

Kesir Dereceli Kaotik Osilatör ile Maskelenmiş Dijital Haberleşme Sisteminin Gürültü Performansının İncelenmesi

Özkan ATAN, Mustafa TÜRK*
Yüzüncü Yıl Üniversitesi
Elektronik-Haberleşme Bölümü
Van
oatan@yyu.edu.tr

*Fırat Üniversitesi
Elektrik Elektronik Mühendisliği Bölümü
Elazığ
mturk@firat.edu.tr

Özet: Bu çalışmada, multi-scroll (MS) kaotik osilatör ile maskelenmiş faz kaydırmalı anahtarlama (PSK) sisteminin, gürültü performansı incelenmiştir. Dijital veri PSK yöntemine göre modüle edilmiş ve daha sonra kesir dereceli multi-Scroll kaotik bir sistemle maskelenmiştir. Maske kaldırma işlemini gerçekleştirmek için yine kesir dereceli bir denetleyici ile senkronizasyon kontrolü yapılmıştır. Gürültülü kanaldan gönderilen veri, alıcı tarafından tekrar elde edilmeye çalışılmıştır. Farklı Sinyal/Gürültü oranlarında bu işlem gerçekleştirilerek sistemin gürültüye karşı dayanımı incelenmiştir. Elde edilen sonuçlara göre MS kaotik sistem ile maskelenme ile sistem güvenliği artırılmış ve kullanılan senkronizasyon denetleyicisi sayesinde kaotik PSK yönteminin, literatürde bulunan çalışmalardan daha iyi performans gösterdiği görülmüştür.

1. Giriş

Kaos son yıllarda matematik ve mühendislik alanında çalışılan önemli konularda biridir. Kaos, başlangıç durumuna karşı aşırı hassas olan sistemler olarak bilinir. Kaotik sistemlerin en yaygın kullanım alanlarından biri haberleşme sistemleridir [1]. Kaotik sistemlerin, özellikle haberleşme sistemlerindeki uygulamalarında bilgi güvenliği için sistemin daha yüksek karmaşıklığa sahip olması istenir. Multi-scroll (MS) kaotik sistemlerin de en önemli avantajı yüksek karmaşıklığa sahip olmasıdır [2]. Bu yüzden MS sistemler ile ilgili son yıllarda yapılan çalışmalar artmıştır [3-5].

Kaotik sistemlerle gerçekleştirilen birçok farklı sayısal haberleşme sistemi mevcuttur. Bunlar: kaotik maskeleme [6], kaotik kaydırmalı anahtarlama (CSK)[7], Kaotik on-off anahtarlama(COOK) [8], farksal kaotik kaydırmalı anahtarlama (DCSK) [9] gibi kaotik haberleşme yöntemleri mevcuttur. Kaotik maskelemede veri, kaos dinamiklerinden biriyle toplanarak haberleşme kanalına gönderilir. Alıcı tarafından alınan bu maskelemiş verinin, tekrardan elde edilebilmesi için gönderici ve alıcı arasında bulunan, master ve slave adlı kaotik sistemlerin senkronize olması gereklidir. Senkronizasyon kontrolünde amaç iki kaotik sistemin mümkün olduğunca hızlı s enkronize olmasıdır. Senkronizasyon için birçok denetim yöntemi vardır [10-12]. Bu yöntemlerden biri de kesir dereceli denetleyicilerdir [13].

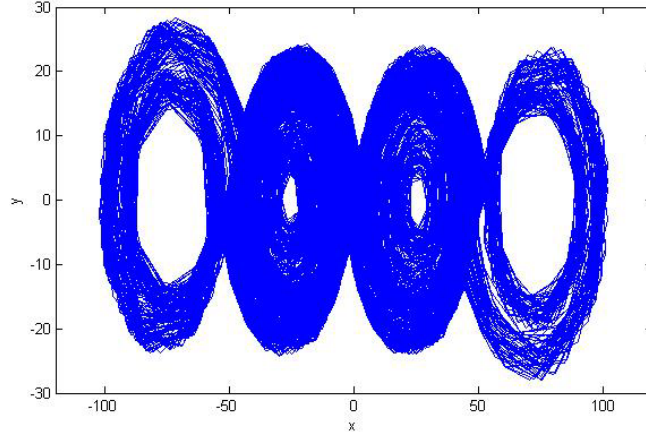
Kesir dereceli PID (FOPID) de bu kontrol yöntemlerinden biridir [14]. FOPID yöntemi, denetleyicide bulunan türev ve integral derecesinin herhangi bir reel sayı olduğu denetim yöntemidir. Özellikle lineer olmayan sistemlerin denetiminde sağladığı başarımlardan dolayı etkili bir denetim yöntemidir.

Bu çalışmada kesir dereceli hiperbolik MS kaotik osilatörle maskelenen, PSK modüleli sayısal taşıyıcı, alıcı tarafından yeniden elde edilmeye çalışılmıştır. Farklı gürültü seviyelerinde gerçekleştirilen bu işlem sonucu bit/hata oranları (BER) incelenerek sistemin performansı değerlendirilmiştir. Aynı zamanda kesir dereceli PID denetleyicisiyle klasik PID denetleyici arasında ki farkı değerlendirmek amacıyla bu denetleyicilerle ayrı ayrı test edilmiştir. Çalışmanın II. Bölümünde MS kaotik sistemler ve bu kaotik sistemlerin senkronizasyonu yöntemi incelenmiştir. Kaotik maskeli PSK yöntemi III. Bölümde incelenmiştir. Simülasyon sonuçları ve sonuç, sırasıyla IV. Bölüm ve V. Bölümde incelenmiştir.

2. Kaotik Sistemler ve Kaotik Sistemlerin Senkronizasyonu

MS kaotik sistemler ve bu sistemlerin senkronizasyonu üzerinde yapılan yeni bir çalışmada MS hiperbolik kaotik sistemlerdir. Sistemin matematiksel ifadesi Denklem 1' de verilmiştir. Burada α , β ve γ katsayıları negatif katsayılardır [5]. Örnek olarak: $\alpha=\beta=\gamma=0.8$, $r=s=1$ ve $\tau=50$ için oluşan kaotik scroll Şekil 1 de verilmiştir.

$$\begin{aligned}
\frac{dx}{dt} &= y \\
\frac{dy}{dt} &= z \\
\frac{dz}{dt} &= \alpha x + \beta y + \gamma z - \alpha \frac{\tau}{2} \left[(r-s) + \sum_{j=-r}^s \tanh(x + j\tau) \right]
\end{aligned} \tag{1}$$



Şekil 1. 4-Scroll hiperbolik kaotik sistemin oluşturduğu çeki

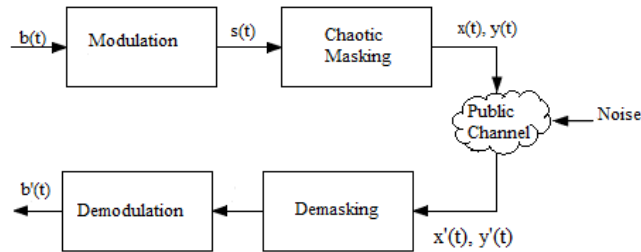
Sistemin senkronizasyonunu sağlamak için Denklem (2)'de görüldüğü gibi bir kontrol girişi yapılır.

$$\begin{aligned}
\frac{dx}{dt} &= y \\
\frac{dy}{dt} &= z \\
\frac{dz}{dt} &= \alpha x + \beta y + \gamma z - \alpha \frac{\tau}{2} \left[(r-s) + \sum_{j=-r}^s \tanh(x + j\tau) \right]
\end{aligned} \tag{2}$$

Bu giriş, master ve slave sistem arasındaki hataya göre çıkış üreten ve lineer olmayan sistemlerin denetiminde yüksek başarı sağlayan, kesir dereceli PID tipi denetleyicidir.

3. Kaotik Maskeli Dijital Haberleşme Yöntemi

Kaos temelli sayısal haberleşmede sayısal veri alıcıdan vericiye iletilirken; modülasyon kaotik maskeleme, haberleşme kanalı, kaotik maske kaldırma ve demodülasyon aşamalarından geçerek hedef noktaya ulaşır. Bu sisteme ait blok diyagramı Şekil 2' de görülmektedir.



Şekil 2. Kaos tabanlı sayısal haberleşme sistemine ait blok diyagram

Modülasyon: Sayısal verinin sürekli sinyale dönüştürülerek kaotik maskeleme için hazırlandığı evredir. Modülasyon için birçok farklı yöntem bulunmaktadır. Bu çalışmada, verinin taşıyıcının fazına kodlandığı PSK yöntemi kullanılarak modülasyon gerçekleştirilmiştir.

PSK modülasyonuna ait matematiksel ifade;

$$s(t) = \begin{cases} \cos(\frac{2\pi}{T}t) & b(t) = 0 \\ -\cos(\frac{2\pi}{T}t) & b(t) = 1 \end{cases} \quad (3)$$

şeklindedir [4]. Burada $b(t) \in [0,1]$ bilgi işareti ve $s(t)$ taşıyıcı işarettir.

Kaotik Maskeleme: Kaotik haberleşme sistemlerinde birçok farklı yöntem vardır. Bunlardan biri de kaotik maskeleme yöntemidir. Bu yöntemde aşağıdaki ifadeden de görüldüğü gibi, bilgi işaretine kaotik bir değişken eklenerek haberleşme kanalına verilir.

$$\hat{x}(t) = s(t) + x_1(t) \quad (4)$$

Veri kaybını en aza indirebilmek için alıcıda bulunan kaotik sistem ile vericide bulunan kaotik sistem, mümkün olan en kısa zamanda senkronize olması gereklidir.

Kaotik Maske Kaldırma: Kaotik maske kaldırma işleminde kanaldan alınan veriden alıcı ile senkronize olmuş kaotik sistem arasındaki fark alınarak yapılır. Maske kaldırma işlemine ait matematiksel ifade Denklem (5) de verilmektedir.

$$s(t) = \hat{x}'(t) - x_2(t) \quad (5)$$

Demodülasyon: Modüle edilmiş sinyalden verinin yeniden elde edilebilmesi için demodülasyon işlemi yapılır. PSK demodülasyonu için maskesi kaldırılmış taşıyıcıdan veri;

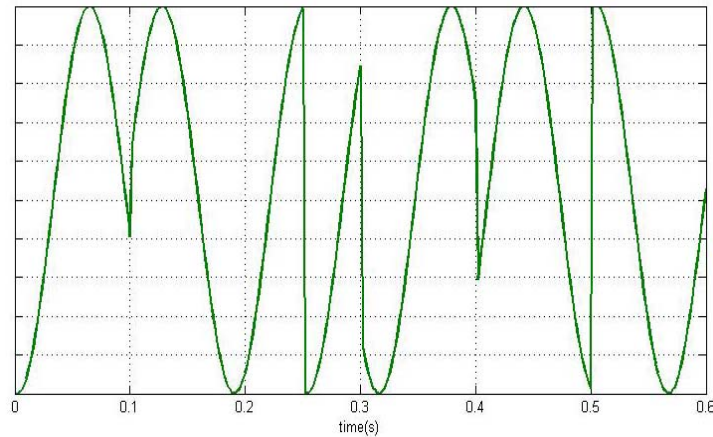
$$b(t) = \begin{cases} 1, & \int_0^T s(t) \cdot \cos(\frac{2\pi}{T}t) > 0 \\ 0, & \int_0^T s(t) \cdot \cos(\frac{2\pi}{T}t) < 0 \end{cases} \quad (7)$$

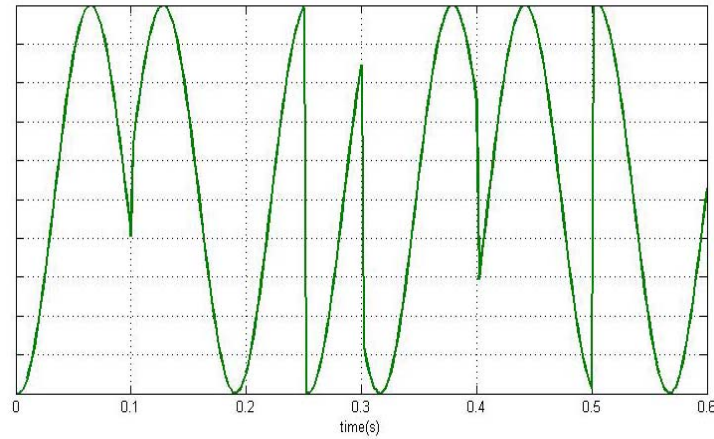
ifadeye göre demodüle edilir.

4. Simülasyon Sonuçları

Simülasyon Matlab/Simulink® programıyla gerçekleştirilmiştir. Veri olarak rastgele gönderilen 10^6 bitlik bir veri gönderilmiş PSK yöntemine göre modüle edilerek, MS hiperbolik kaotik osilatör ile maskelenmiştir. Veri alıcıda tekrardan elde edilmeye çalışılmıştır. Gönderilen verinin modülatör çıkışı ve maskelendikten maskeleme çıkışı Şekil 3'de gösterilmiştir.

Farklı gürültü seviyelerinde kaotik maskelenmiş verinin Bit/Hata oranı Tablo 1'de verilmiştir.





Tablo 1. Farklı kanal gürültüsünde BER oranları

SNR	BER
-	2.10^{-6}
50	2.10^{-6}
40	3.10^{-6}
30	5.10^{-5}
20	2.10^{-3}

Sonuç:

Bu çalışmada kaotik maskeleye yapılarak farklı sayısal haberleşme yöntemlerinin performansı test edilmiştir. Maskeleye işlemi yeni bir yöntem olan, MS hiperbolik kaotik sistemle gerçekleştirilmiştir. Alıcı ve verici arasındaki senkronizasyon için kesir dereceli PID yöntemi kullanılarak sistemin hızlı senkronize olması sağlanmıştır. Elde edilen sonuçlara göre yöntemin gürültü performansı açısından oldukça başarılı sonuç verdiği görülmektedir.

Kaynaklar

- [1]. Ashraf A. Zaher, Abdalnasser Abu-Rezq, "On the design of chaos-based secure communication systems", Communication in Nonlinear Science and Numerical Simulation, 16(9), s. 3721–3737 2011.
- [2]. Kiani-B A., Fallahi K., Pariz N., Leung, H., "A chaotic secure communication scheme using fractional chaotic systems based on an extended fractional Kalman filter", Communications in Nonlinear Science and Numerical Simulation, 14(3), s. 863-879, 2009.
- [3]. Short K.M., "Unmasking a modulated chaotic communication scheme", International Journal of Bifurcation and Chaos, 6(2), s. 367-375, 1996.
- [4]. Chang, W.D., "Digital secure communication via chaotic systems", Digital Signal Processing, 19(4), s. 693-699, 2009.
- [5]. Xu F., Yu P. "Chaos control and chaos synchronization for multi-scroll chaotic attractors generated using hyperbolic functions" Journal of Mathematical Analysis and Applications, 362(1), s.252-274, 2010.
- [6]. Cuomo K.M., Oppenheim A.V., Strogatz S.H., "Synchronization of Lorenz-based chaotic circuits with applications to communications", IEEE Transaction on Circuits Systems II, 40(10), s.626-633, 1993.
- [7]. Hasler M., "Chaos shift keying in the presence of noise: A simple discrete time example", In Proceedings of the 1998 IEEE International Symposium on Circuits and Systems, Mayıs 1998, California, USA, s.271–274.
- [8]. Kolumbán G., Kennedy M.P., Chua L.O., "The role of synchronization in digital communications using chaos-Part II: Chaotic modulation and chaotic synchronization" IEEE Transactions on Circuits and Systems I, 45(4), s. 1129–1140, 1998.
- [9]. Kolumbán G., Kennedy M.P., Kis G., Jako Z., "FM-DCSK: A novel method for chaotic communications", In Proceedings of the 1998 IEEE International Symposium on Circuits and Systems, Mayıs 1998, California, USA, s. 477–480.
- [11]. Chen H.C., Chang J.F., Yan J.J., Liao T.L., "EP-based PID control design for chaotic synchronization with application in secure communication", Expert Systems with Applications 34(2), s.1169-1177, 2008.
- [12]. Chen C.S., "Quadratic optimal neural fuzzy control for synchronization of uncertain chaotic systems", Expert Systems with Applications, 36(9), s.11827-1183, 2009.
- [13]. Yau H.T., Shieh C.S., "Chaos synchronization using fuzzy logic controller" Nonlinear Analysis: Real World Applications, 9(4), s.1800-1810, 2008.
- [14]. Podlubny I., "Fractional-Order Systems and $PI^{\lambda}D^{\mu}$ Controllers", IEEE Transactions on Automatic Control, 44(1), s.208-214, 1999.