

KAOS TABANLI SAYISAL CSK VE DCSK MODÜLASYON TEKNİKLERİNİN MATLAB/SİMULİNK ORTAMINDA GERÇEKLEŞTİRİLMESİ

Hidayet OĞRAŞ

Batman Üniversitesi
Teknik Eğitim Fakültesi
Elektrik Eğitimi Bölümü
hidayet.ogras@batman.edu.tr

Mustafa TÜRK

Fırat Üniversitesi
Mühendislik Fakültesi
Elektrik-Elektronik Mühendisliği Bölümü
mturk@firat.edu.tr

Sezgin OĞRAŞ

Dicle Üniversitesi
Fen Edebiyat Fakültesi
Matematik Bölümü
sezginogras@hotmail.com

ÖZET

Bu çalışma, kaosu haberleşme sistemleri içerisindeki uygulama alanını ve kaos tabanlı haberleşme sistemlerindeki sayısal modülasyon ve demodülasyon tekniklerini içermektedir. Bunun yanında, kaotik haberleşme sistemlerine genel bir bakış ve bu sistemlerde özellikle üzerinde çalışılan modülasyon tekniklerinden: Kaos Kaydırmalı Anahtarlama (CSK) ve Farksal Kaos Kaydırmalı Anahtarlama (DCSK) yapıları anlatılmakta ve güvenli veri iletişimi bu tekniklerin kullanılabilirliği verilmektedir. Bu anlamda, bu çalışmada yer alan bilgiler ele alındığında, bilinen analog ve sayısal haberleşme tekniklerine alternatif olarak bu alana yeni bir yaklaşım getirmektedir. Ayrıca kaotik haberleşme sistemlerinin bilinen haberleşme sistemlerine göre avantajları, bu sistemlerde taşıyıcı olarak kullanılan kaotik sinyalin elde edilişi ve analizi ve son olarak kaos tabanlı sayısal modülasyon ve demodülasyon tekniklerine ait sonuçlar MATLAB/Simulink ortamında grafiksel olarak incelenmektedir.

Anahtar Kelimeler: Kaotik Haberleşme, Kaotik Modülasyon, Kaos Kaydırmalı Anahtarlama, Farksal Kaos Kaydırmalı Anahtarlama

1. GİRİŞ

Bilgi güvenliğinin esas olduğu günümüz teknolojisinde, güvenliğe verilen önem her geçen gün artmaktadır. Özellikle haberleşme sistemlerine olan ihtiyaç ve bağımlılık giderek artmakta ve bunun sonucunda da bilginin güvenli bir şekilde iletilmesi sorun olmaya başlamıştır. Bu durum araştırmacıları, bilinen tekniklerin dışında haberleşmede değişik güvenlik önlemleri almaya yöneltmiştir.

Telekomünikasyon hizmetine olan talebin artması, çok fazla sayıda kullanıcı oluşturmuştur. Kullanılan dar bantlı iletişim sinyalleri çok yönlü yayılıma karşı duyarlıdır ve yüksek oranda gönderilen güç spektrum yoğunluğu diğer kullanıcılar için parazit oluşturmaktadır [1].

Bazı uygulamalarda mevcut bant genişliğinin en verimli şekilde kullanılması önemliyken, bazı uygulamalarda ise bant genişliğinin sınırlı olduğu geniş bant haberleşme tekniğinin kullanılması önemlidir. Her bir kullanıcının, diğer kullanıcılar için parazit oluşturduğu böyle bir ortam için en uygun yöntem, kullanılan haberleşme sinyalinin mümkün olduğunca geniş bantlı olması gerekir. Geniş bantlı haberleşme sinyali iki yol ile oluşturulabilir: Yayılı Spektrum (Spread Spectrum) tekniği kullanılarak bilgi sinyalinin geniş bant

aralığı üzerinde yayılması; ya da her bir sembolün gürültü benzeri dalga biçimi ile temsil edilmesi gerekir. Günümüzde bu probleme yönelik bilinen çözüm birinci yaklaşımı kullanmaktadır [1-2]. Ancak yayılı spektrum tekniğinin kullanılması karmaşık bir sistemi gerektirmekle beraber alıcı-verici devrelerde mükemmel bir senkronizasyonun olması gerekir. Senkronizasyon hatası performans kaybına yol açarken ayrıca sistemin karmaşıklığı fazla güç tüketimine sebep olur. Kaotik haberleşme, bu gibi problemlerin çözümü için yeni bir alandır [3-4].

2. KAOTİK HABERLEŞME

İkinci yaklaşım referans alınarak ve bu çalışmada da kullanılan: gönderilecek bilgilerin periyodik taşıyıcı fonksiyonların toplamı şeklinde değil de kaotik taşıyıcılar ile temsil edilmesi bu duruma alternatif olabilecek bir diğer çözümdür.

Kaos ve kaotik sistem dinamiği ile ilgili birçok çalışma alanı mevcuttur. Kaotik sistemlerin önemli uygulama alanlarından biri de haberleşmedir. Son zamanlarda birçok araştırmacı haberleşme sistemlerinde kaosu karakteristik özelliklerinden yararlanmak için çalışma yolları geliştirmişler ve kayda değer başarılı sonuçlar elde etmişlerdir [1].

Haberleşme sisteminin bu alanı Kaotik Haberleşme olarak adlandırılır [5].

Kaotik sinyaller büyük bant genişliğine ve düşük güç spektrum yoğunluğuna sahip olmalarının yanında çok basit devreler ile herhangi bir frekans bandında elde edilebilir [5-7]. Kaotik sistemlerin güvenli haberleşmeye uygulanışı fikri, Pecora ve Carroll'un kaotik sistemlerin senkronizasyonu ile ilgili sunumuyla ortaya çıkmıştır [8].

Pratikte sadece analog haberleşme kanalları mevcuttur. İletilecek olan bilgi sayısal olsa bile bu bilginin analog bir sinyal ile temsil edilip yollanması gerekir [2]. Bilinen haberleşme sistemlerinde, örnekleme fonksiyonları kanal içinde sinüzoidal dalgaların toplamı şeklinde ve doğrusal olarak gönderilirken, kaotik haberleşmede ise her bir veri, kaotik üreteçler tarafından sağlanan kaotik sinyal parçası ile ifade edilir [7].

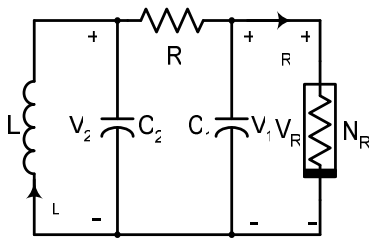
Kaotik taşıyıcı ile sinüzoidal taşıyıcı arasındaki temel fark verilen sembol için örnekleme fonksiyonu kararsızdır ve periyodik değildir. Dolayısıyla aynı bilgi tekrar tekrar yollansa bile bu bilgiyi temsil eden kaotik sinyal hiçbir zaman aynı olmaz. Ayrıca kaotik taşıyıcılar geniş bantlı olmasından dolayı sinüs sinyaline göre çok yönlü yayılıma karşı daha dirençlidir [2, 5].

Farklı bit enerjisine sahip kaotik taşıyıcılar farklı kaotik devrelerden ya da farklı sabit sayılarla çarpılmış aynı kaotik devreden de elde edilebilir [2]. Alıcı tarafta demodülatör devresi gelen sinyalin bit enerji değerini hesaplayarak eşik değer seviyesine göre gönderilen bilgi elde edilebilir [7].

Kaotik sinyal üretici olarak literatürde en çok kullanılan ve tercih edilen kaotik devre modeli ise basit yapıda olan Chua devresi olmuştur [1-2]. Bundan sonraki kısımda ise kaotik üreteç olarak Chua devresi ve buradan elde edilen kaotik sinyale ait özellikler incelenecektir.

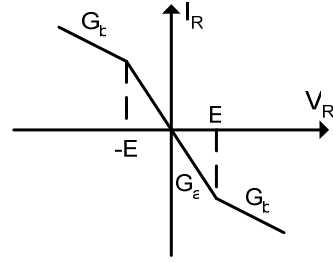
2.1. Chua Devresi

Şekil 1'de gösterilen Chua devresi, bir tane doğrusal olmayan direnç N_R , üç tane enerji depolayabilen eleman ve bir tane de aktif direnç R den oluşan basit bir kaotik osilatördür.



Şekil 1. Chua Devresi

Devrenin doğrusal olmayan bileşeni olan N_R direnci üç segmentli parçalı doğrusal direnç gibidir. Bu bileşene ait $i-v$ karakteristiği Şekil 2'de verilmiştir.



Şekil 2. N_R direncine ait I-V karakteristiği

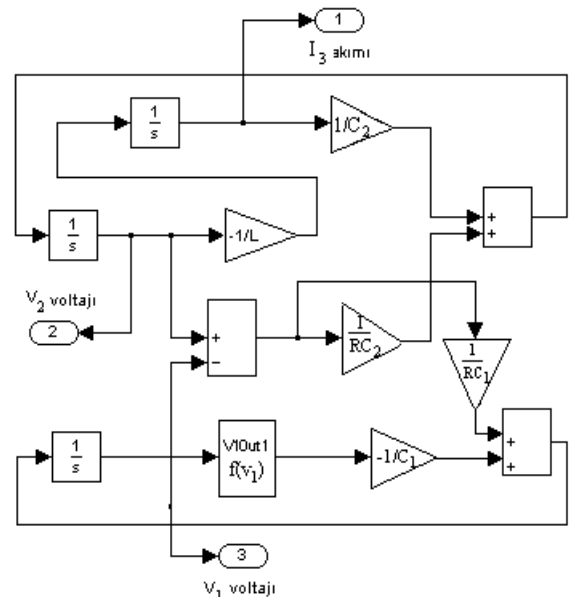
Chua devresi kaos dinamiği konusunda en çok çalışan sistem olması nedeniyle oldukça önemlidir [9]. Ayrıca bu devrenin basit elektronik elemanlar ile oluşturulması, bu devreyi kaotik haberleşme sistemleri içerisinde popüler kılmaktadır. Şekil 1'deki devrenin matematiksel modeli (1)'deki gibi elde edilir.

$$\begin{aligned} \frac{dI_3}{dt} &= -\frac{1}{L}V_2 \\ \frac{dV_2}{dt} &= \frac{1}{C_2}I_3 - \frac{G}{C_2}(V_2 - V_1) \\ \frac{dV_1}{dt} &= \frac{G}{C_1}(V_2 - V_1) - \frac{1}{C_1}f(V_1) \end{aligned} \quad (1)$$

Denklem (1)'deki $f(V_1)$, Şekil 2'de parça parça doğrusallaştırılmış karakteristiği verilen direncin bir fonksiyonu olup, Denklem (2)'deki gibi tanımlanır.

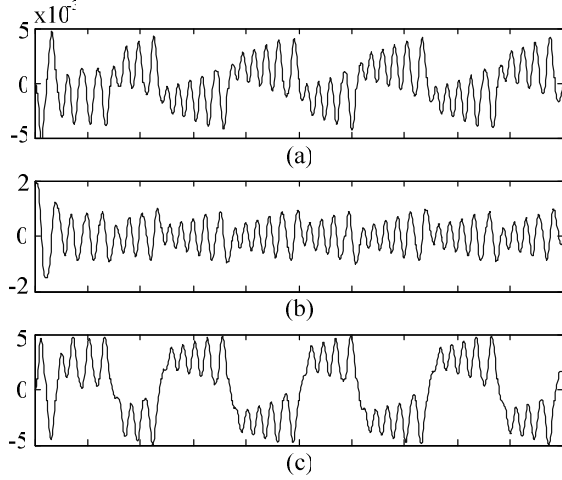
$$f(V_1) = G_b V_1 + \frac{1}{2}(G_a - G_b)[|V_1 + E| - |V_1 - E|] \quad (2)$$

Burada, V_1 ve V_2 kondansatörlerin gerilimlerini, I_3 indüktör akımını gösterirken; G_a ve G_b eğimleri, E ise doğrusal olmayan direncin kırılma noktalarını bir başka deyişle bu doğrusal bölgelerin sınırlarını gösterir.



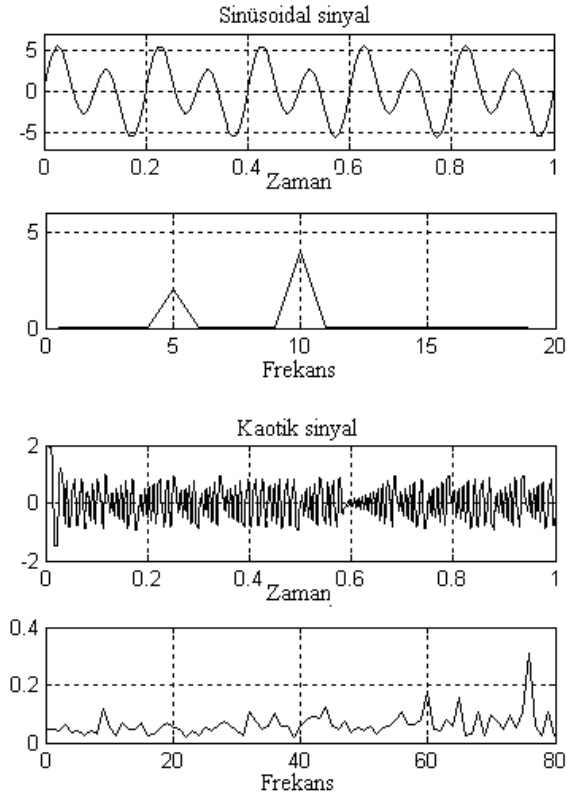
Şekil 3. Chua devresine ait simulink modeli.

Chua devresine ait diferansiyel denklemler Simulink ortamında Şekil 3'de görüldüğü gibi modellendiğinde $V_1(t)$, $V_2(t)$ ve $I_3(t)$ 'ye ait grafiksel sonuçlar Şekil 4'te görüldüğü gibi elde edildi. Bu çalışma boyunca kaotik haberleşme teknikleri için kaotik üreteç olarak Chua devresi kullanıldı.



Şekil 4. Chua devresindeki a) İndüktansın akımı, b) C_2 kondansatörü ve c) C_1 kondansatörü üzerindeki gerilimlerin değişimi

Bu sonuçların elde edilmesinde $L=18$ mH; $C_1=10$ nF; $C_2=100$ nF; $G_a=-757\mu S$; $G_b=-409\mu S$ ve $E=1$ V değerleri alınmıştır.



Şekil 5. Zaman ve frekans domenlerindeki sinüzoidal ve kaotik sinyallerin spektrumları

Şekil 5'de ise zaman ve frekans domeninde herhangi bir sinüzoidal ve bu kaotik sinyallerin özellikleri verilmiştir.

3. KAOS MODÜLASYON

Kaotik sayısal modülasyon, bilgi işaretlerinin geniş bantlı kaotik dalga üzerine eşlenmesi ile ilgili bir tekniktir [5]. Alıcı tarafta ise senkronizasyonun kullanıldığı evreuyumlu (coherent) veya senkronizasyonun kullanılmadığı evreuyumsuz (non-coherent) demodülasyon tekniklerinden biri ile gönderilen sayısal bilgi elde edilebilir [1].

Kaotik senkronizasyon tekniklerinin henüz kullanışlı olmamasından dolayı evreuyumsuz sistemlerin kullanılması daha pratiktir. Ayrıca bu yapıların bir diğer avantajı ise taşıyıcı fonksiyonlar alıcı tarafta tekrar oluşturulmadıkları için devre yapıları evreuyumlu olanlara göre daha basittir [6].

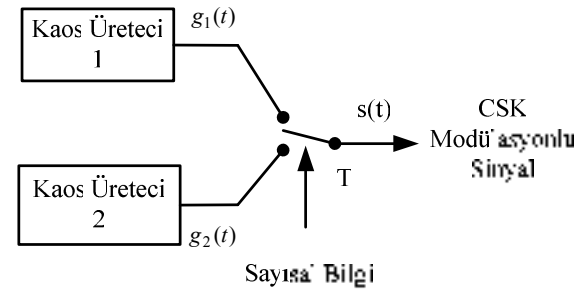
Demodülasyon sırasında kaotik sinyalin bit enerji değeri hesaplanır. Taşınan bilgi periyodik olmayan kaotik sinyal parçaları ile temsil edildiğinden karar devresi için giriş, değişken bir değer olur. Bit başına düşen enerji gönderilen kaotik sinyale ve kanal gürültüsüne bağlıyken, karar devresi için gerekli eşik değer seviyesi kanaldaki sinyal-gürültü oranına bağlıdır [7].

Kaotik taşıyıcı kullanarak sayısal modülasyon ve evreuyumlu alıcı devresi ilk defa 1992 yılında *Kaos Kaydırmalı Anahtarlama* (Chaos Shift Keying, CSK) adı altında ortaya çıkmıştır. Sonraki yıllarda diğer kaotik modülasyon teknikleri sunulmuş ve 1996 yılında daha sağlam bir teknik olan *Farksal Kaos Kaydırmalı Anahtarlama* (Differential Chaos Shift Keying, DCSK) tanıtılmıştır.

Bu çalışmanın geri kalan kısmında kaos tabanlı sayısal modülasyon tekniklerinden evreuyumsuz CSK ve DCSK yapıları tanıtılmakta ve bu tekniklere ait simülasyon sonuçları elde edilmektedir.

3.1. Kaos Kaydırmalı Anahtarlama (CSK)

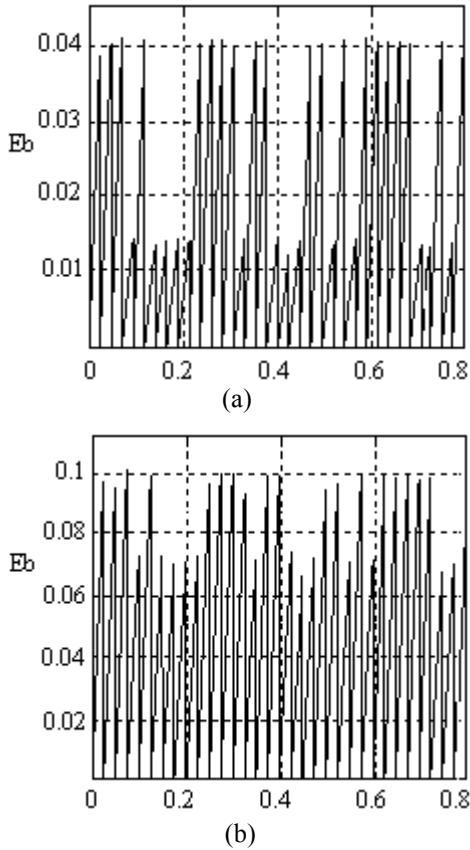
CSK modülasyon tekniği sayısal bilgi göndermek için farklı bit enerjilere sahip iki kaotik üreteç g_1 ve g_2 kullanır. Bu kaotik taşıyıcılar aynı kaotik üreticinin farklı başlangıç değerleri ile oluşturulabilirken, farklı sabit sayılarla çarpılmış aynı kaotik devreden de elde edilebilir [2].



Şekil 6. CSK modülatör şeması

$$s(t) = \begin{cases} g_1(t) & \text{'+' sembolü iletildiğinde} \\ g_2(t) & \text{'-' sembolü iletildiğinde} \end{cases} \quad (3)$$

Şekil 6'da gösterilen CSK modülasyonunda kullanılan devre çok basittir: bit '1' için vericiden bit enerjisi E_b , $g_1(t)$ yayılırken; bit '0' için ortalama bit enerjisi, $g_2(t)$ yayılır [1-2]. Modülasyonun matematiksel ifadesi Denklem (3)'te gösterildiği gibidir. Alıcı tarafta ise bit enerjileri korelatör yardımıyla kestirilebilir [9]. Şekil 7'de farklı bit enerjisine sahip kaotik taşıyıcıların kanal gürültüsünün çok az ve çok fazla olduğu ortamdaki korelatör çıktıları gösterilmiştir.

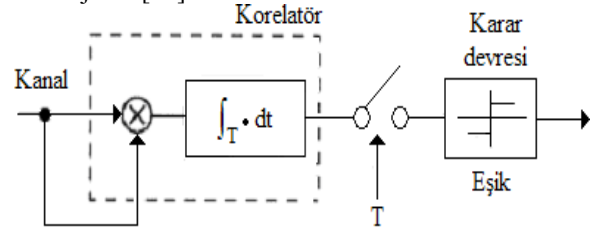


Şekil 7. Farklı bit enerji değerine sahip taşıyıcıların korelatör çıktıları a) Kanal gürültüsünün çok az olduğu b) Kanal gürültüsünün çok fazla olduğu durum.

Kanal gürültüsünün çok fazla olduğu durumda (Şekil 7.b) ise sayısal 1 ve 0'ı temsil eden enerji seviyeleri arasındaki fark çok küçük olmakla beraber bu ortam için seçilecek eşik değerinin hassas olması gerekir. Böylelikle gönderilen veriler alıcı tarafta doğru bir şekilde elde edilebilir. Yukarıda verilen sonuçlardan da anlaşılacağı gibi kaotik taşıyıcıların enerji değerleri farklıdır ve uygun bir eşik değer seviyesi ile bunların temsil ettikleri sayısal bilgiyi ayırt etmek mümkündür. Örneğin, Şekil 7.a grafik sonucuna göre bu eşik değeri, $E_b=0.02$ olarak seçilebilir.

Güçlü bir senkronizasyonun kullanıldığı evreyumlu sistemler, gürültü performansı

açısından evreyumsuz sistemlere göre daha avantajlıdır [10].

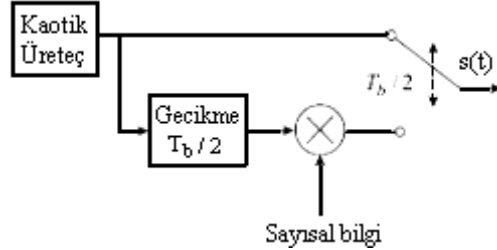


Şekil 8. Evreyumsuz CSK demodülatörü.

Şekil 8'de senkronizasyonun kullanılmadığı evreyumsuz CSK alıcı devresinin blok diyagramı verilmiştir. Kanalda gürültü seviyesi arttıkça eşik değeri de değişecektir.

3.2. Farksal Kaos Kaydırmalı Anahtarlama (DCSK)

Diğer bir modülasyon tekniği olan DCSK ise her bir sembol periyodu için referans ve bu sinyal tarafından takip edilen bilgi sinyali olmak üzere iki kaotik dalga içerir. Sayısal '1' için kaos üreteç devresinden art arda iki referans sinyali ve '0' için ise referans kaotik sinyali ardından bu sinyalin tersi gönderilir [11].



Şekil 9. DCSK modülatörü

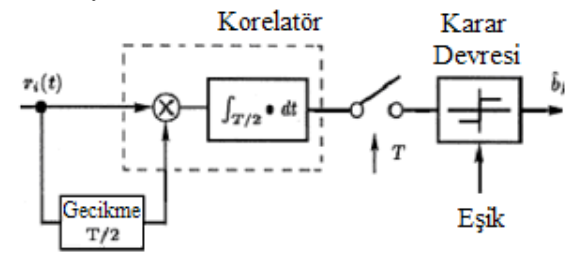
Şekil 9'da gösterildiği gibi DCSK modülasyonunda gönderilen sinyalin kısmen bir yarısı referans kaotik dalga ve diğer yarısı ise modüle olmuş bilgi tarafıdır [11]. Matematiksel ifadesi ise Denklem (4) ve (5)'deki gibidir.

Eğer sembol '+1'

$$s(t) = \begin{cases} c(t) & (l-1)T \leq t < (l-1/2)T \\ c(t-T/2) & (l-1/2)T \leq t < lT \end{cases} \quad (4)$$

Eğer sembol '-1'

$$s(t) = \begin{cases} c(t) & (l-1)T \leq t < (l-1/2)T \\ -c(t-T/2) & (l-1/2)T \leq t < lT \end{cases} \quad (5)$$



Şekil 10. DCSK demodülatörü.

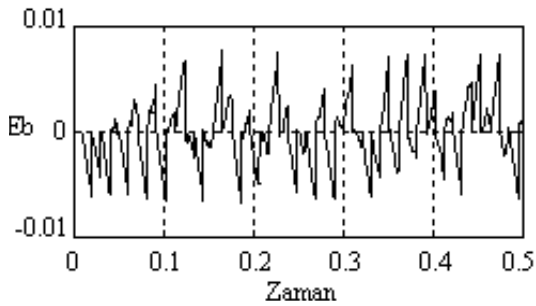
Şekil 10’da gösterilen DCSK demodülasyon yapısında alıcıya gelen r_i sinyali, kendisinden M kadar geciktirilmiş r_{i-M} sinyali ile çarpılarak korelatöre girer. Burada bir örnek fonksiyonuna ait integral alınır ve korelatör çıkışı Denklem (6)’daki gibi hesaplanır.

$$S = \sum_{i=1}^M r_i \cdot r_{i+M} \quad (6)$$

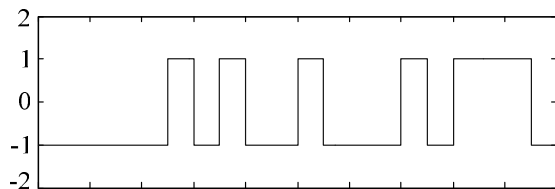
$r_i = s_i + \zeta_i$ ifadesi denklemde yerine yazılırsa,

$$\begin{aligned} S &= \sum_{i=1}^M (s_i + \zeta_i) \cdot (s_{i+M} + \zeta_{i+M}) \\ &= \sum_{i=1}^M (b_i x_i^2 + x_i (\zeta_{i+M} + b_i \zeta_i) + \zeta_i \cdot \zeta_{i+M}) \\ &= b_i \sum_{i=1}^M x_i^2 + \sum_{i=1}^M x_i (\zeta_{i+M} + b_i \zeta_i) + \zeta_i \cdot \zeta_i \end{aligned} \quad (7)$$

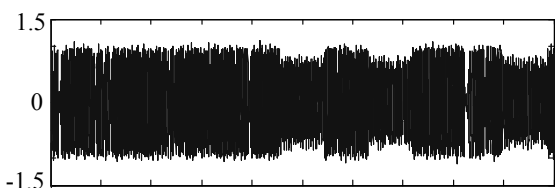
Denklem (7)’de ilk terim kullanılan ve gerekli olan sinyaldir ve diğer terimler ise gürültü ile ilgili bileşenlerdir. Korelatör sonucu 0 dan büyük ise bit 1; küçük ise bit 0 elde edilir [6]. Bu durumda, $b_i \sum x_i^2$ teriminin işareti b_i ’e bağlı olmakla beraber $b_i = 1$ olması bitin ‘1’ olduğunu, 0 veya -1 olması ise bitin ‘0’ olduğunu ifade etmektedir [12]. Korelatör çıkışı Şekil 11’de verilmiştir.



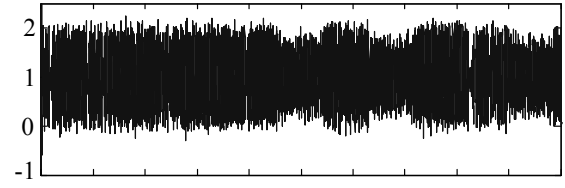
Şekil 11. DCSK’deki korelatör çıkışı.



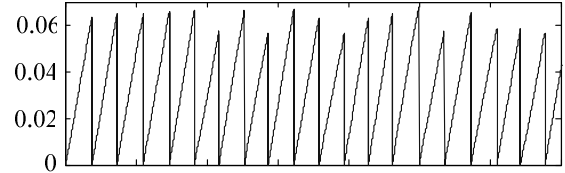
(a)



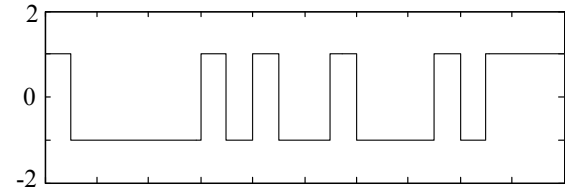
(b)



(c)



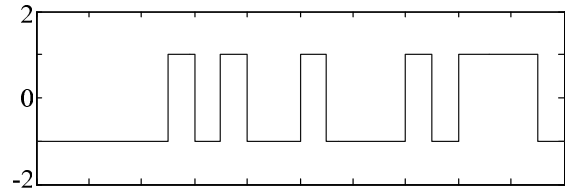
(d)



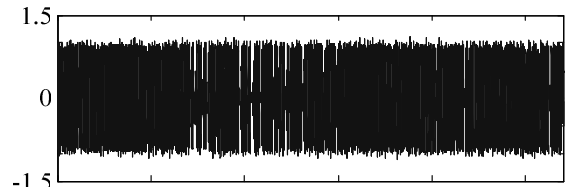
(e)

Şekil 12. CSK modülasyonunda a) iletilen sayısal sinyal, b) CSK modülasyonu sinyali, c) kanal modülasyonu sinyali, d) korelatörün çıkışı ve e) elde edilen sayısal sinyal.

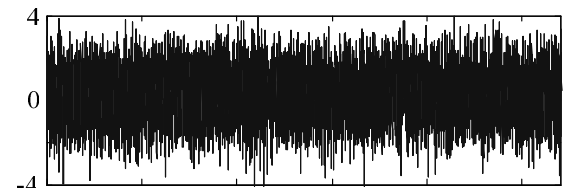
Matlab/Simulink’te yapılmış olan sayısal bilginin kaos tabanlı CSK ve DCSK tekniklerine ait modülasyon ve demodülasyon durumlarına ilişkin grafiksel sonuçlar sırasıyla Şekil 12 ve Şekil 13’de verilmiştir.



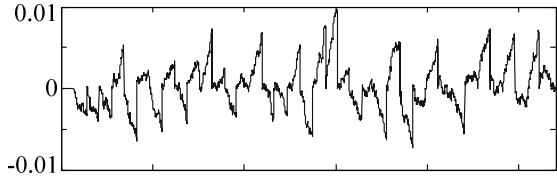
(a)



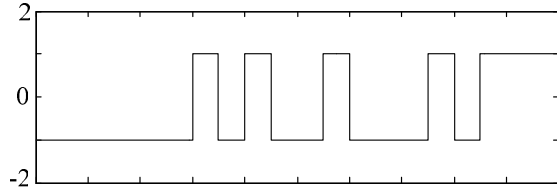
(b)



(c)



(d)



(e)

Şekil 13. DCSK modülasyonunda a) iletilen sayısal sinyal, b) DCSK modülasyonlu sinyal, c) kanaldaki modülasyonlu sinyal, d) korelatörün çıkışı ve e) elde edilen sayısal sinyal.

4. SONUÇ

Bu çalışma, Kaotik haberleşme sistemlerine ve kaos tabanlı sayısal CSK ve DCSK modülasyon tekniklerine genel bir bakışı özetlemektedir. Burada değinilen sayısal modülasyon teknikleri Simulink ortamında modellenmiş olup simülasyonlarda sayısal bilgi sadece 1 bit hata ile alıcıya gönderilmiştir.

Ayrıca kaotik haberleşmede taşıyıcı olarak kullanılan kaotik sinyale ait ,

- Geniş bant spektrumuna sahip olması,
- Gürültü benzeri görünmesi,
- Karmaşık yapıda olması ve periyodik olmaması,

gibi karakteristik özellikler Matlab/Simulink ortamında incelenmiş olup, çıkan sonuçlar ile desteklenmiştir. Evreuyumsuz tekniklerde kanal gürültüsünün değişiminin doğrudan karar devresi eşik değerini değiştirdiği görülmüştür.

KAYNAKLAR

- [1] Gabor, K., Michael, P. K., & Geza, K. (1998). Chaotic communication without synchronization, 6th IEEE Telecommunications Conference, 49-53.
- [2] Michael, P. K., & Geza, K. (1998). Digital communications using chaos, Signal Processing 80, 1307-1320.
- [3] Farah, B., Kachouri, A., & Samet, M. (2006). Design of secure digital communication systems using DCSK chaotic modulation, IEEE, DTIS'06, 200-204.
- [4] Corron, N.J., & Hahs, D.W. (1997). A new approach to communications using chaotic signals, IEEE Transactions on Circuits and Systems, 44(5), 373-383.
- [5] Anjam, R., & Maaruf, A. (2008). Chaotic communications their applications and advantages over traditional methods of communication, CNSDSP 2008, 21-24.
- [6] Geza, K., & Michael, P.K. (1997). The role of synchronization in digital communications using chaos Part-I: Fundamentals of using digital communications, IEEE Transactions on Circuits and Systems, 44(10), 927-936.
- [7] Michael, P.K., Geza, K., Gabor, K., & Zoltan, J. (1998). Recent advances in communicating with chaos. ISCAS'98, 4, 461-464.
- [8] Pecora, L. M., & Carroll, T. L. (1990). Synchronization in chaotic systems, Phys. Rev. Lett. 64, 821-824.
- [9] Kennedy, M. P., Kolumbán, G., Kis, G. & Jáko, Z. (1998). Recent advances in communicating with chaos. Proc. IEEE International Symposium on Circuits and Systems (ISCAS'98), Monterey, California, USA, 461-464.
- [10] Kolumbán, G., Kennedy, M. P., & Chua, L. O. (1998). The role of synchronization in digital communications using chaos-Part II: Chaotic modulation and chaotic synchronization", IEEE Transactions on Circuits and Systems Part I, 45(4), 1129-1140.
- [11] Karuna, T., Donghee, K., Donghee, K., Hong-Mo, C., & Kyung, S., K., (2007). DCSK chaotic modulation with reduced ISI, JCCI 2007.
- [12] Hasler, M. (1998). Chaos shift keying in the presence of noise: a simple discrete time example. Proceedings of the 1998 IEEE International Symposium on Circuits and Systems, ISCAS '98, 3, 271-274.