BİTİRME PROJESİ

Haftalık Rapor – 08.10.2021

8 EKİM 2021

KIRIKKALE ÜNİVERSİTESİ – BİLGİSAYAR MÜHENDİSLİĞİ İÖ

AHMET MUNGAN – 160255081

İÇİNDEKİLER

GİRİŞ

Verinin gizlenmesi konusunun alt dallarından olan audio watermarking (ses damgalaması) Bitirme Projesi-1 konusu olarak seçilmiştir. Güncel teknolojiler ile aslında yapılabilir (algoritması yazılabilir) bir konu olduğu söylenebilse de, açık kaynak olarak bu tarz projelerin yayınlanmadığı aşikardır. Dolayısıyla sektörde açık kaynak kodlu ve matematiksel alt yapı ile ses damgalaması üzerine geliştirilmiş yazılımlar, programlar, alt programlar veya işlem parçacıkları bulmak pek mümkün değildir. Tüm bu sebeplerden ötürü algoritma geliştirme aşamasından evvel medya ortamının[1] ana karakteri irdelenecektir. Bu medya ortamında çalışmış kişilerin başta bilimsel makaleler olmak üzere; yazılarını, fikirlerini, geliştirdikleri çözümleri ve teorileri önemseyerek ses damgalaması üzerine açık kaynaklı bir algoritma geliştirmek bu projenin asıl amaçlarındandır.

Süreç boyunca tutulacak olan tüm raporlarda kaynakça konusunda büyük bir özen gösterilecektir. Bazı özel durumlarda, daha evvel okunmuş fakat uygulanması için bekleyen bazı makaleleri kaynakça olarak gösterilmesi ihmal edilmeyecektir. Fakat bu gibi durumlarda eğer kaynakça gösterilmez ise kasti bir durum olmadığı ve öğrenmenin bir süreci olarak değerlendirilmesi rica edilmektedir. Hassas bir konu olduğu göz önünde bulundurulursa, tüm araştırmalar ve bulgular neticesinde bazı bilgilerin nereden geldiği unutulup kaynakça olarak gösterilmeyebilir. Bu konuda Bitirme Projesi-1'in ithaf edildiği kişiler bu durumu: "emek hırsızlığı" yerine "yoğun öğrenim sürecinde unutulan kaynakça" olarak değerlendirmesi en büyük ricadır.

[1] Medya ortamı ile kastedilen bu proje özelinde ses medyasıdır.

ÖZET

Ses damgalama üzerine farklı yaklaşımların bahsedildiği farklı makaleler incelenip çıkarımlar yapılmıştır. Bu makalelerin seçiminde başta makalenin popülerliği olmak üzere, genel anlamda bahsedilen bilginin bilişim sistemleri ile ilgili olanları benimsenmiştir. Ayrıca veri gizlemede güvenliğin işin başında sıkı tutulması için tersine mühendislik teknikleri ile var olan yöntemlere yaklaşılmıştır. Bu sayede yalnızca ses damgalama değil, aynı zamanda damgalamada güvenliğin arttırılması bu proje kapsamında katma değer olarak yerini almıştır.

LİTERATÜR ARAŞTIRMALARI

Ses ile ilgili literatürde derinlemesine araştırılması yapılmıştır fakat sesin dijital ortamda oluşumu ve sesin matematiksel düzeye indirilmesi konuları şimdilik göz ardı edilecektir. Burada öncelikle odak noktası ses damgalama üzerine en fazla okunan ve üzerine alıntı yapılan makaleler olacaktır. Microsoft Company bünyesindeki iki kişinin yayınladığı, yayılmış spektrumlar üzerinden ses damgalamasını konu alan makaleden[2] birkaç çıkarım yapılmıştır. Bu çıkarımlar:

1. Spektrum ile damgalama sonrası şifre, spektrum dalgalar içerisinde kaybolabilir. Dolayısıyla şifrenin spektrum (sinyal) aracılığı ile saklandığı senaryoda, daha belirgin şifreler kullanılmadır. Daha belirgin ve ses dalgalarının çizildiği sinyallerde şifrelerin daha kalın olması birer güvenlik açığı olarak gözükmektedir. Sinyal sayısı arttıkça güvenliğin düşmesi, sinyal sayısı azaldıkça şifrenin hazır ses sinyalleri ile karışması fakat güvenliğin yükselmesi gibi iki farklı durum söz konusudur. Bu çerçevede düşünüldüğünde ses sinyalleri üzerinde güvenliğin mi yoksa şifrenin belirgin bir şekilde muhafa edilmesi mi gibi tercihler işin durumuna göre değişkenlik gösterir. Uzun süreli, sinyal değişiminin yüksek olduğu, frekansın periyota oranla sıkça değişim göstermesi gibi durumlarda şifrenin güvenliği düşürülüp daha kolay şifreleme/deşifre işlemlerinden geçirilebilir. Kısa süreli, sinyal değişiminin düşük olduğu ve frekansın periyotla birlikte değişiminin az olduğu durumlarda ise güvenlikten zaafiyet vermeden şifrenin kaybolması riskini göze alarak az sinyal kullanılarak işlem gerçekleştirilebilir. Ayrıca bu durumların kombinasyonel durumları için de uygun spektrum şifrelemesi seçilmelidir.
2. İlk çıkarımda bahsedilen güvenliği düşük şifrelemede kırılan şifrelerle birlikte ses orijinal halde kaydedilebilir. Bu da doğal olarak telif haklarını ihlal ettiği düşünülür. Telif haklarının ihlali olduğu söylenebilir fakat bunun dijital ortamda fark edilmesi mümkün değildir. Bir ses dosyasının şifreli bir şekilde

[2] Kaynakça kısmında bu makalenin detayları mevcuttur.

yayınlanmasından sonra, bu dosyanın medya ortamlarındaki takibi bu şifre ile mümkündür. Dolayısıyla şifreyi temizlenip ses dosyasının orjinalinin var olması demek telif haklarını devre dışı bırakan bir hamledir. Bu çıkarımdan anlaşılacağı üzere; telif oluşturan asıl unsur ses dosyasındaki şifredir.

3. Yayılmış spektrum tekniği ile veya literatürde kullanılan diğer ses damgalama tekniklerinin çoğu insan işitsel sistemine dayalı kusurları kullanır. Bu kusurlar, yani "*HAS*"[3] kusurlar normal bir insanın farkına varamayacağı düzeyde kusurlardır. Bu kusurlara; HAS'a uygun olmayan frekanstaki ses dalgalarının[4] bir araya gelmesiyle oluşturulan spektrum örnek verilebilir. Dolayısıyla büyük spektral değişimlerde HAS'ın küçük değişimlere duyarsız kalması da bir nevi veri gizleme olarak kabul edilir.

4. En sık kullanılan damgalama tekniklerin birisi ise korelasyon teknikleri ile düşük genlikli bir yayılmış spektrum dizisinin gizlenmesidir. Korelasyon teknikleri olasılık ve istatistiğe dayanan bir alt yapı ile ses damgalamasının yapılmasını kasteder. Bu kasıt, öyle ki; bir olaya ait farklı ölçümler neticesinde bu ölçümlerin arasındaki ilişkiyi matematiğe döker. Burada olasılıkta olay diye adlandırılan ses damgalamada dalga boyları olarak eşleştirilebilir. Bu eşleştirme sonucunda genliği yüksek ses dalgaları olabileceği gibi, genliği düşük ses dalgaları da bulunabilir. Özetle korelasyon tekniği ile ses damgalama algoritması; ses dalgalarının kıyaslanarak şifrenin en uygun noktaya konulmasını sağlar. Bu algoritmayı genellikle şu kuram üzerine kurulur: Ses dalgalarının yüksek genlikli noktalarına düşük frekanslı şifreli spektrumlar gizlemek. Dolayısıyla ses dosyasının yüksek genliğe ulaştığı noktalarda şifre barındıran spektrumun fark edilmesi zorlaşır. Korelasyon teknikleri ile, ses dosyasının tamamındaki genlik noktalarını yüksek genlik noktalarına göre ilişkisini hesaplayarak doğru tepeciğin bulunması sağlanır.

---

[3] "HAS"ın açılımı anahtar kelimeler kısmında mevcuttur. (Bkz. ANAHTAR KELİMELER)
[4] Bu uygun olmayan ses dalgalarından kasıt insan kulağının duyamayacağı frekans aralığındaki ses dalgaları kastedilmiştir. Frekansı 20-20.000 Hertz dışındaki ses dalgalarıdır.

YÖNTEMLERİN TERSİNE MÜHENDİSLİK İLE YORUMLANMASI

Literatür araştırması[5] kısmında edinilen çıkarımların iyileştirilmesi veya bu yöntemlere tersine mühendislik teknikleri ile yaklaşılması amaçlanmıştır. Bu amacın nedeni; projenin her dönüm noktasında tersine mühendislik uygulanıp, katma değerli bir dökümantasyon oluşturmaktır.

Çıkarımlardan biri olan telif hakları konusunda; "telif varsa şifre vardır" kesinlikle yadsınamaz bir gerçektir. Fakat her durum için geçerli olması beklenmemelidir. Örneğin bir ses dosyasını kişisel bir web sitesinde paylaşmak istersek, bunun telif haklarının yalnızca şifre ile belirlenmesi mümkün değildir. Sesin damgalandığı ve sesin takip edilebildiği platformlara uygun olarak algoritması geliştirilir. Youtube'da doğrulanmış hesaplar tarafından paylaşılan bir ses dosyasının Twitch platformunda telif hakları sebebiyle kullanılmaması gibi örnekler vermek mümkündür. Fakat kişisel bir web sitesinde HTML & CSS teknolojilerinin yardımı ile oluşturulan medya oynatıcıları bu algoritmaya dahil değildir. Dolayısıyla şifreli olan ses dosyası kişisel web sitesindeki medya oynatıcısını şifresinden tanımaz. Bu kişisel web sitesi popülerite kazandığı zaman telif hakları bu web sitesi için de geçerli olacaktır. Yani damgalama ve bu damganın kontrolü için kullanılan algoritma geniştirilecektir.

Bir diğer çıkarım olan korelasyon tekniği ile damgalama yapmak tersine mühendislik için bazı detay niteliğinde riskler barındırmaktadır. Tersine mühendislik ilkelerinde yapılanın tekrar yapılması güvenlik zafiyeti yaratır. Eğer şifre kırıcı zararlı yazılım üreticilerinin ses üzerinde korelasyon teknikleri ile damgalama yöntemlerini bildiği takdirde; şifre kırmak için ses dosyasında yüksek genlikli noktalara odaklanır. Dolayısıyla şifrenin daha güvenli olması için yüksek genlikli alanlar seçilirken, şifre kırıcılar için tam bir kolaylık olabilir. Bu çerçevede yapılanın tekrar yapılması fakat şifrelerin farklı noktalarda da bulunması korelasyon teknikleri kullanılsa bile şifrelemeyi eşsiz kılacaktır. Elbette bu şifrenin oluşturulması sırasında ve deşifrenin gerçekleştirilmesi için gerekli olan algoritma daha karmaşık bir hal alacaktır.

---

[5] Raporun ilk kısmından söz edilmiştir. (Bkz. LİTERATÜR ARAŞTIRMASI)

ANAHTAR KELİMELER

- ***Spektrum*** : Renklerin, seslerin, elektromanyetik dalgaların ya da diğer fiziksel gerçeklerin, belli bir kümesi ile sınırlanmadan birbiri ardına süreklilik içinde sonsuz değişmesi durumudur.
- ***HAS*** : “Human Auditory System” ingilizce tümcesinin baş harflerinden oluşan kısaltma

REFERANS VE KAYNAKÇA

- Darko Kirovski, Henrique Malvar, “Robust Spread-Spectrum Audio Watermarking” Microsoft Research, WA 98052
- P. Bassia, I. Pitas, “Robust audio watermarking in the time domain” Proc. EUSIPCO 98