YAZI DİLİNDE KULLANILAN TÜM KARAKTERLERİN YAPAY SİNİR AĞLARI İLE ŞİFRELENMESİ VE ŞİFRESİNİN ÇÖZÜLMESİ

Şeref SAĞIROĞLU[1] **Necla DEMİRAYAK[2]** **Tuba BAYDAR[3]**

[1,2,3]Bilgisayar Mühendisliği Bölümü
Mühendislik Fakültesi
Erciyes Üniversitesi, 38030, Talas, Kayseri

[1]e-posta: ss@erciyes.edu.tr [2] e-posta: neclad@erciyes.edu.tr
[3] e-posta: tbaydar@yahoo.com

Anahtar sözcükler: *Yapay sinir ağları, Şifre çözme, Şifreleme, Levenberg-Marquardt algoritması*

ABSTRACT

This paper presents a new technique based on artificial neural networks for encryption and decryption of the documentations. Multilayered perceptrons (MLPs) are used for encryption and decryption. Study has two MLP modules: encryption module and decryption module. MLPs are trained with the Levenberg-Marquardt algorithm. All of English characters in writing communication are used in crypto system. The results have shown that the crypto system based on MPLs is very successful. The crypto system presented in this work requires many years to be decrypted and also provides more security and fast operation.

1. GİRİŞ

Bilgi insan hayatında daima önemli olmuş ve insanlar yüzyıllardan beri sahip oldukları bir takım bilgilerini saklama ihtiyacı duymuşlardır. Bunun için en ince detaylarına kadar düşünülmüş protokol setleri ve mekanizmalar geliştirmişlerdir [1-6]. Tarih boyunca bu gizli bilgilere ulaşmak isteyen yetkisiz insanlar da varolmuş ve bilgi güvenliği için oluşturulan mekanizmayı etkisiz hale getirip bilgiye ulaşmak istemişler, çoğunlukla da başarılı olmuşlardır. Bilgi güvenliği, bilginin dökümanlar ile ifade edilmesi, taşınması ve bilgi iletişiminde bu dökümanların kullanılmasıyla daha çok önem kazanmıştır. Günümüzde elektronik iletişimin artmasıyla birlikte bilgi güvenlik sistemlerinin kullanımı artık bir zorunluluk haline gelmiştir [1-6]. Çünkü bilginin elektronik ortamda saklanması ve iletilmesi yetkisiz insanın bu bilgiye erişimini, müdahalesini ve bilgiyi kopyalamasını kolaylaştırmıştır. Günümüz teknolojisi bize çok kısa sürede bir bilginin orijinalinin aynısının yüzlerce kopyasını oluşturabilme ve bir kaç saniye içerisinde farklı ortamlara aktarabilme imkanı sunmaktadır. Bize bu imkanı sunan teknolojinin altında bilgi yoğun işlerin olması ise günümüzde bilginin ekonomik ve stratejik değerini artırmakta ve bu bilginin güvenli bir ortamda saklanması ve iletilmesi için daha fazla çaba sarfedilmesine ve büyük paralar harcanmasına neden olmaktadır. [1-6].

Kriptografi, eskiden beri milli sır ve stratejileri, kurumlara özel bilgileri ve kişisel gizli bilgileri korumak için kullanılan bir sistemdir. Kısaca, bilgi güvenliğinin sağlanması için matematiksel yöntemler kullanılarak oluşturulmuş teknikler setinin bütünü olarak da ifade edilmektedir. Bilgi güvenliğinin sağlanmasında yalnızca matematiksel algoritmalar ve tek başına protokoller yeterli olmamış, belli kuralları olan tekniklerin matematiksel algoritmalarla birleştirilmesine ihtiyaç duyulmuştur [1-6].

Bilgi güvenliği geniş bir kavramdır, ve bilginin gönderildiği yerden, alındığı yere ulaştırılıncaya kadar iletişimin her safhasında bilinmeyen veya yetkili olmayan kişilerin müdahalesinden uzak olması (data integrity), bilginin çıkış-varış adresinin doğruluğu (authentication), iletişim esnasında diğer uyarı sinyal ve işlemlerin etkilerinden korunmuş olması (non-repudiation) ve bilgiyi görmesi gerekenler dışındakilerden saklanması (privacy or confidentiality) olarak bilinir [1].

Şifreleme, mesajın içeriğini anlaşılamayacak formata dönüştürme işlemi (encryption, encipher, kodlama), şifre çözme ise, yapılan şifreleme işleminin tersi yani şifrelenmiş bir mesajı şifrelenmeden önceki formata dönüştürme (decryption, decipher, kod çözme) işlemidir.

Kriptoanalist ve kriptolog, ise şifrelenmiş bir mesajın gizli anlamını bulmak amacıyla şifreleme ve/veya şifre çözme ile uğraşırlar. Kriptolog buna yetkisi olan kişi iken, kriptoanalist yetkisi olmayan kişidir [1-6].

Güvenli bilgi aktarımında bir döküman, bilinen bir matematiksel teknik ile şifrelenir ve döküman bu haliyle alıcı tarafa ulaştırılır, alıcı tarafta şifreleme işleminin tersi gerçekleşir, yani şifrelenen döküman gönderici taraftaki şifreleme yöntemine göre deşifre edilir. DES, IDEA, RC5, CAST, BLOWFISH, 3DES ve RSA bilinen ve en çok kullanılan gizli anahtarlı kripto sistemleridir [1-6]. Bu kripto sistemlerinin kullanımı zaman alıcı, maliyeti yüksek, donanım olarak gerçekleştirilmesi ise oldukça güçtür [1-6].

Yapay Sinir Ağları (YSA), yapılarından kaynaklanan pek çok avantajından dolayı, şifre sorgulamada [7] ve kriptoanalizde [8] kullanılmaktadır. Bu çalışmalarda, eğitim seti olarak türkçe ve ingilizce karakterler kullanılmıştır. Beş giriş - beş çıkış ve sekiz giriş - sekiz çıkış kullanılarak gerçekleştirilen bu çalışmalarda YSA modelleri genel olarak dokümanların şifrelenmesi ve şifresinin çözülmesinde başarılı sonuçlar vermekte, ancak dökümanların tam transferinde yeterli olmamaktadırlar. Bu alanda yapılan çalışmalarda her zaman daha güvenli bir algoritma veya yöntem geliştirmek ise istenilen ve beklenilen bir sonuçtur.

Sunulan çalışmada yapay sinir ağları (YSA), örnekten öğrenebilme özelliği, öğrendiğini genelleyebilme yeteneği kolayca farklı problemlere uyarlanabilirliği, kullanıcının girişle çıkış arasındaki ilişkiyi tarif etme mecburiyetinin olmaması, paralel yapılarından dolayı hızlı çalışabilme yeteneği ve kolay bir şekilde uygulanabilmesi gibi pek çok avantajından dolayı, tercih edilmiştir.

Ayrıca YSA uygulamaları için geçerli olan yazılımsal ve/veya donanımsal gerçekleştirilebilirlik özelliği sayesinde kripto sistemlerinin ihtiyaca göre donanımsal veya yazılımsal olarak gerçekleştirilebilmesi de mümkün olmaktadır. Donanım olarak gerçekleştirilen kripto sistemleri için YSA'nın paralel işlem özelliğinden yararlanılarak hızlı bir şifreleme ve şifre çözme işlemi gerçekleştirilebilir.

Şifreleme ve şifre çözme işlemini gerçekleştirmek için YSA yapılarından en çok kullanılan ve birçok sahada başarılı sonuçlar veren çok katlı perseptronlar (ÇKP) kullanılmıştır [9,10].

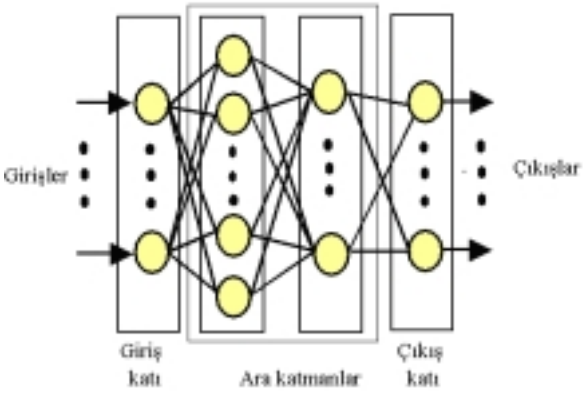
Bu çalışmada ilk defa bir dökümanda yazı dilinde kullanılan bütün karakterlerin, (noktalama işaretleri, sayılar, boşluk ve satır sonu karakterleri (enter), büyük harfler ve küçük harfler) YSA tabanlı bir kripto sistemiyle şifrelenmesi ve şifresinin çözülmesi işlemine tabi tutulduğu yeni bir şifreleme yöntemi sunulmuştur.

2. YAPAY SİNİR AĞLARI

Yapay sinir ağları (YSA) birçok disipline yeni çözümler sunan zeki bir yaklaşım olarak karşımıza çıkmaktadır. YSA'ların birçok farklı yapısı mevcut olup çok katlı perseptronlar (ÇKP), çeşitli alanlara uygulanmış bir YSA yapısıdır [11]. Genel olarak bir ÇKP YSA yapısı, Şekil 1'de gösterilmiştir. YSA üç kattan oluşur. Ara katta bir, iki veya daha fazla saklı tabaka bulunabilir. Giriş katındaki nöronlar tampon gibi davranırlar ve x_i giriş sinyalini ara kattaki nöronlara dağıtırlar. Ara kattaki her bir nöron j'nin çıkışı, kendine gelen bütün giriş sinyalleri x_i'leri takip eden bağlantı ağırlıkları w_{ji} ile çarpımlarının toplanması ile elde edilir. Elde edilen bu toplam, y_j'nin toplam bir fonksiyonu olarak hesaplanabilir ve

$$y_j = f\sum w_{ji}x_i \qquad (1)$$

şeklinde ifade edilebilir. Burada f basit bir eşik fonksiyonu, bir sigmoid veya hiperbolik tanjant fonksiyonu olabilir. Diğer katlardaki nöronların çıkışları da aynı şekilde hesaplanır.



Şekil 1. Bir ÇKP-YSA modeli

Burada ÇKP'ler, şifreleme ve şifre çözme işlevini yerine getirmektedirler. ÇKP'leri eğitmek için bir çok öğrenme algoritması kullanılabilir [11,12]. Bu çalışmada Levenberg-Marquardt öğrenme algoritması (LMA) kullanılmıştır [12].

Temel olarak LMA, maksimum komşuluk fikri üzerine kurulmuş bir hesaplama metodu olup Gauss-Newton ve Steepest-Descent algoritmalarının en iyi özelliklerinden oluşmuştur ve bu iki metodun kısıtlamalarını ortadan kaldırır [12]. Bu yaklaşımda, E(w) nin bir amaç hata fonksiyonu olduğu düşünülürse m tane hata terimi için $e_i^2(w)$ aşağıda verilmiştir.

$$E(w) = \sum_{i=1}^{m} e_i^2(w) = \|f(w)\|^2 \quad (2)$$

Bu eşitlikte $e_i(w) \equiv (y_i^{(t)} - y_i)$dir. LMA'da hedef, parametre vektörü w'nın, $E(w)$'nin minimum iken bulunmasıdır. LMA'nın kullanılmasıyla yeni ağırlık vektörü w_{k+1} bir önceki ağırlık vektör w_k'dan hesaplanır. Ağırlıklar

$$w_{k+1} = w_k + \delta w_k \quad (3)$$

ile güncelleştirilir ve bu ifadedeki δw_k ise aşağıdaki formülden hesaplanır.

$$(J_k^T J_k + \lambda I)\delta w_k = -J_k^T f(w_k) \quad (4)$$

Bu eşitlikte, J f'nin w_k ağırlığında Jakobiyeni, λ Marquardt parametresi ve I ise birim matrisdir. LMA aşağıdaki şekilde özetlenebilir:

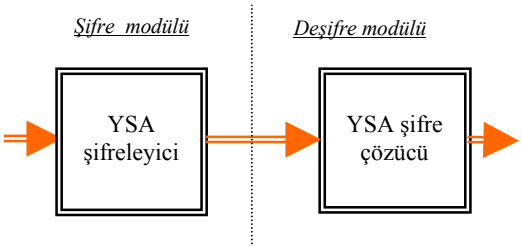
(a) $E(w_k)$'yı hesapla,
(b) küçük bir λ değeri ile başla
(c) w_k için eşitlik (4)'ü çöz ve E $(w_k + \delta w_k)$ değerini hesapla,
(d) şayet E $(w_k + \delta w_k) \geq E(w_k)$ ise λ'yı 10 kat arttır ve (c)'ye git,
(e) şayet E $(w_k + \delta w_k) < E(w_k)$ ise λ'yı 10 kat azalt, w_k: $w_k \leftarrow w_k + \delta w_k$'yi güncelleştir ve (c)'ye git.

Sonuçların elde edilmesi öğretim işlemine ağırlık dizisi w'ye bir başlangıç değerinin atanması ile başlar ve hataların kareleri toplamı e_i^2'nin hesaplanmasıyla devam eder. İşlemler bütün veri seti için tekrar tekrar uygulanır.

3. YSA ile KRİPTOLAMA

Bu uygulamada sunulan YSA ile kriptolama yaklaşımı için kullanılan sistem Şekil 2'de verilmiştir. Bu sistem iki YSA modülünden oluşmaktadır. Şifre modülü kısmında bulunan YSA ile şifreleme işlemi, deşifre modülü kısmında bulunan YSA ile şifre çözme işlemi gerçekleştirilmektedir.

Her bir modüle giriş ve çıkış olarak yazı dilinde kullanılan karakterler uygulanmıştır. Sıralı harflerden oluşan bir giriş setine karşılık, rasgele dizilmiş harflerden oluşan bir çıkış seti uygulanarak eğitim yapılmıştır. Bu karakterler 95 adet olup, noktalama işretleri, sayılar, boşluk ve satır sonu karakterleri (enter), büyük ve küçük harflerden oluşmaktadır.



Şekil 2. YSA ile kriptolama sistemi

Tek yönlü iletişim için şifreleme modülü göndericide, şifre çözme modülü de alıcıda bulunmalıdır. Eğer çift yönlü bilgi akışı yapılacaksa her iki modül de her iki tarafta bulunmalıdır. YSA modüllerini eğitmede maksimum 100 epok kullanılmıştır. Giriş ve çıkış katmanları arasında iki ara katman kullanılmış olup bu katmanlardan her ikisi de onaltı nörondan oluşmuştur. YSA'nın bu işlemde başarısını test etmek için 3 farklı eğitim seti kullanılmış ve her birinde tam sonuç elde edilmiştir.

Bu çalışmada YSA kullanılmasının en temel nedenlerden biri, sunulan şifreleme yöntemiyle şifrelenmiş mesajlara saldırılara karşı anahtarın mantıksal olarak yorumlanamayacak şekilde ağırlıklarda saklanmış olması ve bu ağırlıkların şifreleme tekniği ve şifrelenen mesajla ilgili en ufak bir bilgi taşımıyor olmasıdır. Anahtar bilgisinin bu şekilde anlaşılmayacak bir formatta ağırlıklarda tutulmasıyla şifreleme güvenliği artmakta , YSA'nın bu özelliği amaca uygun bir şekilde kullanılmakta ve bir kripto analistin pasif yolla bu kriptoyu çözmesi çok zorlaşmaktadır.

Kripto sistemi için anahtar görevi yapan yapay sinir ağı ağırlıklarından bazıları okuyucuların şifrelenmiş mesajın yorumlanmasının güçlüğünü görebilmeleri için Tablo 1'de verilmiştir.

W(i,j) ağırlık	[0 1.4763 0.47331 … 0.4641 -2.1672]
W(j,k) ağırlık	[-2.5826 2.7135..... 3.5863 3.8196]
W(k,l) ağırlık	[-1.0261 0.91151 .....-7.6996 3.9209]
b(j)bias ağırlık	[-2.9322;-1.5511;…. -2.0828; 0.55456]
b(k) bias ağırlık	[2.8; 4.33; -2.23; …….. 1.467; -4.3236]
b(l) bias ağırlık	[2.3386; -0.15817; ….; 1.2103; 5.3828]

Tablo 1. Şifrelemede anahtar olarak kullanılan YSA ağırlıkları

4. SONUÇLAR

Yazı dilinde kullanılan tüm karakterleri içerisine alan YSA tabanlı yeni bir şifreleme ve şifre çözme yaklaşımı bu çalışmada başarıyla sunulmuştur. Yapay sinir ağları kullanılarak yapılan çalışma sonucunda elde edilen sonuçlar hem şifreleme hem de şifre çözme işlemi için, sunulan yeni yaklaşımın başarılı olduğunu göstermiştir. YSA'nın bugüne kadar dezavantaj olarak bilinen ağırlıkların yorumlanamaması burada faydaya dönüştürülmüş ve amaca uygun bir şekilde kullanılmıştır.

Bir kripto analistin, burada sunulan yaklaşımla şifrelenmiş bir mesajı, mümkün olabilecek bütün kombinasyonları deneyerek çözmeye çalışması, 95!x8! adet farklı kombinasyonun denenmesini gerektirdiğinden binlerce yıl sürecek uzun ve zor bir iştir. Bu yüzden burada sunulan şifreleme yöntemi güvenli bir şifreleme yöntemidir.

Buna benzer çalışmaların ülkemizde yaygınlaşması, konuya ilgisi olan kişilere yeni ufuklar kazandıracak ve yeni şifreleme sistemlerinin geliştirilmesini sağlayacaktır. Böylelikle eğitime, bilime, ülke ekonomisine ve çıkarlarına katkılar sağlayacaktır.

KAYNAKLAR

[1] Menezes A. J. , Oorschot P. C. and Vanstone S. A. , Hanbook of Cryptografy, CRC Press,1997.

[2] Stinson D. : Cryptography; Theory and Practice, CRC Press Inc., 1996, 2nd edition.

[3] Koblitz N. , A Course in Number Theory and Cryptography, Springer, 1994, 2nd edition,

[4] Seberry J. and Pieprzyk J., Cryptography: An Introduction to Computer Security, Prentice-Hall,1989.

[5] The National Security Agency, http://www.nsa.gov/about_nsa/faqs_internet.html

[6] Keys to Secret Drawers: The Clipper Chip and Encryption, http://www.stardot.com/~lukeseem/j202/essay.html

[7] Cin İ. , Şifre sorgulamada yapay sinir ağlarının kullanılması, Master Tezi, Osman Gazi Üniversitesi,1996

[8] Tanrıverdi H. , Yapay Sinir ağlarının kriptolojide uygulanması, Master Tezi, Orta Doğu Teknik Üniversitesi,1993

[9] Sağıroğlu Ş. ,Demirayak N ve Baydar T., Şifreleme ve Deşifreleme için Yapay Sinir ağlarıyla Yeni Bir Yaklaşım, GAP IV. Mühendislik Kongresi (Uluslararası Katılımlı), 6-8 Haziran 2002, Vol.1, s.527-531, Şanlıurfa.

[10] Sağıroğlu Ş., Demirayak N. ve Baydar T. , Şifreleme ve Deşifreleme için Yapay Sinir ağlarıyla Yeni Bir Yaklaşım, Bilişim Kurultayı, oral sunum için kabul edildi.

[11] Haykin S., Neural Networks: A Comprehensive Foundation. ISBN 0-02-352761-7, Macmillan College Publishing Company, New York, USA, 1994.

[12] Pham D. T. and Sagiroglu S, Three methods of training multi-layer perceptrons to model a robot sensor. Int. J. of Robotica, Vol.13, 1995, pp.531-538.