Metin İçin Yapay Sinir Ağı Tabanlı Hash Fonksiyonu

Yakup KUTLU ve Apdullah YAYIK

***Özet*—Bu çalışmada 5 katmanlı Yapay Sinir Ağı (YSA) ile tek yönlü hash (özet) fonksiyonu tasarlanmıştır. Bu fonksiyon herhangi bir uzunluktaki açık metni şifreleyerek sabit uzunlukta (256-bit veya 512-bit) veri elde edilmesini sağlamaktadır. Hash değerlerinin metindeki karakterlere bağlı duyarlılıkları incelenmiş ve grafiklerle gösterilmiştir. Analizler sonucunda, gerçekleştirilen YSA tabanlı hash fonksiyonunun yüksek duyarlılığa sahip olduğu görülmüştür.**

***Anahtar Kelimeler*—Yapay Sinir Ağı, Hash Fonksiyonu, Duyarlılık, Tek Yönlülük**

***Abstract* — In this paper 5 layered neural network based one way hash function is designed. This function is used to obtain 256-bit or 512-bit length data by encrypting any length text. The hash values are tested for sensitivity and shown by graphics. It is learned that ANN based hash function is on a one-way and seems to be sufficiently high sensitivity.**

***Index Terms*— Neural Network, Hash Function, One-Way**

I. GİRİS

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. SHA-2 güvenli hash fonksiyonunu ve yapay sinir ağı tabanlı hash fonksiyonu istatistiksel testlerden geçirilmiş ve neredeyse aynı sonuçlar elde edilmiştir [1]. Bu çalışmada metnin hash değeri YSA tabanlı hesaplanmıştır. Hash değeri birçok çalışmada hexadecimal olarak hesaplanmıştır. Bu çalışmada ise hash değeri iki farlı şekilde; "yalnızca büyük harf, büyük ve küçük harflerden oluşan kombinasyon şeklinde "256-bit ve 512-bit " uzunluklarında oluşturulmuştur.

II. MATERYAL VE YÖNTEMLER

Hash fonksiyonları ile büyük tanım bölgeleri küçük değer bölgelerine dönüştürülür.

Birinci Yazar Yakup KUTLU, Mustafa Kemal Üniversitesi Bilgisayar Mühendisliği Bölümü, Hatay Türkiye,Tel: +90 (326) 613-5600/ 4323; e-mail=ykutlu@mkü.edu.tr

İkinci Yazar. Apdullah YAYIK, Türk Silahlı Kuvvetleri, Mustafa Kemal Üniversitesi Fen Bilimleri Enstitüsü Enformatik Ana Bilim Dalı, Hatay Türkiye, e-mail=apdullahyayik@gmail.com.

Elde Hash değerleri duyarlılık testi sınanmıştır. Sonuç olarak YSA' nın tek yönlü hash fonksiyonu olarak kullanılabilirliği gösterilmiştir.

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 [2].

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 [3].

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.

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 [4].

A. *Yapay Sinir Ağları*

İnsan vücudu, sinir sistemi sayesinde yaşadığı olaylardan meydana gelen her türlü fiziksel, biyolojik ve kimyasal 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 [5].

Doğada olduğu gibi yapay sinir ağlarında da elementler arasındaki bağlantı ağ fonksiyonunu belirtmektedir. Elementler arasındaki bağlantılar (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 [6]. Net bir ifadeyle, yapay sinir ağları yapay nöronların ağırlıklandırılmış grafiğidir [7]. 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 [5].

Çok katmanlı ağlar (MLP) giriş, bir veya daha fazla sayıda ara ve çıkış katlarına sahip olup mimari açıdan ileri beslemeli, öğrenme algoritması bakımından danışmanlı öğrenen ağları sınıfındandır. 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 [8].

B. *Yapay Sinir Ağlarının Tek Yönlülüğü*

Yapay sinir ağlarının kriptoloji uygulamalarının birçok avantajı vardır [8]. 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 hedeflenen değerden giriş değerini hesaplamak kolay olmaktadır. Yapay sinir ağları bu özelliğinden dolayı hash fonksiyonlarında kullanılmaktadır.

$$y_k = \emptyset(\sum_{j=1}^{m} w_{k.}\, x_j\, b_k) \qquad (1)$$

Yapay sinir ağlarında paralel uygulama önemli bir özelliktir. Her katman paraleldir. Böylece her katmanda bağımsız fonksiyon uygulanabilir. Bu yüzden veri işleme uygulamaları için uygundur. Yapay sinir ağlarının doğrusal olmayan ve karmaşık değerler arasında ilişki kurma yeteneği vardır. 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.

D. *Açık Metin Duyarlılığı (AMD)*

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.

$$\boldsymbol{Duyarlılık} = \frac{Fark(H_o, H_i)}{S_b} \times 100 \qquad (2)$$

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

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

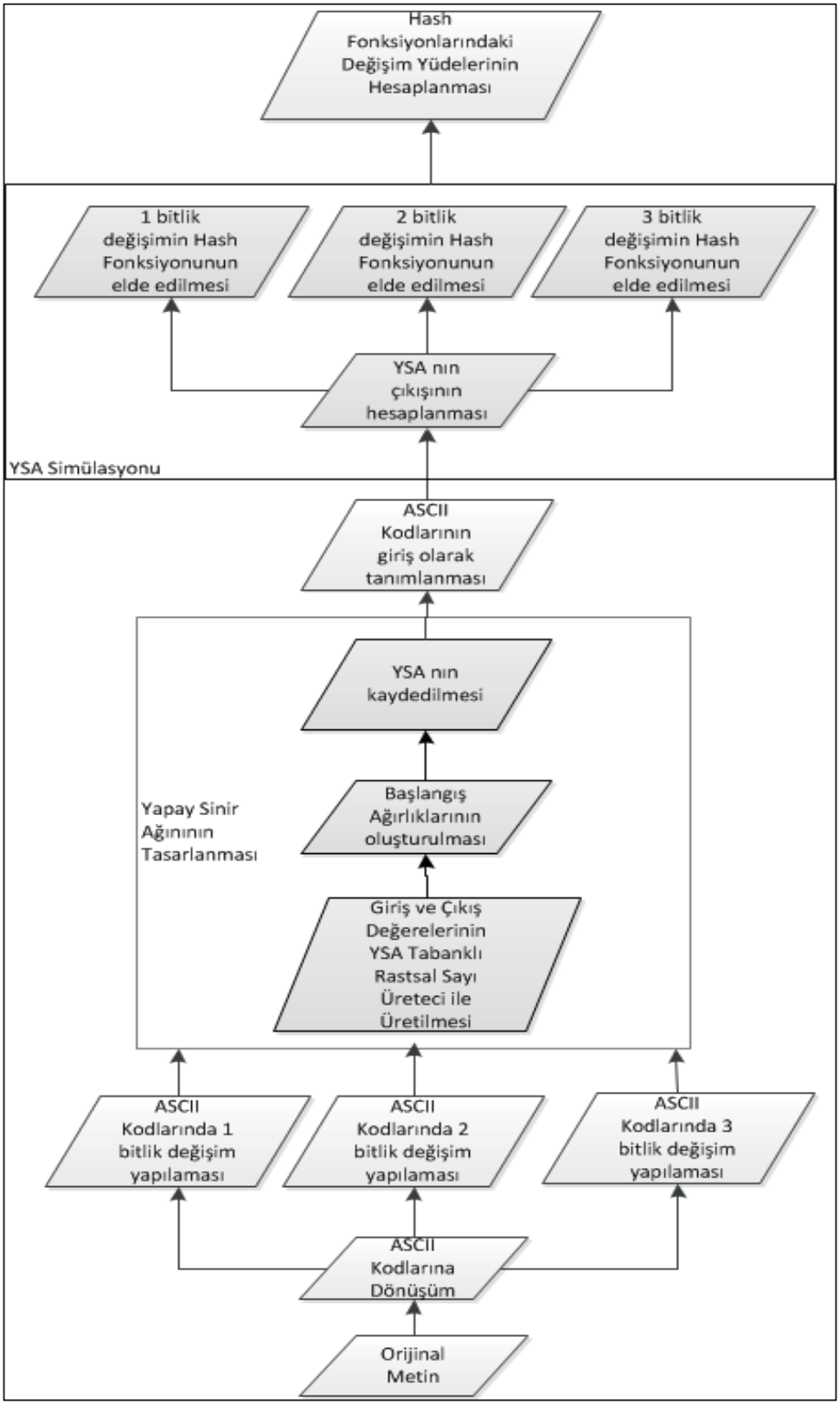
$\boldsymbol{S_b}$ =Hash Değerinin karakter sayısı

Fark işlemi parantez içerisindeki değerlerin birbirlerine göre farklılık seviyesini belirlemektedir.

Böylelikle algoritma istatistiksel saldırılara karşı güvenlidir denilebilir [1]. YSA tabanlı hash fonksiyonunun açık metin duyarlılığını test etmek maksadıyla açık metinin (orijinal metin) ASCII karakterlerinde küçük değişiklikler yapılarak hash değerindeki değişimler gözlemlenmiştir.

E. *Hash Değeri Üretim Aşamaları*

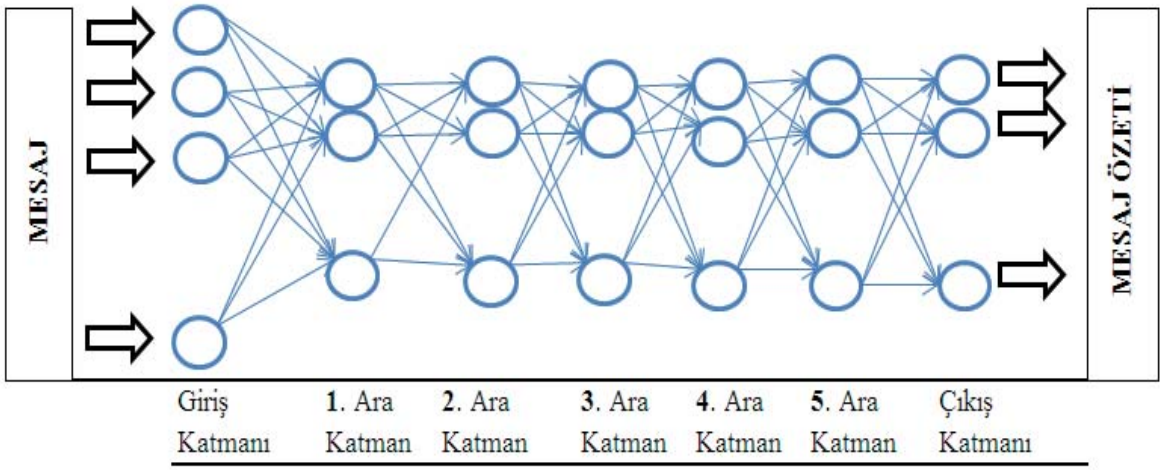
Bu uygulamada kullanılan YSA tabanlı hash fonksiyonu üretim aşamaları Şekil 1'de belirtilmiştir.



Şekil 1 Yapay Sinir Ağı Tabanlı Hash Fonksiyonu.

Girilen orijinal metin ASCII kodlarına dönüştürülür. Giriş ve çıkış değeri sözde rastsal sayı üreteci [10] 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 olduğundan çıkış değeri 0 ve +1 aralığında isteğe göre 1x32, 1x128, 1x256 veya 1x512

uzunluğunda vektör olarak elde edilir. Normalizasyon ve dönüşüm işlemleri sonunda büyük ve küçük harflerden veya yalnızca büyük harflerden oluşan hash değeri elde edilmektedir. Kullanılan Yapay Sinir Ağının yapısı Şekil 2' de gösterilmiştir.



Şekil 2 Hash Fonksiyonu YSA Yapısı

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 32-bit hash fonksiyonu;

"uJOYbbBfsDbcRQGTGKXCKFTChCVTKBij" dir.

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

- *1 bitlik değişiklik yapıldığında hash fonksiyonu*

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

- *2 bitlik değişiklik yapıldığında hash fonksiyonu*

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

- *3 bitlik değişiklik yapıldığında hash fonksiyonu*

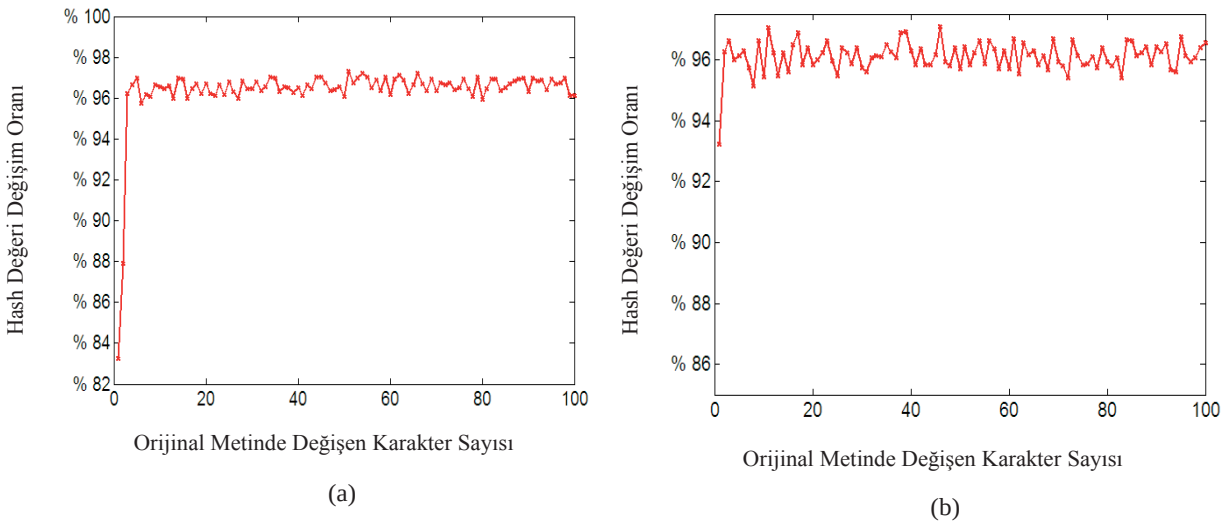
"rMWLuiIxtUgbJETHDBCAGMUJjMTEWWyl" olmaktadır ve orijinal metnin hash fonksiyonuna göre %96 değişiklik göstermektedir.

III. SONUÇ

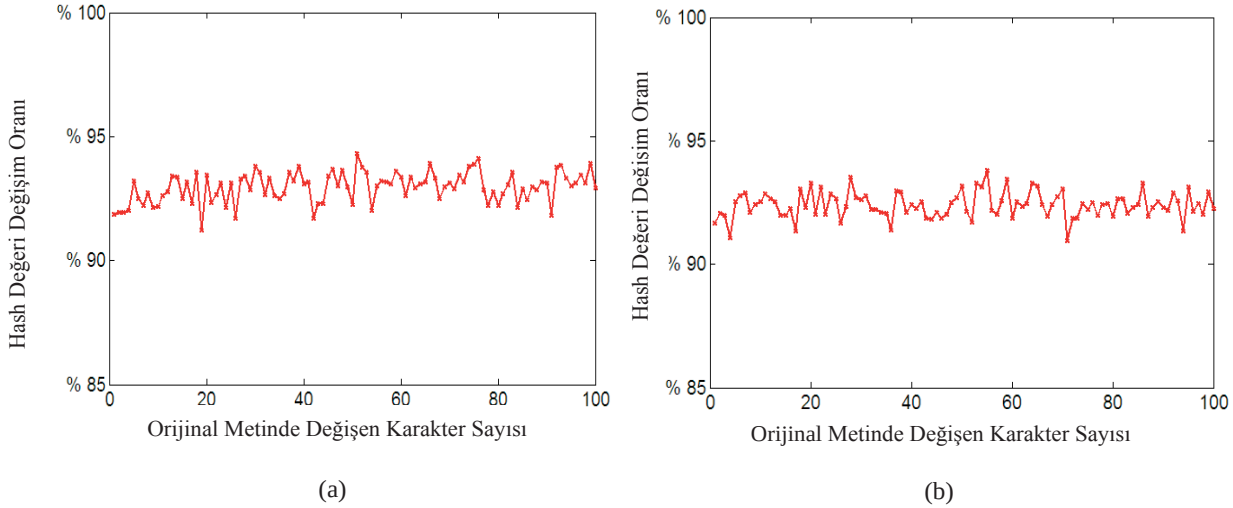
Bu çalışmada; hash değeri YSA tabanlı hesaplanmıştır. Hash değeri birçok çalışmada hexadecimal olarak hesaplanmıştır. Bu çalışmada ise hash değeri iki farlı şekilde; "yalnızca büyük harf, büyük ve küçük harflerden oluşan kombinasyon" şeklinde "32, 128, 256 ve 512bit " uzunluklarında oluşturulabilmektedir.

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 3 ve Şekil 4' de gösterilmiştir.



Şekil 3 YSA Tabanlı (a) Yalnızca büyük harflerden oluşan, (b) Yalnızca büyük ve küçük harflerden oluşan 256- bit Hash Değerinin Duyarlılığı.



Şekil 4 YSA Tabanlı (a) Yalnızca büyük harflerden oluşan, (b) Yalnızca büyük ve küçük harflerden oluşan 512- bit Hash Değerinin 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 [1] 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 256 veya 512 adet nöron bulunan 2 adet geri beslemeli YSA tasarlanmıştır. Tasarlanan YSA ile metin ve resmin hash değerleri hesaplanmıştır. Farklı bit sayılarının kullanılması hash değerinin bit sayısına göre ne gibi farklılıklar gösterdiğini tespit etmektir.

Metin ve resmin hash değerinin duyarlılığını anlayabilmek için metnin üzerinde belirli oranlarla artan değişiklikler yapılmış, resme ise belirli oranlar ile gürültüler eklenerek hash değerindeki değişim gözlemlenmiştir. Hash fonksiyon eğer doğru işlem yapıyor ise hash değerinin duyarlılık değeri kesinlikle düz çizgi olmamalıdır sürekli salınım yapmalıdır ve %100 'e yakın olmalıdır.

Metinin üzerindeki değişikliklerin hash fonksiyonunda değişim oranı %90 ile %100 arasında (Şekil 3 ve Şekil 4) olan yüksek miktarda değişikliğe sebep olduğu sonucuna ulaşılmıştır. Dolayısıyla YSA' nın hash fonksiyonu uygulamalarında doğru bir etkili tercih olduğunu söylenebilir. Farklı YSA yapıları ile daha yüksek sonuçlar elde edilebileceği düşünülmektedir.

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

TEŞEKKÜRLER

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

KAYNAKLAR

[1] Gadgi Sumangala, V.R. Kulkarni, Shridevi Sali, and Sulabha Apte, "Perfoance Analayses of SHA-2 Algorithm with and without Using Artificial Neural Networks," *World of Science and Technology* , pp. 12-20, 2011.

[2] Seniye Soyalıç, "Kriptografik Hash Fonksiyonları ve Uygulamaları," *Erciğes Üniverstesi Matematik Anabilim Dalı Yüksek Lisans Tezi*, 2005.

[3] Mustafa Dülgerler and N.S. Sarısakal, "Elgamal Şifreleme Algoritmasını Kullanan Güvenli Bir E-Posta Uygulaması: Md Message Controller," *İstanbul Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü*, 2003.

[4] Resmi Gazete, Elektronik İmza İle İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğde Değişiklik Yapılmasına Dair Tebliği, 30.01.2013.

[5] İlker Dalkıran and Kenan Danışman, "Artificial Neural Network Based Choatic Generator For Crytography," *TUBİTAK Eng&Comp.Sci.*, vol. 12, no. 18, 2010.

[6] The Matworks. [Online]. www.mathworks.com/help/techdoc/rendstream.html, (2013)

[7] Bruce Scheinder, "Applied Cryptography Protocols Algorithms and Source in C," *2nd New York John Wiley & Sons Inc.*, 1996.

[8] Çetin Elmas, *Yapay Zeka Uygulamaları*. Ankara: Seçkin Yayımcılık, 2011.

[9] N. Mohammed and S. Babak, *Desigh of S-box on Neural Network*.: International Conferance on Electronics and Information Engineering (ICEIE), 2010.

[10] Yayik and Kutlu , "Improving Randomness of Pseudo-Random Number Generators," *Signal Processing and Communicaion Conferance April, 2013*

Yakup KUTLU (1977) Lisans eğitimini 2001 yılında Dokuz Eylül Üniversitesi Elektrik ve Elektronik Mühendisliği bölümünde, Yüksek Lisans eğitimini 2004 yılında Mustafa Kemal Üniversitesi Elektrik ve Elektronik Mühendisliği Ana Bilim Dalında, Doktora eğitimini ise 2010 yılında Dokuz Eylül Üniversitesi Elektrik ve Elektronik Mühendisliği Ana Bilim Dalında tamamlamıştır.
2002-2005 yılları arasında Mustafa Kemal Üniversitesi Elektrik ve Elektronik Bölümünde araştırma görevlisi olarak görev yapmıştır. 2011 yılından itibaren Mustafa Kemal Üniversitesi Bilgisayar Mühendisliği Bölümünde öğretim üyesi olarak çalışmaktadır.
Yardımcı Doçent Doktor KUTLU, Biyomedikal Sinyal İşleme, Kriptoloji, Örüntü Tanıma, Yapay Sinir Ağları ve Genetik Algoritma konularında çeşitli çalışmalar yapmıştır.

Apdullah YAYIK (1986) Lisans Eğitimini 2008 yılında Akdeniz Üniversitesi Fizik Bölümünde, Yüksek Lisans Eğitimini 2013 yılında Mustafa Kemal Üniversitesi Enformatik Ana Bilim Dalında tamamlamıştır.
2010 yılından itibaren Türk Silahlı Kuvvetlerinde çalışmaktadır.
Biyomedikal Sinyal İşleme, Örüntü Tanıma ve Kriptoloji konularında çeşitli çalışmalar yapmıştır.