Soft Computing (IJSC) , Vol.1, No.1.

Lee L. ve Wong K. (2004). **A Random Number Generator Based Eliptic Curve Operators**. Computer and Mathematics with Applications , 217-226.

Lin, A., ve Jui-Cheng, Y. (2000). **Design and Realization of a New Chaptic Neural Encryption/Decryption Network.** IEEE Asia-Pasific Conf.Cir.&Syst , 335-338.

Marsaglia, G. (1995). **Diehard of Tests Of Battary Randomness**. Supercomputer Computations Research Institute and Department of Statistics .

Marsaglia, G., ve Zaman, A. (1993). **A New Class of Random Number Generators**. Ann Applied Prob. (462-480).

Mooney. (1997). **Monte Carlo Simulation**.

Munukur, R., ve Gnanam, V. (2007). **Neural Network Based Decryption For Random Encryption Algorithms.** Deparment of Electronics and Communication Engeneering PSG College of Technology India .

Neumann, J. V. (1951). **Various Techniques Used In Connection with Random Digits**. Applied Mathematic Series , 36-38.

Noughabi, M., ve Sadeghiyan, B. (2010). **Design of S-Box On Neural Network**. 2010 International Conferance and Information Engineering (ICEIE) .

Orlandi, G., Piazza F., Uncini A., Luminari E., Ascone A. (1990). **Parallel Architectures and Neural Networks.** Third Italian Workshop World Science , 337-343.

Othman, K., ve Al Jammas, M. H. (2011). **Implementation of Neural Cryptographic System Using FPGA.** Journal of Engineering Science and Technology , 4 (6), 441-428.

Önal, S. (2009). **Yapay Sinir AğlarıI Metodu İle Kızılırmak Nehrinin Akım Tahmini.** Yüksek Lisans Tezi, Süleyman Demirel Üniverstesi .

Öztürk, İ. (2003). **Görüntü Şifreleme.** Gebze Institute of Technology .

Pointcheval, D. (1994). **Neural Networks and Their Cryptographic Applications**. Proc.of Euro code , 183-193.

Resmi Gazete. (30.01.2013). **Elektronik İmza İle İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğde Değişiklik Yapılmasına Dair Tebliği**. 28544 sayılı .

Rivest, R. (1990). **The MD-4 Message Digest Algorithm**. MIT Laboratory for Computer Science.

Rivest, R. (1991). **The MD-5 Algorithm**. RSA Labratuarı.

Ruttor, A. (2006). **Neural Synchronization and Cryptography**. Phd Thesis Bayerischen Julius-Maximilians Universty,Germany .

Sağıroğlu, Ş., ve Özkaya, N. (2007). **Neural Solutions For Information Security.** Journal Of Polytechnic , 1 (10), 21-25.

Scheinder, B. (1996). **Applied Cryptography Protocols Algorithms and Source in C**. 2nd New York John Wiley & Sons Inc.

(1995). **Secure Hash Standard. National Institute of Standards and Technology** (NIST) Federal Information Processing Standard (FIPS).

Sivagurunathan, G., Rajendran, V., ve Purusothaman, T. (2010). **Classification of Substitution Chippers Using Neural Networks**. IJCSNS International Journal of Computer Science and Network Security , 3 (10).

Soyalıç, S. (2005). **Kriptografik Hash Fonksiyonları ve Uygulamaları.** Erciğes Üniverstesi Matematik Anabilim Dalı Yüksek Lisans Tezi .

Sulak, F. (2011). **Statical Analyses of Block Chiphers and Hash Functions**. Msc Thesis Middle East Technical Universty .

Sumangala, G., Kulkarni, V., Sali, S., ve Apte, S. (2011). **Perfoance Analayses of SHA-2 Algorithm with and without Using Artificial Neural Networks.** World of Science and Technology , 12-20.

Tanrıverdi, H. (1993). **Yapay Sinir Ağlarnın Kriptolojide Uygulanması.** Yüksek Lisans Tezi Orta Doğu Teknik Üniverstesi .

The Matworks. (2013). (The Matworks) www.mathworks.com/help/techdoc/rendstream.html adresinden alınmıştır

Walker. (1998). **ENT Randomness Test**.

Yavuz, N. (2006). **Kaotik Ortamlarda Güvenli Veri Transferi** . Karadeniz Teknik Üniverstesi Bilgisayar Mühendisliği Ana Bilim Dalı Yüksek Lisans Tezi .

Yayik, A. ve Kutlu, Y.(2013). **Improving Randomness of Pseudo-Random Number Generators.** Signal Processing and Communicaion Conferance April, 2013 .

Yee, L., ve De Silva, L. C. (2002). **Application of Multilayer Perceptron Network as a One-Way Hash Function**. IEEE Trans.Neural Networks , 2 (12), 340-348.

Yerlikaya, T. (2004). **Eliptik Eğri Şifreleme Algoritması Kullanan Dijital İmza Uygulaması.** Trakya Üniverstesi .

Yerlikaya, T. (2003). **Kripto Algoritmalarının Gelişimi ve Önemi.** Trakya Üniverstesi Dergisi .

Yılmaz, R. (2007). **Kriptolojik Uygulmalarda Bazı İstatistik Testler.** Yüksek Lisans Tezi Selçuk Üniverstesi Fen Bilimleri Enstitüsü .

TEŞEKKÜR

Bu çalışma Mustafa Kemal Üniversitesinin 8702 numaralı Bilimsel Araştırma Projesi (BAP) desteği ile yapılmıştır.

Çalışmalarıma sürekli destek veren danışmanın Sayın Yardımcı Doçent Doktor Yakup KUTLU' ya, Bilgisayar Mühendisliği Bölümü Öğretim Üyelerine, eşim Nagehan YAYIK' a, ablam Sevilay GÜVEN' e ve ailesine teşekkürlerimi sunuyorum.

ÖZÇEÇMİŞ

1986 yılında Ankara' da doğdum. 2004 yılında Süleyman Demirel Anadolu Lisesini bitirdikten sonra 2008 yılında Akdeniz Üniversitesi Fen Edebiyat Fakültesi Fizik Bölümünden mezun oldum. 2010 yılında Kara Harp Okulunda Subay Temel Askerlik ve Subaylık Anlayışı Kazandırma Eğitimi tamamladım. 2011 yılında Hatay İskenderun' a tayin oldum. Halen 39'uncu Mekanize Piyade Tugay Komutanlığı Muhabere (Haberleşme) ve Elektronik Bilgi Sistem (MEBS) birimimde görev yapmaktayım.