BİTİRME PROJESİ

Haftalık Rapor – 03.12.2021

3 ARALIK 2021

KIRIKKALE ÜNİVERSİTESİ – BİLGİSAYAR MÜHENDİSLİĞİ İÖ

AHMET MUNGAN – 160255081

İÇİNDEKİLER

ÖZET

Ses damgalamada etkili yöntemlerden biri olan two-set yöntemi incelenmiştir. Bu yöntemin matematiksel çıktıları, olasılıksal hesaplamaları, istatistik ile elde edilen değer ve denklemlerin açıklamaları ile birlikte ortaya konulmuştur. Yöntemin olmazsa olmazlarından patchwork scheme isimli yöntemi destekleyici alt algoritma incelenmiştir. Bu yöntemin, diğer yöntemlere kıyasla avantaj ve dezavantajları raporun tersine mühendislik kısmında yorumlanmıştır.

İKİ KÜME YÖNTEMİ

Geçen haftalar itibariyle genel olarak veri gizlemede en önemli yere sahip LSB yönteminin açıklanması ve program kodunun yazılması gerçekleştirilmiştir. Bu çerçevede program kodu bilinenin aksine tersine mühendislik ilkelerini benimseyerek, en doğru tabirle üst akıl bakış açısı ile LSB yöntemi kodlanmıştır.

Ses damgalamada az kullanılan bir diğer yöntem ise two-set method olarak geçen iki küme yöntemidir [1]. Bu yöntemde damgalama şemaları ortaya çıkarılır ve 2 adet damga şeması seçilir. Bu şemalar mevcut yöntemin iki kümesi olur. Bu iki küme birbirinden farklıysa bu verinin üzerinde damga vardır denebilir. Elbette ki kesin olmamakla birlikte, farklı iki kümenin çıktığı durumlarda veri üzerinde bir damga olmayabilir. Ayrıca bu iki kümenin farklı olduğuna dair kararı veri seti üzerinde çalışan algoritmalar aracılığı ile belirlemek gerektiğinden; genellikle iki küme arasındaki ortalamaların matematiksel farkına dayanan bir dizi testler ile belirlemek mümkündür. İki küme şartı yöntemin temel bileşenleri tanımlanırken zorunlu kılınmış olsa da, günümüzde çok katmanlı damgalamalar da yapıldığı görülmektedir [2]. Çok katmanlı damgalama mantığından ötürü bu yöntemde de iki veya daha fazla küme kullanılabilir. Bu durumdan yola çıkarak, akla şu gelmelidir: Bu yöntem ile damgalanan verinin geri dönüşü mümkün müdür? Bu yöntemin geri dönüşü çok düşük ihtimallerle mümkündür. Bu ihtimaller matematiksel olarak veri setinin içeriği ile değişkenlik gösterse de, steganografik olarak incelenen ve frekans aralığı sabit bir ses için;

$$P_{demarking} = \frac{d + k}{d_{all}} \qquad \dots (1)$$

şeklinde (1) ile ifade edilmiştir. Yani damganın kaldırıması işlemlerinde bir k katsayısı ile verinin o anki enerjisi (iki küme arasındaki fark) toplanarak tüm verilere bölünmesiyle damganın kaldırılması işleminin ihtimali ortaya çıkar. Bu ihtimal

genellikle ortalama bir ses için $(10^{-2}, 10^{-17})$ gibi olasılıksal bir açık değer aralığı olarak hesaplanmıştır.[1]

Bu sebeplerden ötürü damganın kaldırılması işlemleri yapıldıktan sonra damgalama analizlerine tabi tutulursa başarı ve performans sonuçları bu yöntem için çok kötü sonuçlar verir [3][4]. Dolayısıyla bu yöntemde kör damgalama[2] yapmak kabul edilebilir. Hatta damganın kaldırılması bu kadar arka planda tutulan daha iyi bir yöntem bulunamayabilir.

LSB yöntemine benzer bir şekilde verinin bitleri üzerinde de two-parity (iki komşu) olarak gerçekleştirilebilir. Benzer şekilde komşu bit setlerinin üzerinde damgalama yapılarak, bu iki bit setinin ortalama farkları (bit shifting operations) alınarak yine bu işlem gerçekleştirilebilir. Aynı şekilde 2 veya daha fazla bit seti için bu damgalama yöntemi kullanılabilir. Bit setleri ile bu işlemin yapılmasında, yukarıda verilen demarking işlemleri sonrasında performans için olasılıksal hesapları daha yüksektir. Fakat bu yüksek olasılık sanıldığı kadar ya da LSB ham yönteminde olunabileceği kadar başarıyı temsil etmez.

Yama Çalışması Şeması

İki kümeli yöntemin içerisinde barındırdığı önemli bir kriter ise yama çalışması şemasının çıkarılmasıdır. Bu sayede damga, diğer yöntemlerde olduğu gibi sağlam bir şekilde veri ile birleşir.

Bu şemanın algoritması ses kesitinden alınmış bir sinyal için tasarlanmış bir istatistik barındırır. Bu ses kesiti özel olarak, sesin sözde-rassal bir noktasına tekabül etmesi gerekmektedir. Bu sözde-rassal kesit imgeleyici olmalıdır. Bu kesit iki sefer seçilerek varolan yöntemin bileşenleri sağlanır. Fakat seçilen ikinci kesit için de özel bir istatistik barındırması gerekir. Ayrıca sıkça kullanılan bu istatistik sabit olarak seçilip, bir kesit ile toplanırken diğeri ile çıkarılabilir [5].

Algoritmayı 3 adım halinde iki küme için özetlemek gerekirse:

1. Sözde-rassal kesit alınır.

---

[1] Burada genel-geçer seslerin dahil edilmediği bilinmesi gerekir.
[2] Kör damgalama: Damgadan geriye dönüşün önemsenmediği türden damgalama.

2. Sabit bir d değerini bir yamaya eklenir.

3. Sabit bir d değerini diğer bir yamadan çıkarılır.

Matematiksel olarak ifade etmek gerekirse:

$$a_i^* = a_i + d \quad \ldots (2)$$

$$b_i^* = b_i - d \quad \ldots (3)$$

şeklinde (2) ve (3) denklemleri ile ifade edilebilir. Bu kesitler yukarıdaki ifadeler ile gerçekleştikten sonra kesitlerin alındığı yerlere geri yerleştirilmesi de algoritmanın bir adımı olarak karşımıza çıkar. Bu adım genellikle yama şeması algoritmasında söylenmez çünkü bu adımları takiben olasılıksal değerlerin hesapları için beklenen değerlerin tutulması gerekir. Beklenen değerler birbirine göre ters olasılıkta eşitse, yani;

$$P(a^*) = 1 - P(b^*) \quad \ldots (4)$$

şeklinde (4) gibi bir denklik elde ediliyorsa yamalı kısım doğru bir şekilde yerine yerleşebilir denebilir. Bu olasılıkları hesaplamak için de bu iki kümenin beklenen değer ilişkilerine bakılması gerekir. Beklenen değerin E ile gösterildiği ve d istatistiği bulunduğu söylenirse:

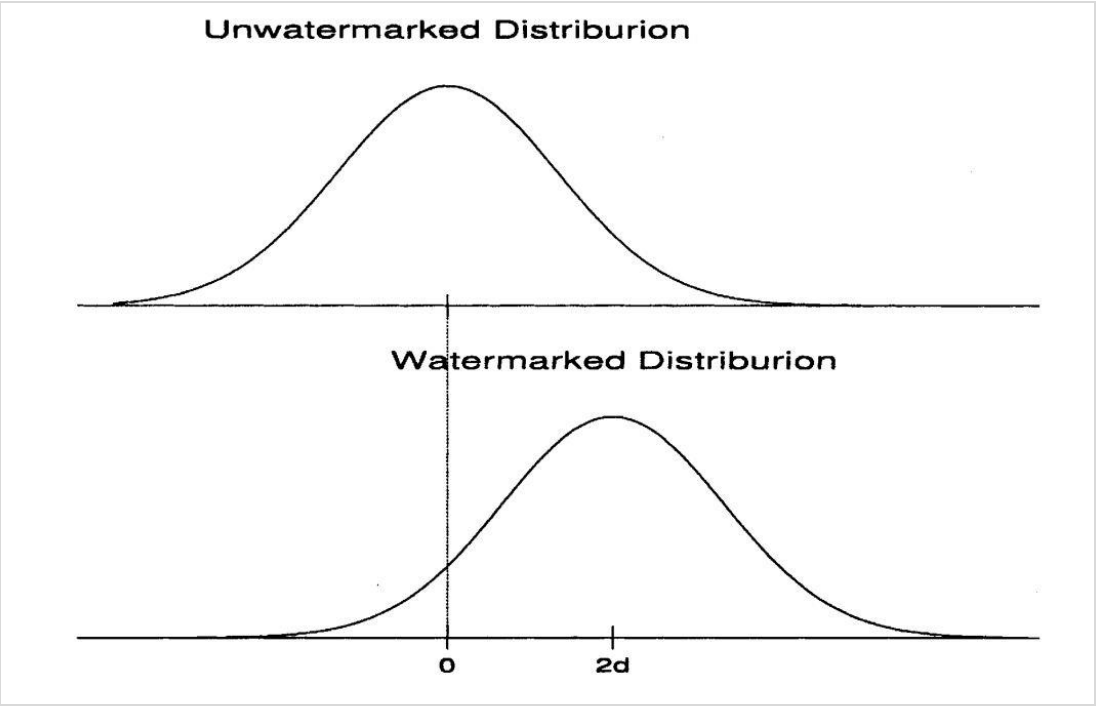
$$E\left[\bar{a}^* - \bar{b}^*\right] = E[(\bar{a} + d) - (\bar{b} - d)] \quad \ldots (5)$$

ile beklenen değer hesabı yapılabilir. Aynı zamanda beklenen değer E için d istatistiğini dışarda bırakmak gerekirse, (4) için eşitliğe ek olarak:

$$E\left[\bar{a}^* - \bar{b}^*\right] = E\left[\bar{a} - \bar{b}\right] + 2d \quad \ldots (6)$$

ifadesine eşit olur.

Burada (6)'dan çıkarımla d istatistiğinin ne kadar önemli olduğu matematiksel olarak ortadadır. Bu istatistik yerine göre anlamlı, yerine anlamsız ve çoğu zaman sabittir. Bu istatistiğin sabit olmasından ve beklenen değeri doğrudan etkilemesinden ötürü bu yöntem ile damgalama yapılırken yama çalışması şemasını da kullanmak dağılımı etkiler. Bu dağılım $2d$ olarak etkilenir.



Şekil 1

Şekil 1'de görüleceği gibi, damgalandıktan sonra dağılım d istatistiğinin 2 katı kadar X-Eksen noktasına referansla kaymış durumdadır [5].

İKİ KÜME YÖNTEMİNİN TERSİNE MÜHENDİSLİK İLE YORUMLANMASI

Bu yöntem LSB yöntemine kısmen benzerlik gösterse de aslında damgalama sonrasında daha güvenli olduğu söylenebilir. Bu söylem, yukarıda denklemi verilen damganın kaldırılma olasılıkları (1) düşünülürek söylenmiştir. Olasılıkların çok düşük olması demarking işlemini zorlaştıracağı için güvenlik tehditi oluşturması yine aynı olasılığa bağlıdır.

Yöntemin unutulmaması gereken bir noktası ise; damganın kaldırılması sırasında damgalayan şahısların bu damgayı, iki kümeyi ve d istatistiğini bilmesine rağmen Şekil 1'deki dağılıma uğradığı için tespit edememesidir. Bu durum tespiti zorlaştırdığı için telif hakkı iddiasını veya aitlik durumlarını yine (1) denklemindeki olasılığa bağlı bir şekilde azaltacaktır. Eğer telif hakkının ciddi bir düzeyde önemli olmadığı, damganın kaldırılmasının önemli olmadığı veya herhangi bir sebepten sadece damgalama yapılmak istenmesi gerektiği durumlarda iki küme yöntemi kullanılabilir. Yönteme dair zaafiyetlerin yanında algoritmasının karmaşık olmaması zaman ve maliyet açısından avantajdır.

Ayrıca d istatistiği damga üreticisi tarafından sabit tutulmaması algoritmayı bu yöntem için daha karmaşık bir hale getirir. Algoritmanın karmaşıklığının az olması bu yöntem için sayılabilecek en büyük avantaj iken karmaşıklığın arttırılması yönteme dair hiçbir avantaj bırakmayacak gibi gözükmektedir. Fakat yöntemlerin her biri düşünüldüğünde damganın kaldırılması işlemlerini tam performans ile yapamadığı göz önünde bulundurulursa büyük bir dezavantaj olmadığı görülebilir. Dolayısıyla bu damgalamada algoritmanın karmaşıklığı d eldesinin karmaşıklığı kadar olacaktır.

Diğer tüm ses damgalama yöntemleri gibi, bu yöntemin avantajları ve dezavantajları göz önünde bulundurularak yöntemin seçilmesi gerekir.

REFERANS VE KAYNAKÇA

[1] Bas, Patrick, J-M. Chassery, and Benoit Macq. "Geometrically invariant watermarking using feature points." IEEE transactions on image Processing 11.9 (2002): 1014-1028.

[2] 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

[3] Hernandez, Juan R., Martin Amado, and Fernando Perez-Gonzalez. "DCT-domain watermarking techniques for still images: Detector performance analysis and a new structure." IEEE transactions on image processing 9.1 (2000): 55-68.

[4] Solachidis, V., et al. "A benchmarking protocol for watermarking methods." Proceedings 2001 International Conference on Image Processing (Cat. No. 01CH37205). Vol. 3. IEEE, 2001.

[5] Yeo, In-Kwon, and Hyoung Joong Kim. "Modified patchwork algorithm: A novel audio watermarking scheme." IEEE Transactions on speech and audio processing 11.4 (2003): 381-386.

EKLER

Bitirme Projesi 1'e ait doküman, haftalık rapor ve ek bilgilerin paylaşıldığı github linki için tıklayınız.