Journal of the Faculty of Engineering and Architecture of Gazi University 32:1 (2017) 131-139

Mühendislik Mimarlık Fakültesi Dergisi
Journal of The Faculty of Engineering and Architecture of Gazi University

Elektronik / Online ISSN : 1304 - 4915
Basılı / Printed ISSN : 1300 - 1884

Dik eşleştirme arayış yöntemi ile hibrit veri sıkıştırma ve optiksel kriptografi

Ertan Atar[1, 2*], Okan K. Ersoy[3], Lale Özyılmaz[1]

[1]Yıldız Teknik Üniversitesi, Elektronik - Haberleşme Mühendisliği Bölümü, İstanbul, Türkiye
[2]Türk Telekomünikasyon A.Ş., İstanbul, Türkiye
[3]Purdue Üniversitesi, Elektronik - Bilgisayar Mühendisliği Bölümü, Indiana, ABD

Ö N E Ç I K A N L A R

- Sıkıştırılmış algılama (SA) ile hibrit optiksel kriptografi uygulaması
- Çift rastgale eşlenik anahtarlı DC3T dönüşümlü hibrit optiksel kriptografi edilmesi
- Data boyutu azaltma (sensör sayısı azaltma), güçlendirilmiş ve hibrit kriptografiye ulaşılması

Makale Bilgileri
Geliş: 29.11.2015
Kabul: 12.08.2016

DOI:
10.17341/gazimmfd.300602

Anahtar Kelimeler:
Sıkıştırılmış algılama, dik eşleştirme arayış algoritması, optiksel hibrit kriptografi, çift rastgale faz anahtar şifrelemesi, veri boyutu ve sensör azaltma

ÖZET

Sıkıştırılmış Algılama (SA) son zamanlarda veri boyutunun ve sensör sistemlerinin azaltılması gibi çok fazla uygulamayı mümkün kılmasından dolayı çok önemli bir araştırma alanı olmuştur. Datayı önce elde edip, onu sonra sıkıştırması yerine sıkıştırılmış algılamada veri, sıkıştırılmış formda işlem görmektedir. Bu uygulama sensör sayısının azaltılmasına neden olmaktadır. Bu çalışmada eş zamanlı sıkıştırılmış algılama ile yeni bir kriptografi uygulaması ve bu sayede haberleşme alanındaki önemli iki problem olan efektif/etkin/verimli işaret işleme ve bu işareti güvenli olarak iletme konularına alternatif çözüm araştırması amaçlanmıştır. Bu çalışmada sıkıştırılmış algılama için Dik Eşleştirme Arayış (DEA) algoritması kullanılmıştır. Daha sonra, hem sıkıştırma hem de şifreleme başarmak için SA-DEA algoritması ile çift rastgele faz şifreleme (DRPE) yöntemi birleştirilmiştir. Yüksek güvenlik elde etmek için sıkıştırılmış algılamada ve DRPE metodunda kullanılan anahtarlar alıcıya asimetrik kriptografi metodu ile iletilmiştir. DRPE simetrik optiksel şifreleme metodu olduğundan bu sebeple tüm kriptografik sistem, hibrit optiksel sistem (hem simetrik hem de asimetrik) olarak çalışmaktadır.

Hybrid data compression and optical cryptography with orthogonal matching pursuit

H I G H L I G H T S

- Hybrid optical cryptography application with compressive sensing
- Obtaining hybrid optical cryptography with DC3T transform with double-random conjugate keys
- Data size reduction (sensor number reduction), enhanced and hybrid optical cryptography reach

Article Info
Received: 29.11.2015
Accepted: 12.08.2016

DOI:
10.17341/gazimmfd.300602

Keywords:
Compressive sensing, orthogonal matching pursuit algorithm, optical hybrid cryptography, double random phase keys encyrption, data and sensor reduction

ABSTRACT

Compressive Sensing (CS), which makes it possible to reduce the amount of data and thereby to greatly simplify the sensor system has become a very important research area. In this method, data is compressed before measurements whereas data is first measured and then compressed in the current technology. This approach leads to reducing the number of sensors. In this study, simultaneous compressive sensing and hybrid optical cryptography is developed as a new approach to handle two important problems in the field of communications, namely, effective and efficient signal processing and secure transmission of information. In this work, CS is achieved with the orthogonal matching pursuit (OMP) algorithm. Then, the CS-OMP algorithm is combined with the double random phase encyrption (DRPE) method to achieve both compression and encyrption of data. In order to achieve high security, the keys used in CS and DRPE are transmitted to the receiver by an asymmetric cryptography method. Thus, the overall cryptographic system is a hybrid optical system (both symmetric and asymmetric) since DRPE is a symmetric optical encyrption method.

* Sorumlu Yazar/Corresponding author: ertan.atar@turktelekom.com.tr / Tel: +90 212 309 5095

1. GİRİŞ (INTRODUCTION)

Günümüz hayatında ses, görüntü, radar, video gibi birçok uygulamada kullanılan sinyaller genel olarak bir alanda seyrek veya sıkıştırılabilir işaretlerdir [1]. Sinyallerin sıkıştırılabilirliği kullanılarak birçok ölçümle elde edilen sinyal, bilgiyi içeren az sayıdaki dönüşüm katsayısıyla ifade edilebilmektedir. Sıkıştırılmış algılama (compressive sensing, CS) teorisi, seyrek olarak gösterilebilen sinyaller için bilgiyi içeren kısmın nasıl ölçümler kullanılarak geri elde edilebileceğini açıklamaktadır [2]. Sıkıştırılmış algılamadaki temel mantık, herhangi bir alanda seyrek (veya sıkıştırılabilir) olarak gösterilebilen bir sinyalin normale göre çok daha az sayıda rastgele doğrusal izdüşümlerle oluşturulan ölçümleri kullanarak sinyalin tekrardan geri dönüştürülmesidir. Bu geri dönüştürme için ilk olarak büyük boyutlu verideki bilgiyi içeren kısmı doğru bir şekilde çıkartabilecek algılama vektörlerinin oluşturulması ve daha sonra ise gözlem sonuçlarından veriyi doğru bir şekilde geri dönüştürecek yöntemlerin geliştirilmesi gerekmektedir [3]. Sıkıştırılmış algılamada doğru geri dönüşümün yapılabilmesi için gerekli ölçüm sayısı *(M),* sinyalin gösterildiği alandaki seyreklik derecesine *(K),* sinyal boyutuna *(N)* bağlıdır. Sıkıştırılmış algılamanın ölçüm sayısının ne derecede azaltılabildiği ve gerekli ölçüm sayısının kestirilebilmesi en önemli noktalardan biridir [4]. Literatürde ölçüm sayısı *(M)* ile ilgili birçok bağıntı kurulmuştur. Genel olarak kullanılan bağıntı en temel haliyle Eş. 1'deki bağıntıda belirtilmiştir [5].

$$M \geq (K \text{ x } log\ (N)) \tag{1}$$

Önerdiğimiz bu çalışmada, verimli sinyal işleme ve güvenlik konularını birleştirerek yeni bir eş zamanlı uygulama amaçlanmaktadır. Verimli sinyal işleme için sıkıştırılmış algılama ve güvenlik için simetrik, asimetrik ve hibrit kriptografi hedeflenmektedir. Tüm bu işlemler eş zamanlı olarak yapılmaktadır. Kriptografinin tanımına bakıldığında, bilginin şifrelenmesi ve şifrenin çözülmesi için kullanılan yöntemler olarak adlandırılmaktadır. Güvenilirlik, veri bütünlüğü, kimlik doğrulama gibi bilgi güvenliği konularıyla ilgilenen matematiksel yöntemler üzerine yapılan çalışmalar kriptografinin önemli konularıdır [5]. Bu çalışma ile, sıkıştırıcı algılama, 4f optik özelliği ve çift kompleks, rastgele ve dağıtılmış faz anahtarlarının beraber kullanılması sayesinde, hem veri boyutu azaltma (sensör sayısı azaltma) hem de hibrit optiksel kriptografi elde edilmiştir.

2. TEMEL BİLGİLER (FUNDAMENTAL INFORMATION)

2.1. Sıkıştırılmış Algılama Dik Eşleştirme Arayış Algoritması
(Compressive Sensing Orthogonal Matching Pursuit Algorithm)

Sıkıştırılmış Algılama (SA) ile klasik görüntü sıkıştırma yöntemlerinin verimli olmadığı sinyallerin veya görüntülerin istenen çözünürlüğünün çok altında bir sayıda örnek alınarak yeniden oluşturulabilmesi sağlanmaktadır [6]. Bu yöntemde büyük boyutlardaki bir x sinyali φ algılama matrisi yardımı ile orjinaline oranla daha küçük bir y vektörü içerisine toplanmaktadır. x sinyali, N uzunluğunda, ayrık, tek boyutlu bir sinyal (bilgi vektörü) olarak tanımlanmaktadır. Bu sinyalin k tane değeri sıfırdan farklıysa x sinyali k seyreklikte olarak ifade edilmektedir. Klasik örnekleme metodunda x sinyali $N * N$ boyutundaki birim matris olan ölçüm matrisi ile çarpılmaktadır. Böylece N tane ölçüm yapılarak $N * 1$ boyutunda gözlem vektörü elde edilmektedir. SA metodunda φ , sinyalin bütün bileşenlerini almak, yani N tane ölçüm yapmak yerine sadece M $(M<<N)$ tane doğrusal ölçüm yaparak sinyalin veri kaybına uğramadan geri elde edilebilmesini sağlamaktadır [7].

$$y=<x,\varphi> \tag{2}$$

$$y_k=<x,\varphi_k>,\ k=1,2,\ldots\ldots,m \tag{3}$$

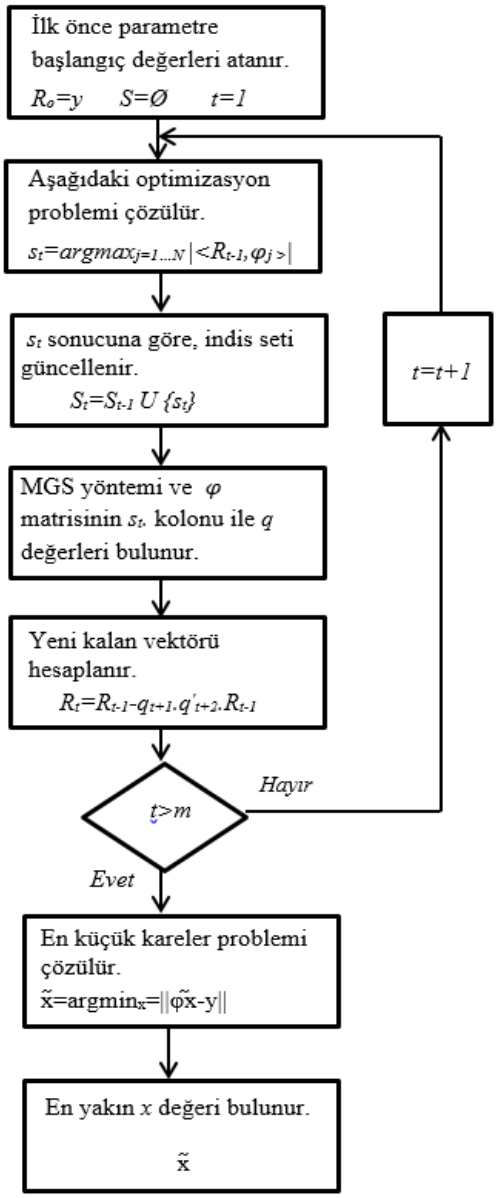
Eş. 2'de gösterildiği gibi x *ve* φ arasında tanımlanan vektörel iç çarpım sonucunda, Eş. 3'deki y ölçüm vektörü elde edilmektedir. Burada m sayıdaki ölçümler x sinyalinin boyu olan n değerinden çok daha küçük olmaktadır.

$$m<<n \tag{4}$$

Eş. 4'deki m sayıdaki ölçüm, sinyalin sıkıştırılabilme derecesini göstermektedir ve sıkıştırma oranı olarak adlandırılmaktadır. Sıkıştırma oranı sinyalin seyrekliği ile orantılıdır ve seyrek bir görüntüde sıkıştırma oranı Nyquist oranının altında bir değere ulaşabilmektedir [8]. Şekil 1'de verilen Dik Eşleştirme Arayış (Dik Eşleyen Takip) - (DEA) (Orthogonal Matching Pursuit) algoritması örnekleme matrisinin hangi bileşenlerinin sıfırdan farklı elemanlarıyla ilişkili olduğunu belirleyerek seyrek sinyali oluşturmaktadır [9]. DEA algoritması ölçüm sayısı olan *m, k* sayısına göre büyük olduğu sürece k-seyrek bir sinyalden yeniden oluşturma özelliğini başarılı bir şekilde yapabilmektedir. Bir x sinyali m seyrek bir sinyal ise, y ölçüm vektörüne etkisi bulunan φ örnekleme matrisinin m sayıda kolonunun bulunması gerekmektedir. İndis seti olarak adlandırdığımız S vektörü ilk adımda boş kümedir [10].

Algoritmanın her tekrarında y ölçüm vektörünün kalan kısmı ile en çok ilişkili örnekleme matrisi kolonu seçilmektedir [11]. R vektörünü kalan vektörü olarak adlandırılmasının sebebi algoritmanın tekrarlarında y ölçüm vektörüne etkisi bulunan φ örnekleme matrisinin s_t. kolonu R_t vektöründen çıkarılmasıdır. Buradaki s_t vektörü, φ algılama matrisi ile y ölçüm vektörü arasında en yüksek ilişkiye sahip vektörü temsil etmektedir. Modified Gram Schmidt (MGS) yöntemi kullanılarak kolonun y ölçüm vektörüne katkısı hesaplanır ve y vektöründen çıkartılmaktadır. En son aşamada ise, orjinal sinyal olan x vektörünün yaklaşık değeri, en küçük kareler denklemi çözülerek bulunmaktadır [12].

DEA programında hızlı fourier dönüşümü (HFD), ayrık kosinüs dönüşümü (AKD), gerçek sinusoidal dönüşümü (GSD), haar dalgacık dönüşümü, hadamard dönüşümü, ayrık sinus dönüşümleri(ASD) kullanılmıştır. Ayrıca sıkıştırılmış algılama dönüşüm matrisinde daha önce kullanılmayan ayrık kosinüs-III dönüşümü (AK3D) [13] de kullanılmıştır. Referans [13] de belirtildiği gibi AK3D, AKD ye göre daha az çarpma işlemi gerektirdiği için daha hızlı sonuç vermektedir. Dönüşümlerin kullanıldığı algılama matrisinde birbirine yakın satır ve sütunlardaki değerlerin yumuşak geçişler ve sıfıra yakın değerler olduğunda sonuçların daha iyi olduğu gözlenmiştir. Bu dönüşümler içerisinden süre ve doğruluk dikkate alındığında en iyi sonucu birbine yakın olarak, AK3D, akabinde sırasıyla AKD, HFD, GSD, ASD ve en kötü sonucu da hadamard ve haar vermektedir.



Şekil 1. Dik eşleştirme arayış algoritması
(Orthogonal matching pursuit algorithm)

2.2. Kriptografi (Cryptography)

Bir gönderici bir alıcıya açık ağlar üzerinden bir ileti göndermek istediği zaman, açık ağlardan gönderilen iletiler üçüncü şahıslar tarafından dinlenme ve değiştirilme tehdidi altındadırlar. Burada söz konusu ileti düz metindir. Bazı kullanımlarda plaintext adı da verilmektedir. Bir iletinin içeriğini saklamak üzere yapılan gizleme işlemi de şifrelemedir (encryption). Bu işlem düz metini şifreli metine dönüştürmektedir. Bilginin içeriği başkalarının anlamayacağı hale gelmektedir. Bu bilgi bir yere iletilmek amacıyla şifrelenen bir mesaj veya saklanmak amacıyla şifrelenen bir bilgi olabilir. Şifrelenmiş bir ileti şifreli metindir (ciphertext). Şifreli metini düz metine geri çevirme işlemi şifre çözümüdür (decrypt) [14]. Simetrik şifreleme algoritmaları, şifreleme ve şifre çözme işlemleri için aynı anahtarı kullanır. Gizli veri alışverişi yapacak kişi veya uygulamalar simetrik anahtarı kendi aralarında, emniyetli bir şekilde değiştirmelidir [15]. Simetrik şifreleme, oldukça hızlıdır ve elektronik cihazlarda uygulamak çok daha kolaydır. Asimetrik şifrelemede ise iki farklı anahtara dayalı şifreleme sistemi kullanılmaktadır. Bu sistemde bir tane şifreleme için genel anahtar ve bundan farklı olarak bir tanede şifre çözmek için özel anahtar bulunmaktadır [16]. Asimetrik şifreleme algoritmalarında çok büyük asal sayılar kullanılmaktadır. 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. Asimetrik kriptografi için RSA algoritması kullanılmıştır. RSA algoritması büyük asal sayılar modüler aritmetiğine dayanmaktadır [17].

Asimetrik RSA algoritması aşağıda verilmiştir.

• P ve Q gibi çok büyük iki asal sayı seçilir.
• Bu iki asal sayının çarpımı $N = P.Q$ ve bu bir eksiklerinin $\varphi(N)=(P-1).(Q-1)$ hesaplanır.
• 1'den büyük $\varphi(N)$'den küçük $\varphi(N)$ ile aralarında asal bir E tamsayısı seçilir.
• Seçilen E tamsayısının *mod* $\varphi(N)$'de tersi alınır, sonuç D gibi bir tamsayıdır.
• E ve N tamsayıları genel anahtarı, D ve N tamsayıları ise özel anahtarı oluşturur.

M açık mesajını şifrelemek için; Eş. 5'deki işlem uygulanır.

$$C=M^E \bmod N \quad (5)$$

C şifreli mesajı çözmek için; Eş. 6'daki işlem uygulanır.

$$M=C^D \bmod N \quad (6)$$

Simetrik ve asimetrik şifrelemenin beraber uygulamasına ise hibrit kriptografi denilmektedir. Hibrit Kriptografi, simetrik ve asimetrik şifrelemenin dezavantajlarını giderir, avantajlarını artırmaktadır [18].

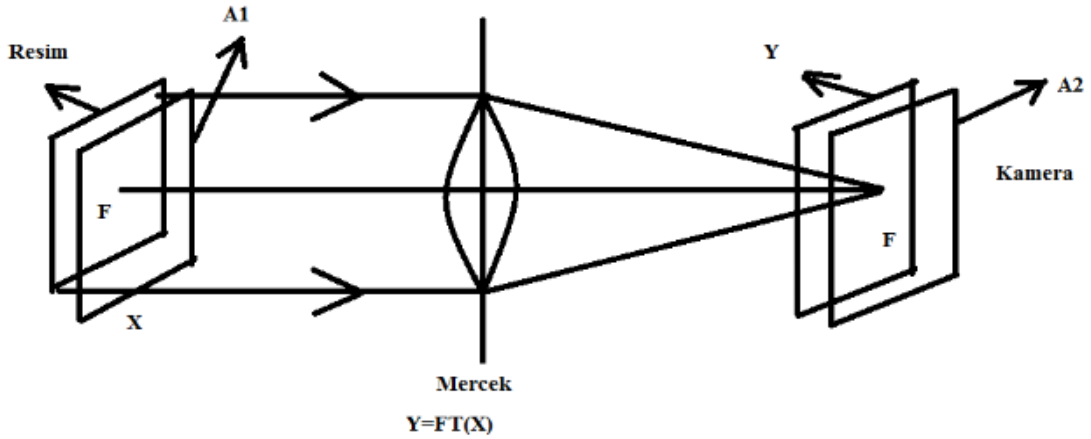
2.3. Önceki Yapılan Çalışmalar (Previous Studies)

Dataların şifreleme üzerine bazı algoritmalar önerilmiştir. Amir ve Esther tarafından [19] de belirtilen çalışmada, EEG işaretini ölçüm vektöründe boyut sıkıştığı için şifrelenmiş işaret olarak kullanılacağını öne sürülmektedir. Herhangi bir kriptoanaliz çalışması yapılmamıştır. Minal ve Rajankar'ın [20] deki uygulamada, algılama matrisinin satırları ve sütunları yer değiştirilerek şifreleme yapılmıştır. Şekiller bozuk olarak geri elde edilmiştir. Kriptoanaliz uygulaması belirtilmemiştir. Rachlin ve Baron tarafından [21] da belirtilen ve Dwork, McSherry ve Talwar tarafından [22] de belirtilen çalışmalarda sıkıştırıcı algılamanın Nyquist teoreminin aksine data güvenliği, şifreleme konusunda da kullanabileceğini öne sürmüştür. Burada şifreleme ve şifre çözme için algılama matrisinin kullanabileceğini açıklamışlardır. Örsdemir, Altun ve Sharma tarafından [23] deki çalışmada rastgele üretilen algılama matrisinin şifrelemedeki anahtar görevini üstlenebileceği belirtilmektedir. Ramezani, Seyfe ve Bafghi tarafından [24] de belirtilen çalışmada, ölçüm sayısı (M) ve seyreklik derecesi (K) için M>2K özelliğini sağlaması şartıyla algılama matrisinin şifreleme ve şifre çözmede kullanabileceğini göstermişlerdir. Zhang, Wong, Xiao ve Li tarafından [25] deki çalışmada, iki adet algılama matrisi kullanarak simetrik şifreleme ve şifre çözme uygulaması gerçekleştirilmiştir. Zhang, Ren, Feng ve Qian tarafından [26] deki çalışmada, algılama matrisinde iki farklı transform ile şifreleme ve şifre çözme işlemi uygulanmıştır. Mo, Zhang, Zheng ve Zhou tarafından [27] de belirtilen çalışmada, algılama matrisinde hadamard matrisi kullanılarak şifreleme ve şifre çözme anlık yapılacağını göstermişlerdir. Atar, Ersoy ve Özyılmaz tarafından [28] de sıkıştırıcı algılama ile simetrik şifreleme uygulaması yapılmıştır. Abdulghani, Rodriguze ve Villegas, sıkıştırılmış algılama ile şifrelemenin ne kadar zor kırılabileceğini göstermiştir [29]. Ayrıca Çavuşoğlu, Uyaroğlu ve Pehlivan tarafından kaotik haberleşme ile ilgili kaotik gizleme, kaos kaymalı anahtarlama, kaos modülasyonu gibi farklı kodlama ve kod çözme yöntemleri uygulaması yapılmıştır [30]. Uğur ve Soğukpınar tarafından eşleme tabanlı kriptografi uygulaması gerçekleştirilmiştir. Bu uygulamanın altındaki temel fikir, iki kullanışlı kriptografik grup arasında problemler arası indirgemeye dayanan ve yeni kriptografik şemalar oluşturmaya izin verebilecek bir denklik ilişkisi inşa etmektir [31]. Erdem ve Kocaoğlu tarafından ağ güvenliği ve ataklar incelenmiştir [32]. Dener tarafından web ve veri tabanı sunucusu kullanılarak kablosuz algılayıcı ağlarda ortamda bulunan algılayıcı düğümlerin, ortamdan elde ettikleri sıcaklık, nem, ışık değerlerinin 128 bitlik şifrelenerek web ve mobil ortam üzerinden analiz edilebilmesini, görselleştirilmesini sağlayan güvenli bir izlemi sistemi geliştirilmiştir [33].

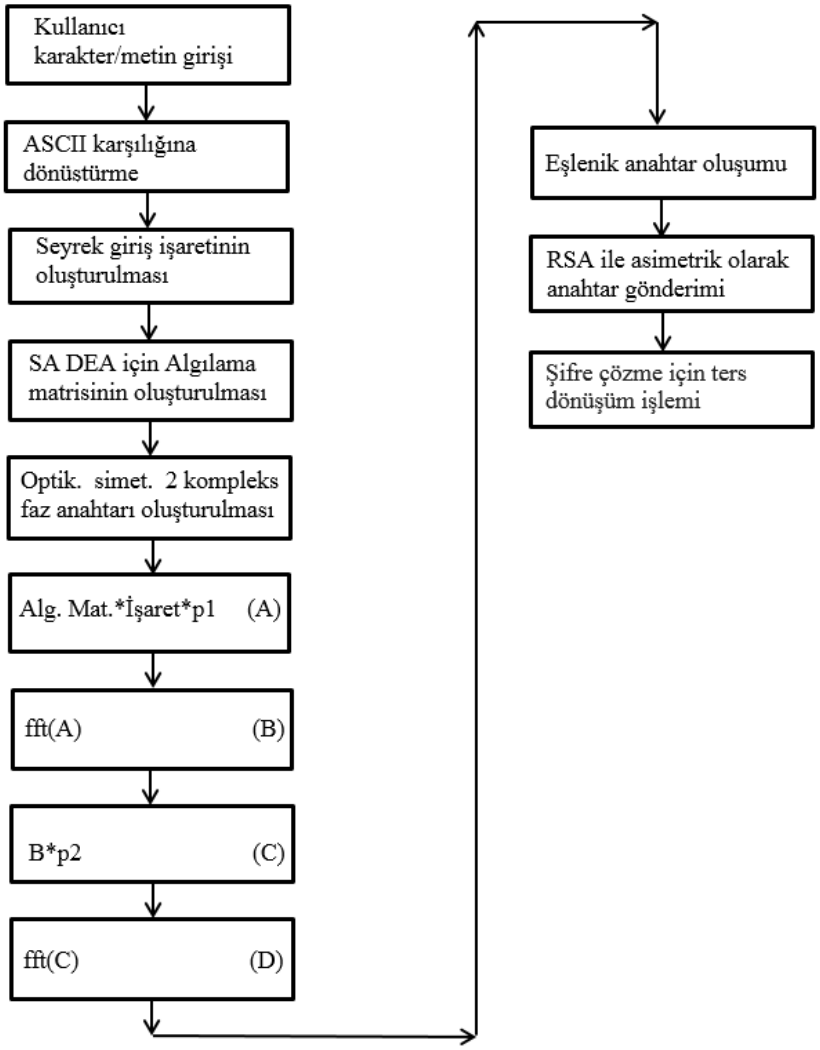
3. SONUÇLAR VE TARTIŞMALAR (RESULTS AND DISCUSSIONS)

Önerilen uygulamada, eş zamanlı sıkıştırılmış algılama ile optiksel hibrit kriptografi geliştirilmiş ve simetrik kriptografi anahtarlarının daha güvenli olması için karşıya asimetrik kriptografi ile taşıma işlemi yapılmıştır. Asimetrik kriptografi için RSA algoritması kullanılmıştır. RSA algoritmasının temelinde büyük asal sayıların modüler aritmetiği bulunmaktadır.

Bu çalışmada sıkıştırılmış algılama dik eşleştirme arayış (SA-DEA) algoritması ve algılama matrisinin içine gizlenmiş bir şekilde kullandığımız çift rastgele faz anahtarları ile hem sıkıştırma (data boyutu azaltma) hem de simetrik, asimetrik ve hibrit optiksel şifreleme ve deşifreleme uygulaması eş zamanlı olarak gerçekleştirilmiştir. Dışarıdan girilen tüm karakterler giriş (orijinal) işaret olarak kabul edilmektedir. ''1'' bağıntısına göre seyrek sinyali elde edilmektedir. *K* seyreklik derecesi olarak kullanıcının dışarıdan girdiği karakter sayısı alınmaktadır. Programda, permütasyon matrisleri ile beraber algılama matrisi elde edilmektedir, bu algılama matrisi oluşturulurken, hızlı Fourier dönüşümü (HFD), ayrık kosinüs dönüşümü (AKD), gerçek sinusoidal dönüşümü (GSD), Haar dalgacık dönüşümü, Hadamard dönüşümü ve ayrık sinus dönüşümleri (ASD) kullanılabilirliği kanıtlanmış ve en iyi dönüşüm araştırılmıştır. İlave olarak daha önce kullanılmayan ayrık



Şekil 2. Optiksel şifreleme, 2-f optik şifreleme (Optical encryption, 2-f optic encryption)

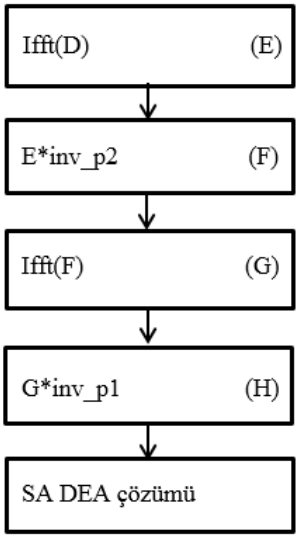


Şekil 3. Önerilen uygulamanın akış diyagramı (Recommended application flow diagram)

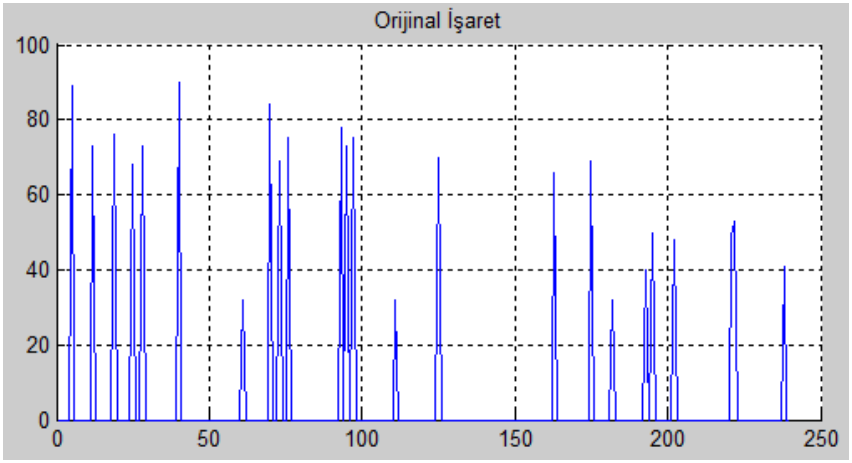
kosinüs-III dönüşümü de (AK3D) kullanılmaktadır. Algılama matrisi her çip teknolojisinde kullanılabilmesi ve giriş işaretinin durumu sonucu değiştirmemesi için oluşturulan algılama matrisi giriş işaretinden bağımsız olarak oluşturulmaktadır. Kriptografinin güçlü olması için optiksel p1 ve p2 faz anahtarları kompleks rastgele sayılardan oluşmaktadır. Bu çift rastgele faz şifrelemesinde kompleks sayıların kullanılması iyi saçılma sağlamaktadır. Saçılma sayesinde şifrelemenin güvenliği daha da artmaktadır. Ayrıca bu kompleks sayıların 360 derece tam yayılması için p1 faz anahtarını 2π ile çarpma işlemi yapılmaktadır. Saçılmayı daha da arttırmak ve şifrelemeyi daha zorlaştırmak için 2π ile çarpılmış p1 faz anahtarını tekrar kompleks ve 2π ile çarpılmış rastgele sayılardan oluşan optiksel ikinci bir p2 faz anahtarı kullanılmaktadır. Böylece optiksel kaynaklı çift rastgale faz şifreleme işlemi (DRPE metodu) yapılmış olmaktadır. Şekil 2'de optiksel şifreleme gösterilmiştir. Orijinal optiksel şifrelemede (4-f optical processor) iki mercek kullanılmıştır. Böylece örnek giriş işareti tamamen gürültü görüntülü olmaktadır. Asimetrik kriptografinin uygulanabilmesi için iki rastgale faz kompleks anahtarın reel ve imajiner kısımları ayrılmıştır ve RSA ile asimetrik olarak anahtarlar alıcıya gönderilmiştir. Alıcı da ise bu gelen anahtarları kullanarak simetrik olarak sıkıştırılmış algılama dik eşleştirme arayış algoritması ile şifre çözümü ve orijinal işaret elde edilmektedir.

Şekil 3 ve Şekil 4'de önerilen yöntemin akış diyagramları verilmiştir. Önerilen bu uygulama incelendiğinde şifrelenmiş işaret orijinal işarete göre çok daha fazla karmaşık ve gürültü görüntülü olmaktadır. Böylece şifrelemenin güvenirliği artmaktadır. Algoritma diğer farklı girişler için de doğru olarak çalışmaktadır.

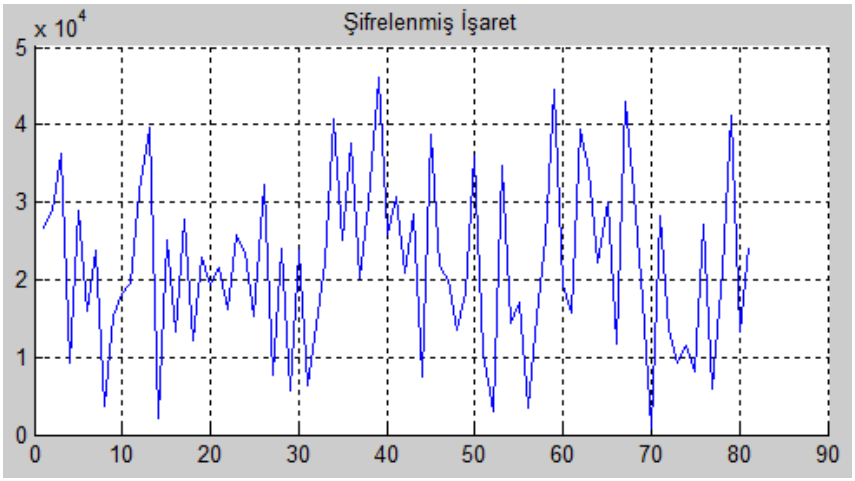
Şekil 5, 6, 7 ve 8 de yatay eksen işaretin uzunluğunu, dikey eksen ise işaretin ASCII karşılığını göstermektedir. Şekil 9'deki eksenler, kompleks faz anahtarların i ve j eksen çizimlerini göstermektedir. Şekil 5'de giriş işaretinin ASCII karşılığı verilmektedir.



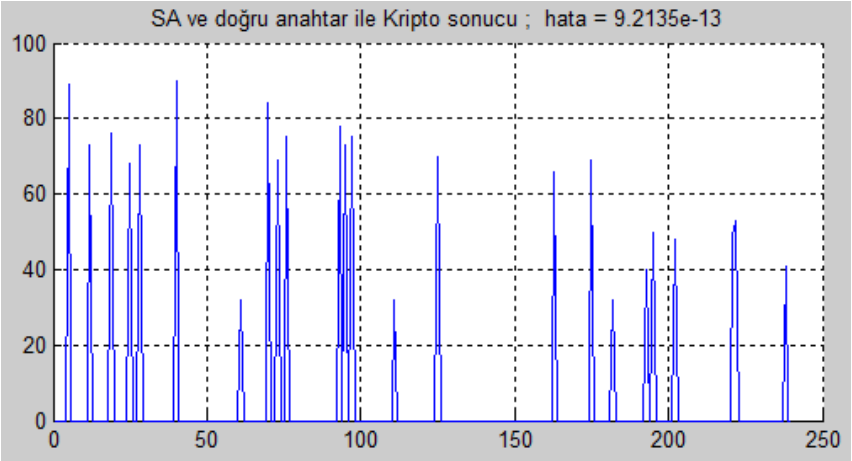
Şekil 4. Şifre çözme için ters dönüşüm akış diyagramı (Inverse transform flow diagram for he decryption)



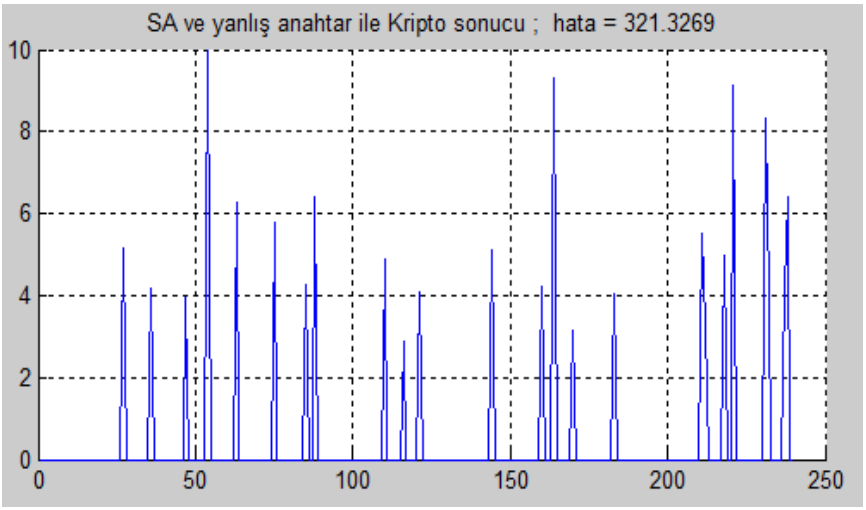
Şekil 5. Orijinal işaret (Original sign)



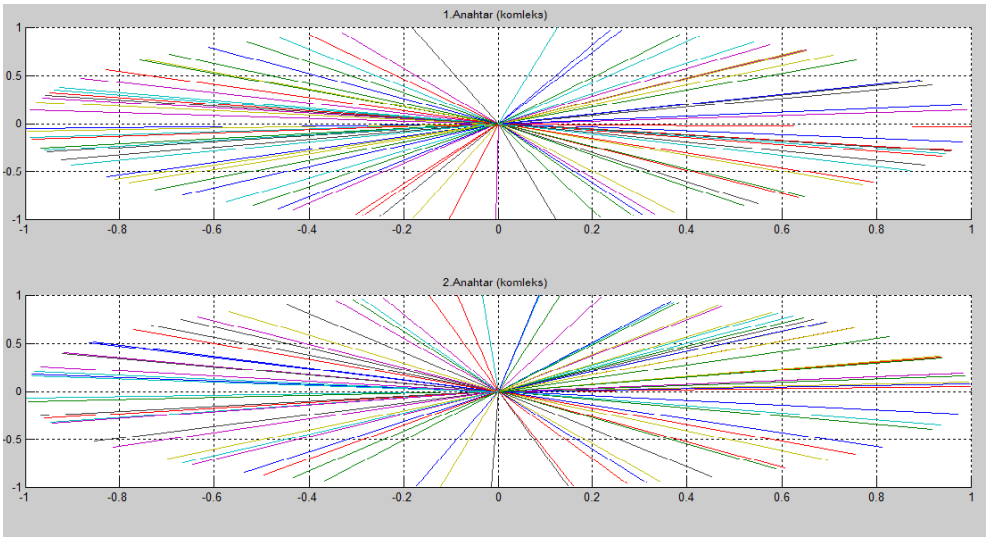
Şekil 6. Şifrelenmiş işaret (Encryted sign)



Şekil 7. Sıkıştırılmış algılama ve doğru anahtarlar ile kriptografi sonucu
(Compressive sensing and crypto result with correct keys)



Şekil 8. Sıkıştırılmış algılama ve yanlış anahtarlar ile kriptografi sonucu
(Compressive sensing and crypto result with wrong keys)



Şekil 9. Optiksel iki faz anahtarları (optical two phase keys)

Şekil 6'de girişe göre oluşturulan seyrek işaretin ASCII karşılığı için orijinal ve şifreli işaret, Şekil 7 ve Şekil 8'de doğru ve yanlış anahtar sonuçları gösterilmektedir. Bu şekillere bakıldığında şifreli işaretin orijinal işaret boyutundan çok daha küçük olduğu ve çok karmaşık olduğu görülmektedir. Doğru anahtarlar ile alıcıda aynı orijinal işaret elde edilmekte, yanlış anahtarlar ise orijinal işaretten tamamen farklı bir işaret elde edilmektedir. Son olarak Şekil 9'da ise kompleks, rastgele ve 360 derece tam dağıtılmış şifrelemede ve şifre çözmede kullanılan 2 faz anahtarları görülmektedir.

4. SONUÇLAR (CONCLUSIONS)

Önerilen bu algoritmada, sıkıştırılmış algılama ile optiksel kaynaklı DRPE metodu hibrit kriptografi uygulaması eş zamanlı olarak başarılı bir şekilde gerçekleştirilmiştir. Referans [34] de belirtilen saldırıda sıkıştırılmış algılama kullanılmadığı için şifrelenmiş işaret ile orijinal işaret boyutu aynı olmaktadır, ancak önerilen uygulamada sıkıştırılmış algılama kullandığı için şifrelenmiş işaret orijinal işaretten çok daha küçük boyutta olmaktadır. Ataklar karşısında ayrıca şifrelenmiş işaret bilinmiş olsa bile önerilen yöntemde kullanılan farklı adımlardaki eşlenik faz anahtarları ve ters fft dönüşümleri sayesinde iki rastgele faz anahtarı bulunamamaktadır, bu da şifrelenmiş işareti ataklara karşı çok daha fazla koruyucu yapmaktadır. Ayrıca şifrelenmiş işaret, orijinal işarete göre boyutu daha az olduğu (boyut 2/3 oranında azalmaktadır) için verimli ve efektif data transferi olmaktadır. Önerilen bu algoritma hızlı FFT türü dönüşümler sayesinde çok hızlı çalışmaktadır. Referans [13] de belirtilen AK3D dönüşümü, AKD'ye göre daha az çarpma işlemi içerdiğinden diğer dönüşümlere göre en hızlı sonucu vermektedir. Ayrica AK3D doğruluk ve süre açısından en iyi sonucu vermektedir. En hızlı iki dönüşümün ortalaması alınarak kıyaslamasında; AKD ile işlem süresi: 0.915616 saniye. Hata: 2.24e-13, AK3D ile işlem süresi: 0.265875 saniye. Hata: 1.02e-13 değerleri elde edilmiştir. Bu uygulama ile sıkıştırılmış algılama dik eşleştirme arayış yöntemi ve DRPE metodu optiksel kriptografi iç içe kullanılmış, böylece hem sıkıştırılmış algılama ile data boyutu azaltma (sensör sayısı azaltma) hem de SA algılama matrisinde güçlendirilmiş optiksel iki defa kompleks faz şifreleme ve şifre çözme ile güvenliği artırılmış hibrit kriptografi (simetrik ve asimetrik) içeren tüm işlemler eş zamanlı olarak elde edilmiştir.

KAYNAKLAR (REFERENCES)

1. Candès E., Romberg J., Tao T., Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information, IEEE Trans. on Information Theory, 52 (2), 489-509, 2006.
2. Donoho D., Compressed sensing, IEEE Trans. on Information Theory, 52 (4), 1289 - 1306, 2006.
3. Donoho D., Chen, S., Saunders, M., Atomic decomposition by basis pursuit, SIAM Journal on Scientific Computing, 20 (2), 33-61, 1998.
4. Karakuş K., Programlanabilir donanım üzerinde sıkıştırıcı algılama ile görüntü yeniden oluşturma algoritmasının tasarımı, Yüksek Lisans Tezi, Ankara Üniversitesi, Fen Bilimleri Enstitüsü, 2011.
5. Krishnamurthy M., Seagren E.S., Alder R., Bayles A.W., Burke J., Carter S., Faskha E., Basics of Cryptography and Enryption, How to Cheat at Securing Linux, Syngress Publishing, Inc., Elsevier, Inc., 30 Corporate Dr., Burlington, MA 01803, 2008.
6. Septimus A., Steinberg, R., Compressive sampling hardware reconstruction, International Symposium on Circuits and Systems, 35 (3), 3316-3319, 2010.
7. Baraniuk R., Compressive sensing, IEEE Signal Processing Magazine, 24 (4), 118-121, 2007.
8. Borghi A., Darbon J., Peyronett S., Chan T., Osher S., Compressive sensing algorithm for parallel many-core architectures, Journal of Signal Processing Systems, 7 (1), 1-20, 2013.
9. Donoho D., Stark, P. B., Uncertainty principles and signal recovery, SIAM, J. Appl. Math., 49 (3), 906-931, 1989.
10. Candès E., Wakin, M., An introduction to compressive sampling, IEEE Signal Processing Mag., 25 (2), 21-30, 2008.
11. Satheesh B., Deepa B., Subhadra B, Devi S., Compressive Sensing for Array Signal Processing, India Conference (INDICON), India, 104-108, 7-9 Aralık, 2012.
12. Tropp J., Gilbert A.C., Signal recovery from partial information via orthogonal matching pursuit, IEEE Trans. Inform. Theory, 53 (12), 4655-4666, 2007.
13. Ersoy O. K., Nouira A., Image coding with the discrete cosine-III transform, IEEE Journal On Selected Areas In Communications, 10 (5), 21-45, 1992.
14. Herranz J., Identity-based ring signatures from RSA, Theoretical Computer Science, 89 (2), 100-117, 2007.
15. Ham L., Ren J., Efficient identity-based RSA multisignatures, Computer & Security, 27 (2), 12-15 March 2008.
16. Menezes A. J., Oorschot P. C., Vanstone S. A., Handbook of applied cryptography, Boca Raton: CRC Press, ISBN: 0-8493-8523-7, 1997.
17. Bellovin S.M., Cryptography and the internet, 18th Annual International Cryptology Conference Santa Barbara, California, USA, 107-111, 23–27 Ağustos, 1998.
18. Schneier B., Applied cryptography - Protocols, Algorithms and Source Code in C, John Wiley & Sons, Inc., 2nd edition, 1996.
19. Amir M. A., Esther R., Compressive sensing: From compressing while sampling to compressing and securing while sampling, 32nd Annual International Conference of the IEEE EMBS Buenos Aires, Argentina, 7-11, 31 Ağustos-4 Eylül, 2010.
20. Minal C., Rajankar S., Study the effects of encryption on compressive sensed data, International Journal of Engineering and Advanced Technology, 2 (5), 2249-8958, 2013.
21. Rachlin Y., Baron D., The secrecy of compressed sensing measurements, In:Proceedings of the 46th annual allerton conference on communication, control,

and computing, Monticello, Illinois, 813–17, 23-26 Eylül, 2008.

22. Dwork C., McSherry F., Talwar K., The price of privacy and the limits of LP decoding, Proceedings of the 39th Annual ACM Symposium on Theory of Computing, San Diego, California, USA, 85-94, 11-13 Haziran, 2007.

23. Örsdemir A., Altun H., Sharma G., On the security and robustness of encryption via compressed sensing, In: Proceedings of the IEEE military communications conference, San Diego, California, 16-19 Kasım, 2008.

24. Ramezani M., Seyfe B., Bafghi H.G., Perfect secrecy via compressed sensing, Communication and Information Theory, Tahran-İran, 1-5, 8-9 Mayıs 2013.

25. Zhang Y., Wong K., Xiao D., Zhang L.Y., Li M., Embedding cryptographic features in compressive sensing, Cryptography and Security, Information Theory, Neurocomputing, 205 (3), 472-480, 2015.

26. Zhang X., Ren Y., Feng G., Qian Z., Compressing encrypted image using compressive sensing, Intelligent information hiding and multimedia signal processing, 2011 Seventh International Conference on, Dalian-Çin, 222 – 225, 14-16 Ekim, 2011.

27. Yan M., Zhang A., Zheng F., Zhou N., An image compression-encryption algorithm based on 2-D compressive sensing, Journal of Computational Information Systems, 9 (24), 57-64, 2013.

28. Atar E., Ersoy O., Özyılmaz L., Sıkıştırıcı algılama dik eşleştirme arayış yöntemi ile kriptografi, Signal Processing and Communications Applications Conference (SIU), 2015 23th, Malatya Üniversitesi, Malatya, 216-219, 16-19 Mayıs 2015.

29. Abdulghani A., Rodriguze-Villegas E., Compressive sensing: from compressing while sampling to compressing and securing while sampling, In: Proceedings of the 32nd annual international conference of the IEEE engineering in medicine and biology society, Buenos Aires-Argentina, 1127–30, 1-4 Eylül, 2010.

30. Çavuşoğlu Ü., Uyaroğlu Y., Pehlivan İ., Design of a continuous-time autonomous chaotic circuit and application of signal masking'', Journal of the Faculty of Engineering and Architecture of Gazi University, 29 (1), 79-87, 2014.

31. Uğur A., Soğukpınar İ., Sustainable authorization in enterprise workflow and authorized digital signature model, Journal of the Faculty of Engineering and Architecture of Gazi University, 29 (3), 559-568, 2014.

32. Erdem O.A., Kocaoğlu R., A new approach for network security: dynamic intelligent firewall architecture, Journal of the Faculty of Engineering and Architecture of Gazi University, 29 (4), 707-715, 2014.

33. Dener M., A secure monitoring system design for wireless sensor networks, Journal of the Faculty of Engineering and Architecture of Gazi University, 29 (4), 745-754, 2014.

34. Peng X., Zhang P., Yu B., Wei H., Known-plaintext attack on optical encryption based on double random phase keys, Optics Letters, 31 (8) 15-23, 2006.