TERSİNE MÜHENDİSLİK İLE SES DAMGALAMA YÖNTEMLERİNİN YORUMLANMASI

AUDIO WATERMARKING METHODS INTERPRETATION WITH REVERSE ENGINEERING

Fahrettin Horasan, Ahmet Mungan

Bilgisayar Mühendisliği Bölümü, Mühendislik Fakültesi, Kırıkkale Üniversitesi

fhorasan@kku.edu.tr

ahmetmungan@outlook.com.tr

ÖZET

Bu makale ses damgalama yöntemlerinin açıklanması, ses damgalamada veri şifreleme, tüm yöntemlerin tersine mühendislik ile yorumlanması ve sonuçları içerir. Öncelikle yöntemlerden ve bahsedilmiştir. Bu yöntemlerin hangi veri yapılarında işe yaradığı anlatılmıştır. Ses damgalama yaparken tercih edilecek yöntemlerin güvenirliği ve performansı konusunda fikir verir. Ayrıca veri gizleme (steganografi) kavramı ile sıkça karıştırılan kavramlardan olan veri şifreleme bu makalede özet olarak anlatılmıştır. Verinin şifrelenerek damgalanması, şifrelenmeden damgalanması veya hangi durumlarda şifrelenmesi gerektiği konularından bahsedilmiştir. Tüm bu içeriklerin tek başına kullanımı ile hangi yönlerinin kuvvetli olduğu tersine mühendislik ilkeleri ile tespit edilmiştir. En optimum çözümleri sunmaya çalışan tersine mühendislik disiplini, insansız sistemlerde yanıltıcı sonuçlar yüksek verebileceğinden, değerlendirme insan gözlemleri ile yapılmıştır.

Anahtar Kelimeler: Ses damgalama, tersine mühendislik, veri gizleme, steganografi.

ABSTRACT

This article includes explanation of audio stamping methods, data encryption in audio stamping, reverse engineering interpretation of all methods and results. First of all, the methods and are mentioned. It is explained in which data structures these methods work. It gives an idea about the reliability and performance of the methods to be preferred when stamping sound. In addition, data encryption, which is frequently confused with the concept of data hiding (steganography), is briefly explained in this article. It has been mentioned about the issues of stamping the data with encryption, stamping without encryption or in which cases it should be encrypted. With the use of all these ingredients alone, which aspects are strong have been determined by reverse engineering principles. Since the reverse engineering discipline, which tries to offer the most optimum solutions, can give misleading results in unmanned systems, the evaluation was made with human observations.

Keywords: Audio watermarking, reverse engineering, data hiding, steganography.

1. GİRİŞ

Telif hakları sosyal medyanın yaygınlaşmasıyla ve Web 2.0 gelişimi ile birlikte gündem konusu olmuştur [1]. Dijital ortamlardaki eser ve fikirlerin paylaşımında bir sınır olmadığı düşünülürse, telif haklarının önemi ortaya çıkacaktır. Hukuk alanında dijital ürünlerin telif haklarının korunması için aksiyonlar alınmıştır [2]. Dijital ortamlarda bu hakların savunulması için eser ve fikirler içerisine içerikten bağımsız veriler gizlenir [3]. Günümüzde birçok medya çıktısının içerisine veri/veriler aracılığı ile damgalama işlemi

yapılabilmektedir [4, 5, 6]. Damgalama işlemi için bu süreçte yöntemlerin biri/birkaçı seçilerek süreç başlar. Bu sürecin gereksinimleri göz önünde bulundurularak damgalama işlemi yapılır. Bu makalede ise spesifik olarak ses üzerinde şu ana kadar geliştirilen damgalama tekniklerinin yönteme dayalı biçimde açıklamaları yapılıp, bu yöntemlerin tersine mühendislik ile yorumlaması yapılacaktır [7]. Tersine mühendislik yorumu son yıllarda popülerleşen bir disiplindir [8]. Bu disiplin üç boyutlu modellemeler ile tanınmıştır [9]. Fakat bu disiplinin kullanışlı olması sebebiyle bilgisayar ve beşeri bilimlerde yaygın olarak kullanılmaya başlanmıştır [10, 11]. Tersine mühendislik disiplini ile ses verisi üzerinde damgalama yöntemlerine değinmek; ses verisine dair belirleyici unsurlardan olan kaliteyi pozitif anlamda etkilemesi beklenir. Veri kalitesinde özellikle son yıllarda artan veri miktarı/boyutu belirleyici olan işlemlerin yapılmasını zorlaştıran bir durumdur [12]. Bu durum veri üzerinde işlem yaparken ham olmayan birçok içeriğin işleme ve algoritmanın çalışması kısımlarına dahil edilmesiyle performanssız, kesikli ve süreksiz sonuçların eldesi kaçınılmazdır.

2. YÖNTEMLER

Ses damgalama yöntemleri genel anlamda dijital medya öğelerinin damgalanması ile kullanılan yöntemlerden bazılarıyla benzerlik gösterir. Hatta bu benzerlik özellikle görüntü damgalama yöntemlerinin bazıları ile aynı olabilmektedir. Örneğin LSB algoritması ile damgalama yöntemi literatürde hem görüntü hem de ses için kullanılan bir yöntemidir [13, 14]. Steganografi bilimi, internet dünyasında veri gizleme konusunda bir takım yöntemleri barındırır [15]. Fakat steganografi bilimi, ortaya koyulduğu tarih gereği teknolojinin gelişmesinden önceki dönemlere dayandığı için tek başına yeterli değildir. Bu yöntemler atası atası steganografi biliminin ışığında ve daha kesin sınırları olan yöntemlerdir. Bu makalede yöntemlerin kullanımı sonrasında alınan en iyi sonuçlar düşünülerek değerlendirilmesi yapılmıştır. Yöntemlerin karakteristik yönleri ve yönteme ait alt yöntemlerin olması işlem karmaşıklığı ve çeşitliliğini arttırmaktadır.

2.1. Yayılmış Spektrum

Ses dalgalarının üzerinde damgalama yapmayı öneren bu yöntem, sesin genlik ve frekans özelliklerini referans alır [16]. Yöntemin karakteristik özelliği ise ses dalgası üzerinde genliğin en yüksek değerine ulaştığı noktada veri gizlemeye dayanır. Gizlenecek verinin türü değişkenlik gösterse de karakteristik özelliğe bağlı kalınarak sinyal gömme işlemi yapılabilmektedir. Günümüzde damganın tespit edilebilirliği yüksek olması sebebiyle bu yöntemin güçlendirilmiş literatür kazanımları ve karma modelleri mevcuttur [17].

2.2. LSB

Bilgisayar bilimlerinde tüm veriler için temelde 0 ve 1 için yorumlanmasını esas alır. Bu sebeple bu yöntem medya öğelerinin damgalanmasında ortak olarak kullanılır. Temelde en anlamsız bit veya bitler tespit edildikten sonra o bitin değiştirilmesine dayandığı için ismini algoritmanın türünden alır. Bu yöntemin geliştirilmiş ve katmanlı olarak sistematik çalışmasını ortaya koyan yöntem de bulunmaktadır [18]. Ayrıca LSB algoritmasının hızlı çalışmasından ötürü en sık kullanılan yöntemlerden biridir.

2.3. İki Küme

Damgalama şemalarından iki adet küme seçilerek bu iki küme damgalandığı için ismini buradan almaktadır. Damga, belirlenen bu iki kümenin matematiksel farklarına dayanarak yapılır. Bu yöntem öne sürülen alt yöntemleri ile tanımlanmış ve ünlenmiştir [19].

2.4. Replika

Ses sinyalinin damgalanmamış halinden bir kesit alınarak damgalanmasıdır. Bu kesit modülü sözde-rassal bir dizi olarak seçilebildiği gibi alt yöntemlerin sunduğu algoritmalar ile belirlenebilir. Yankı gizleme alt yöntemi ile birlikte incelenmesi gereken bu yöntem, sinyalin ötelenmesi ve zamana referanslandırılması konusunda yardımcı olur [20].

3. VERİ ŞİFRELEME

Veri damgalama yöntemlerinde bazı açıkları kapatmak için, veri şifrelenerek gizlenir. Veri şifrelenirken genel itibariyle kriptosistemlerden yardım alınabildiği gibi kişisel şifreleme yöntemleri de kullanılabilir. Veri şifrelendiğinde karakterini kaybederse damgalama algoritmasında performans düşüklüğüne sebep olabilmektedir. Formatı gereği genel veri yapılarına uygun olan hill algoritması veri gizlemede yaygın olarak kullanılan kriptosistemlerdendir [21]. Veri yapısına uygun kriptosistem seçiminin doğru bir şekilde yapılması gerekir. Örneğin sadece karakterler üzerinde uygulanan kriptosistemler veri gizleme için işlevsiz kalabilmektedir. Aynı şekilde sadece nümerik değerler üzerinde çalışan kriptosistemler veri gizleme için yetersiz ve işlevsiz kalabilir. Göz önüne alındığında, veriyi gizlemeden önce şifrelemek ne kadar gerekli ise, doğru kriptosistemin seçimi de tüm sistem performansını doğrudan etkileyeceği için o kadar gereklidir. Bu duruma yardımcı olabilecek araştırmalar mevcuttur [22]. Bazı özel telif durumlarında kullanılan kriptosistemin tahmin edilebileceği gerçeği unutulmamalıdır.

En doğru kriptosistemin seçimi tersine mühendislik ile veri gizleme yöntemine yaklaşım ile ortaya çıkabilmektedir. Bu yaklaşımı çok parametreli ve ilkeleri zayıf tutarak, kurallara bağlı kalmadan yorumlayarak anlamak mümkündür. Veri şifrelenmesi mecburi bir durum ise öncelikle doğru bir damgalama yöntemi seçilmelidir. Damgalama yöntemi doğası gereği performanslı çalışabilir fakat sistemin başında mecburiyetten doğan veriyi şifreleme isteği sistemin performansında değişiklik yaratabilir. Eğer bir sistemde ses verisi üzerinde sıkça damgalama ve damganın kaldırılması işlemleri yapılıyorsa, sistemin performansını en az etkileyecek kriptosistemlerden kaydırmalı (sezar, vigenere vb. blok şifrelemeler) kriptosistemler kullanılabilir [23]. Fakat günümüzde kriptosistemlerin farklı alanlarda kullanılması sebebiyle yaygınlaştığı göz önüne alınırsa, kriptosistemleri saf bir şekilde kullanmak güvenilirliği azaltacaktır.

4. TERSİNE MÜHENDİSLİK

Yöntemler ve çevresinde gelişen alt yöntemlerin tekil kullanımı halinde tersine mühendislik ile yorum yapılması mümkün gibi gözükür. Kuralsız ama ilkeli yaklaşımın temeli budur. Eğer bir sisteme tersine yaklaşılırsa, sistem bileşenlerinin yapısı iyi bilinmelidir. Tersine mühendislik disiplini bilgelik seviyesi ve eğer varsa bu seviyenin üst kademelerinde bir birikim sahibi olmak yorumlama yapabilmek için faydalı olacaktır. Sistem bileşenlerinin en iyi şekilde tanınmasının yanı sıra bileşenlerin birleşip sistemsel sonuçlarının ve sistemin verdiği tepkilerin de bilinmesi gerekir. Bir bütün olarak incelendiğinde tersine mühendislik ile işlem yapabilmek, araştırma ve geliştirme aşamalarından sonra gelir.

Kriptosistemlerin zaafiyetleri ile ilgilenen kriptanaliz, bilinen şifre algoritmaları sistemlerinin kırılmasını esas alır. Kriptanaliz ile ses damgalamada kullanılan hill algoritması kırılabilirdir. Diğer tüm algoritmaların da kırılması mümkündür. Günümüzde kırılması en zor ve matematiksel alt yapısının ayrık logaritma problemine dayanan sistemlerin zaafiyeti söz konusudur [24]. Bu sebeple yaygın olarak kullanılan kriptosistemlerin tekil kullanımı zaafiyet yarattığı gibi, ses damgalama yöntemlerinin tekil kullanımı da bu örnekleme üzerinden zaafiyet yaratacağı kesindir. Ses damgalama yöntemlerinin tamamında yöntemin bilindiği durumlarda damganın kaldırılması için damga dedektör algoritmaları mevcuttur [25, 26]. Ataklara kapalı ve güvenli olması için ses damgalama

yöntemlerinde, yöntemler hibrit bir şekilde kullanılabilir. Tekil yöntemlerin tespit algoritmaları bulunduğu gibi, hibrit yöntemlerin tespit algoritmaları için tersine mühendislik disiplininden yararlanılabilir mi sorusunun cevabı aranmıştır.

Sesin sinyal bazında incelenmesiyle ortaya çıkan damgalama yöntemlerinden yayılmış spektrum yönteminde sesin genliği ve frekansı yüksek olduğu kısımlarda damgalama yapıldığı bilinir. Güvenlik açısından bu algoritmayı tam tersine, genliği ve frekansı en düşük kısımlarında uygulamak mümkündür. Örneklemeden de anlaşılacağı üzere farkında olmadan tersine mühendisliğin bu alanda kullanıldığı söylenebilir. Bu ve sesin sinyal bazında damgalandığı diğer yöntemlerde, korelasyon dedektörleri yardımıyla damga için uygun noktalar belirlenebilir [27].

$$r = \frac{\sum(xy) - (\sum x)(\sum y)/n}{\sqrt{(\sum x^2 - (\sum x)^2/n)(\sum y^2 - (\sum y)^2/n)}} \qquad (1)$$

Katsayısı olarak r standart gösterim belirlenirse (1)'deki denklem korelasyon katsayısıdır. Bu katsayı kadar ses sinyalinde, sinyalin darbe özelliği kullanılarak damgalama yapılabilir.

$$\frac{df(t)}{dt} = \lim_{\varepsilon \to 0^+} \frac{f(t) - f(t-\varepsilon)}{\varepsilon} \qquad (2)$$

Bunun tespiti için sinyalin birim darbe tanımı (2)'deki denklemde limit ile dikkate alınırsa, limitin sınır değerleri değiştirilerek sinyalin tüm noktaları incelenebilir. ε değerini tersine bir işleme tabi tutarsak, 0 gibi sözde-sabit bir değer yerine sonsuza götürüldüğü varsayılabilir. Bu varsayım beraberinde sesin sonsuz küçük parçadan oluşabileceği gerçeğini doğurur. Sonsuz küçük her parça için dedektör algoritmasının çalışması gerekir.

5. SONUÇ

KAYNAKÇA

[1] Kaynak, Selva, and Serhat Koç. "Telif Hakları Hukuku'nun Yeni Macerası: Sosyal Medya." *Folklor/Edebiyat* 21.83 (2015): 389-410.

[2] Bozbel, Savaş. *Fikri mülkiyet hukuku*. Oniki Levha Yayıncılık, 2015.

[3] Bender, Walter R., Daniel Gruhl, and Norishige Morimoto. "Techniques for data hiding." *Storage and Retrieval for Image and Video Databases III*. Vol. 2420. International Society for Optics and Photonics, 1995.

[4] Kirovski, Darko, and Henrique Malvar. "Robust spread-spectrum audio watermarking." *2001 IEEE international conference on acoustics, speech, and signal processing. Proceedings (Cat. No. 01CH37221)*. Vol. 3. IEEE, 2001.

[5] Potdar, Vidyasagar M., Song Han, and Elizabeth Chang. "A survey of digital image watermarking techniques." *INDIN'05. 2005 3rd IEEE International Conference on Industrial Informatics, 2005.*. IEEE, 2005.

[6] Asikuzzaman, Md, and Mark R. Pickering. "An overview of digital video watermarking." *IEEE Transactions on Circuits and Systems for Video Technology* 28.9 (2017): 2131-2153.

[7] Kim, Hyoung Joong, et al. "Audio watermarking techniques." *Intelligent watermarking techniques* 7 (2004): 185.

[8] Canfora, Gerardo, and Massimiliano Di Penta. "New frontiers of reverse engineering." *Future of Software Engineering (FOSE'07)*. IEEE, 2007.

[9] Wang, Jun, et al. "A framework for 3D model reconstruction in reverse engineering." *Computers & Industrial Engineering* 63.4 (2012): 1189-1200.

[10] Csete, Marie E., and John C. Doyle. "Reverse engineering of biological

complexity." *science* 295.5560 (2002): 1664-1669.

[11] Varady, Tamas, Ralph R. Martin, and Jordan Cox. "Reverse engineering of geometric models—an introduction." *Computer-aided design* 29.4 (1997): 255-268.

[12] Koyuncugil, Ali, and Nermin Özgülbaş. "Veri madenciliği: Tıp ve sağlık hizmetlerinde kullanımı ve uygulamaları." *Bilişim Teknolojileri Dergisi* 2.2 (2009).

[13] Singh, Ranjeet Kumar, Dilip Kumar Shaw, and M. Javed Alam. "Experimental studies of LSB watermarking with different noise." *Procedia Computer Science* 54 (2015): 612-620.

[14] 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.

[15] Kumar, Arvind, and Km Pooja. "Steganography-A data hiding technique." *International Journal of Computer Applications* 9.7 (2010): 19-23.

[16] Li, Rangkun, Shuzheng Xu, and Huazhong Yang. "Spread spectrum audio watermarking based on perceptual characteristic aware extraction." *IET Signal Processing* 10.3 (2016): 266-273.

[17] Kirovski, Darko, and Henrique Malvar. "Robust spread-spectrum audio watermarking." 2001 *IEEE international conference on acoustics, speech, and signal processing*. Proceedings (Cat. No. 01CH37221). Vol. 3. IEEE, 2001.

[18] 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.

[19] 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.

[20] Tekeli, Kadir, and Rifat Asliyan. "A comparison of echo hiding methods." *The Eurasia Proceedings of Science Technology Engineering and Mathematics 1* (2017): 397-403.

[21] Swain, Gandharba, and Saroj Kumar Lenka. "A dynamic approach to image steganography using the three least significant bits and extended hill cipher." *Advanced Materials Research. Vol. 403*. Trans Tech Publications Ltd, 2012.

[22] M. Yılmaz, S. Ballı, "Veri Şifreleme Algoritmalarının Kullanımı İçin Akıllı Bir Seçim Sistemi Geliştirilmesi", *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, Cilt: 2, No: 2, Sayfa: 18-28, 2016.

[23] Topaloglu, Nurettin, M. Hanefi Calp, and Burak Turk. "A Novel Data Encryption Algorithm Design and Implementation in Information Security Scope." *arXiv preprint* arXiv:1902.04418 (2019).

[24] Moldovyan, Nikolay Andreevich, and Aleksandr Andreevich Moldovyan. "Finite non-commutative associative algebras as carriers of hidden discrete logarithm problem." *Вестник Южно-Уральского государственного университета.* Серия: Математическое моделирование и программирование 12.1 (2019).

[25] Iwendi, Celestine, et al. "Keysplitwatermark: Zero watermarking algorithm for software protection against cyber-attacks." *IEEE Access 8* (2020): 72650-72660.

[26] Yu, Xiaoyan, Chengyou Wang, and Xiao Zhou. "A survey on robust video watermarking algorithms for

copyright protection." *Applied Sciences 8.10* (2018): 1891.

[27] Chen, Tianyu, et al. "Insight into split beam cross-correlator detector with the prewhitening technique." *IEEE Access 7* (2019): 160819-160828.