
# BİTİRME PROJESİ

Haftalık Rapor – 05.11.2021

5 KASIM 2021

KIRIKKALE ÜNİVERSİTESİ – BİLGİSAYAR MÜHENDİSLİĞİ İÖ

AHMET MUNGAN – 160255081

# İÇİNDEKİLER

# ÖZET

Ses damgalamasında önemli bir yere sahip olan LSB damgalama yöntemi incelenmiştir. Bu yöntemin getirdiği kavramlar, metotların uygulanış biçimleri ve temel birçok öğe işlenmiştir. Dayanılan tüm gerekçeler, kaynakçaların desteği ve yardımıyla kanıtlanmaya çalışılmıştır. Bu yöntemin uygulanırken veya uygulama sonrası avantajları ve dezavantajları raporun tersine mühendislik ile yorumlaması kısmında paylaşılmıştır.

## LSB YÖNTEMİ İLE SES DAMGALAMA

LSB algoritmasına dayalı veri gizleme teknikleri steganografi temellidir [1]. Bu çerçevede LSB algoritmasıyla oluşturulan tüm yöntemler aslında aynı temele dayanır. Bu temelin anlaşılması için LSB ve steganografi ibarelerinin açıklanması gerekir. Daha sonra ise bu kavramlardan oluşturulan ses damgalama yöntemi açıklanmalıdır.

### LSB (Least Significant Bit)

Bilgisayarda karşılaşılan veya verilerin[1] dizilişlerinde en önemsiz bite ekleme yöntemi olarak yarı-kişisel bir tanım yapılabilir [2]. En önemsiz bit ile kastedilen biti bulmak veya bu bitin varlığını saptamak kolaydır. Fakat burada en düşük basamaktaki biti bulmak kimi zaman hataya yol açabilir. Buradaki hata şu örnekle desteklenebilir: Eğer bir bit dizisi karıştırılıp belirli frekans ve aralıklara göre dizilmişse, LSB'nin tespiti mümkün olmayabilir. Bu yöntem kapsamında; ses verisi bit dizisi halindeyken bu dizinin sıralı olması kabul edilerek yönteme devam edilir. Eğer dizi sıralı değilse LSB tespiti için farklı yöntemler[2] kullanılabilir.

### Steganografi

Steganografi bilgiyi gizleme anlamına gelir. Gizleme ile şifreleme arasındaki farklardan en önemlisi, gizlenen bilginin gizli olup olmadığının bilinmemesidir [3]. Fakat şifreli bilgilerde bilgi anlamsızdır. Bilginin anlamsız olamayacağından ötürü, şifrelenen aslında verilerdir. Dolayısıyla bilginin güvenli şifrelemekten değil, gizlemekten gelir. Steganografi eski çağlardan beridir kullanılmaktadır. Eski Yunanistan zamanlarından, ikinci dünya savaşı dönemlerine kadar örnekleri genişletmek mümkündür. Bilgisayar bilimlerinde ise "veri içine veri gömmek" olarak ünlenmiştir. Sadece ses olmamakla birlikte, resim ve video gibi medya ortamlarında da kullanılır. Öyle ki; steganografi tekniği günümüz teknolojisiyle etkisini yitirmiş gibi gözükse de, birçok alanda kullanımı mevcuttur. Resim içerisine yazı gizlemek, yazı

[1] Buradaki veri ses verisi olarak değerlendirilecektir.
[2] Bu yöntemler kriptosistemler ile şifrelenmiş bir dizi olabileceğini ortaya koymaktadır.

içerisine resim gizlemek, sesin içerisinde dalga gizlemek, dalga boylarının değişim noktalarına bitmap gizlemek gibi farklı işlemlerin olduğu görülmektedir. Bu işlemler steganografinin sunduğu ve az evvel bahsi geçen LSB yöntemi ile mümkündür. Sayısallaştırılabilen veri kaynakları üzerinde bu değişiklikler LSB (en anlamsız bit) üzerinden gerçekleştirilebilmektedir.

Steganografi ve LSB kavramlarının açıklanmasından sonra, ses damgalama yönteminin nasıl olduğu konusu daha anlaşılır olacaktır.

**Yöntem**

Ses damgalama senaryosunda, bu yönteme göre iki temel gereklilik esastır [1]. Bu gerekliliklerden ilki algısal şeffaflık, bir diğeri ise gizli verilerin yüksek veri hızıdır. Algısal şeffaflık tüm veri gizleme yöntemlerinde aslında genel itibariyle gereklilik olarak kabul gören bir ibaredir. Bu ibare veri tüketicisinin veya bilginin beslenme kaynaklarının, veri üzerindeki değişiklikleri duyular ile fark edememesidir. Buradaki duyu kavramı verinin hitap ettiği alana göre değişir fakat ses üzerine düşünüldüğünde; normal algılayan bir kulağın fark edememesi olarak söylenebilir. Bu çerçevede veri üzerinde oluşturulan gürültüyü[3] algısal olarak belirlemek için psikoakustik denilen modeller kullanılmaz.

LSB gizli anahtarlı şifrelemeyi baz almıştır. Dolayısıyla şifrenin seçimi; bilgisayar tarafından oluşturulan seslerin[4] örneklem alınarak bir alt küme olarak alınmasıdır. LSB'nin yerleştiği yerler işte bu alt kümelerdir. Alt küme üzerinde çalışılmasının neticesinde damgalanacak şifrenin tüm örneklerinin bilinmesi gerekir [4].

Damgalama için kullanılan tüm şifrelerin arasından rastgele seçilerek sesin damgalanması, Gauss Gürültüsünü (AWGN) ortaya çıkarır [5]. Gauss gürültüsü olasılıkta sık kullanılan gauss dağılımının aslında ortalama değerine karşılık gelir. Bu da standart sapmanın en yüksek olduğu (veri kaybının en yüksek olduğu) noktaya karşılık gelir. Bu hesabın ham ses verisinin bitleri üzerinde gauss dağılımına uygun olarak hesaplandığında çıkan değere karşılık; damgalı ses verisinin bitleri üzerindeki

[3] Damgalanan veri burada ham halinden sonra gürültülü olacağı varsayılarak tanımlanmıştır.
[4] Bu sesler bilgisayar tarafından kayıt edilmiş seslere ait veri setleri olarak sınırlandırılabilir.

gauss dağılımının hesabıyla örtüşmediği görülür. İşte bu durum gauss gürültüsünün varlığını kanıtlar. Dolayısıyla gauss gürültüsü, LSB'nin sayısını doğru orantılı bir şekilde etkiler. Bu sebeple LSB yönteminde gauss gürültüsüne yüksek derecede izin vermemek için, LSB sayısının sınırlı bir düzeyde tutulduğu söylenebilir.

## LSB YÖNTEMİNİN TERSİNE MÜHENDİSLİK İLE YORUMLANMASI

LSB ve steganografi gibi yöntemler ile damgalama yapmak, çok eskide kalmış bir teknolojidir. Fakat günümüz teknolojilerinde kullanıldığı görülmektedir [6]. Bu kullanımı sağlayan başlıca etken LSB gerçekleştirilirken kullanılan algoritmaların hesaplama karmaşıklığının düşük olmasıdır. Düşük karmaşıklı bir algoritmanın maliyeti de düşük olacağından, ses verisi gibi büyük veri setleri ile çalışılması muhtemel senaryolarda performansın yüksek olacağı göz önündedir. Maliyetin düşük olmasındaki sebeplerden ilki; bit düzeyinde (bilgisayarın ana dilinde) programlama yapılmasıdır. Dolayısıyla geliştirilen yazılımın işlemci tarafında maliyeti 44,1 kbps gibi, günümüz bilgisayarlarını zorlamayacak düzeydeki frekans gereksinimi düşük maliyeti kanıtlar [1]. Düşük maliyet ise beraberinde işlemci için yapılması gereken yazılımsal optimizasyonu minimize eder. Fakat burada karıştırılmaması gereken bir kavram vardır: Optimizasyonun minimize edilmesi yalnızca LSB yönteminin kendine has algoritması ile ilgilidir, gizlenecek verinin şifrelenmesi/deşifrelenmesi optimizasyon gerektirebilir. İşte bu gibi avantajlarından ötürü LSB damgalama gerçek hayat uygulamalarında kullanılması en muhtemel yöntemlerden biridir.

Bu yöntemin dezavantajlarını tersine mühendislik ilkeleri ile incelersek:

1. En yaygın kullanılan yöntem olduğu için güvenli değildir.
2. Bit bazında çalışıldığı için ses verisinde sıralı ve en önemsiz bitlere brute force saldırılarında şifrenin kaybolması söz konudur.
3. Bit bazında çalışıldığı için sesin içerisindeki damganın; dijital-analog ve ardından analog-dijital dönüşümünde varlığını sürdürmesi düşük ihtimallere dayanır.
4. Damgalı veriye tersine yaklaşıldığında ses üzerindeki en ufak değişiklikler bile damganın bozulmasına (dejenere olmasına) neden olur.

Bu maddelerin önderliğinde bir ses dosyası elde edilip incelenirse, aslında çoğu ses dosyasında varlığını sürdüren damgayı da beraberinde elde etmiş oluruz. Bunun bilincinde hareket edildiğinde, elde edilen analog ses dosyasını herhangi bir programlama ortamında sadece import ve export işlemlerine tabi tutarak LSB yöntemi ile damgalanan verinin kaybolabileceği göz önündedir. Dolayısıyla bu yöntemin

varlığından ve kriptoanaliz konusundan haberdar olan kişiler rahatlıkla LSB yöntemi ile oluşturulan damgayı kaldırabilecektir. Bu tam anlamıyla zaafiyet midir yoksa bu teknik detayları bilmeyen aslında sadece kullanıcı olarak adlandırdığımız bünyelerde kullanılması mantıklı mıdır? Günümüz teknolojilerinde sosyal medyanın yaygınlaşması ve web sitesi sayısının artması ile birlikte telif haklarının kontrolü ve en önemlisi 'hızı' gündemdedir. Dolayısıyla LSB algoritmalarının hızlı çalışması, sosyal medya platformlarının ve web sitelerinin 'hızlı tüketim' anlayışını benimseyen kullanıcı bünyeleri için yararlı bir yöntem olabilir.

## REFERANS VE KAYNAKÇA


[1] Cvejic, Nedeljko, and Tapio Seppanen. "Increasing robustness of LSB audio steganography using a novel embedding method." International Conference on Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004.. Vol. 2. IEEE, 2004.

[2] Esin, E. Murat, and Erdal Güvenoğlu. "Resim İçine Yazı Gizlenmesi Amacıyla Kullanılan Lsb Ekleme Yönteminin Shuffle Algoritmasıyla İyileştirilmesi." Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi 2.1 (2007).

[3] Steganografi ile ilgili wikipedia tanımı. Link için tıklayınız.

[4] Cvejic, Nedeljko, and Tapio Seppanen. "Increasing the capacity of LSB-based audio steganography." 2002 IEEE Workshop on Multimedia Signal Processing.. IEEE, 2002.

[5] Gauss gürültüsü üzerine bir yazı. Link için tıklayınız.

[6] Chadha, Ankit, and Neha Satam. "An efficient method for image and audio steganography using Least Significant Bit (LSB) substitution." arXiv preprint arXiv:1311.1083 (2013).