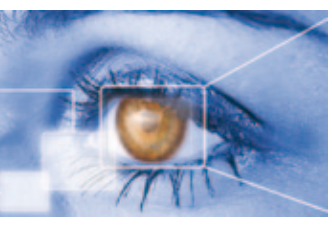
Çağatay Karabat

Steganografi ve Sayısal Damgalama: Geçmişten Günümüze Bilgi Gizleme Teknikleri

Bilgi saklama ve gizli haberleşme yöntemleri çok eski çağlardan beri insanoğlunun ilgisini çekmiş konulardır. Bilginin gizlenmesi ve yalnızca istenilen kişiler tarafından okunmasına izin verilmesi "steganografi" bilimi olarak adlandırılır ve tarihten bugüne kadar çeşitli amaçlarla kullanılmaktadır. Örneğin, günümüzde internet ve çoklu ortam ürünlerinin kullanımının gittikçe yaygınlaşması sonucunda telif hakları sorunu ortaya çıkmıştır. Bu sorunu çözmek amacıyla çoklu ortam ürünlerine, aidiyet bilgilerini içeren "sayısal damga" ekleme teknolojileri geliştirilmiştir. Göz ile fark edilemeyen bu sayısal damgalar aracılığıyla imge, ses ve video gibi çoklu ortam ürünlerinin içerisine ürünle ilgili ve ürüne özel çeşitli bilgiler yerleştirilebilmektedir. Bu gizli damgalar, o çoklu ortam ürününün kime ait olduğu, kimin tarafından ve nerede üretildiği, hangi tarihte üretildiği, seri numarası gibi, kötü niyetli kişilerin bilemeyeceği ve erişemeyeceği türden bilgileri içerir. Burada amaç, bu ürünlerin çoğaltılması, dağıtılması gibi yasal olmayan davranışların önüne geçmektir.

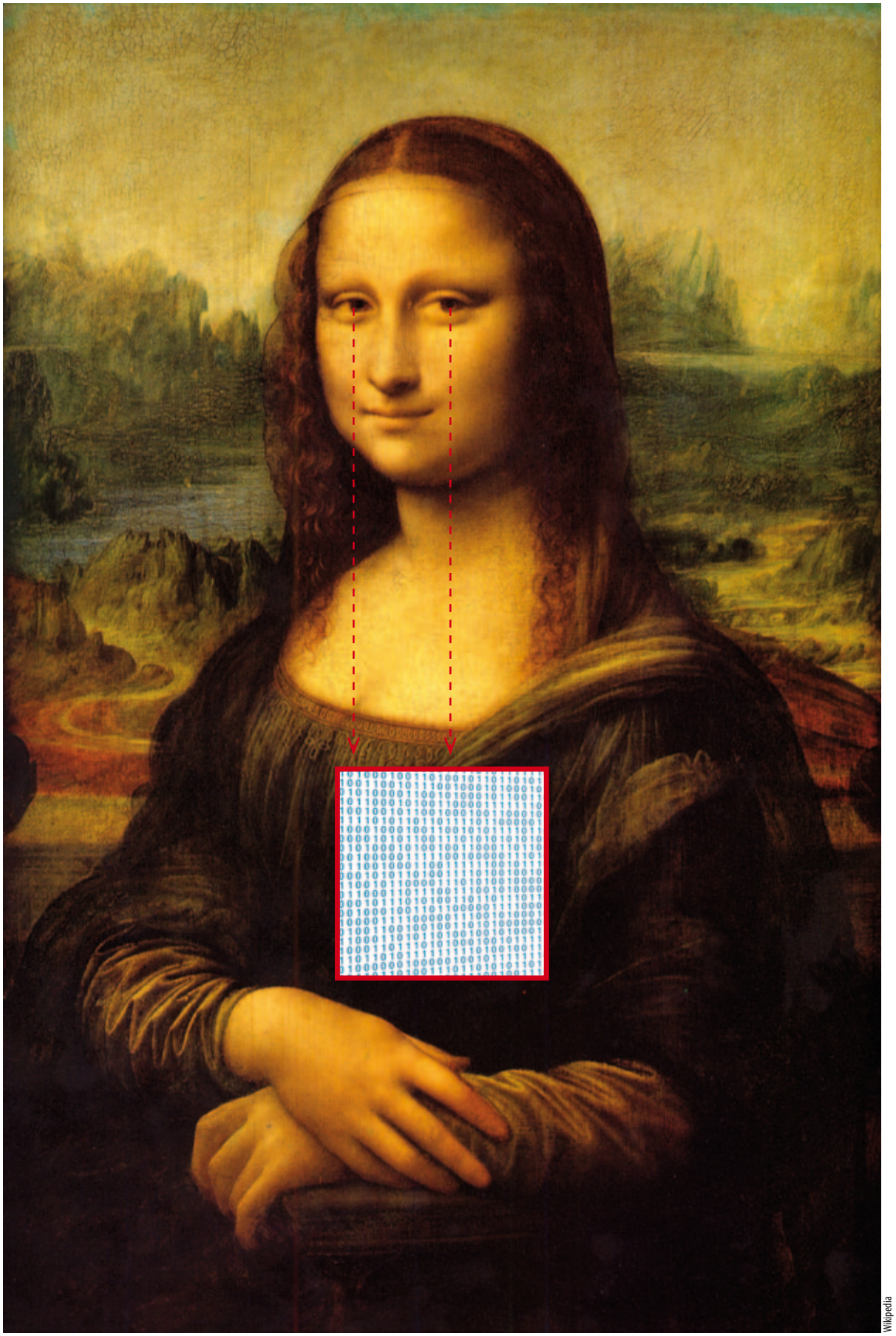
Steganografi: Gizli Haberleşme Sanatı

Steganografi terimi Eski Yunancada "gizli" anlamına gelen "*steganos*" ve "yazı" anlamına gelen "*graphia*" kelimelerinin birleşmesinden oluşmuştur. Diğer bir deyişle, steganografi gizli haberleşme sanatına verilen addır. Steganografinin kriptolojiye göre en büyük üstünlüğü, bir bilgiyi gören bir kimsenin gördüğü şeyin içinde gizlenmiş başka bir bilgi olduğunu fark edemiyor olmasıdır, dolayısıyla da kişi gördüğü bilginin içerisinde gizli bir bilgi aramaz. Steganografide amaç iki tarafın birbiriyle gizli haberleşmesi olduğu için bu tip sistemlere yapılabilecek olası bir saldırı ancak bu iki taraf arasındaki haberleşmenin fark edilmesi şeklinde olabilir.



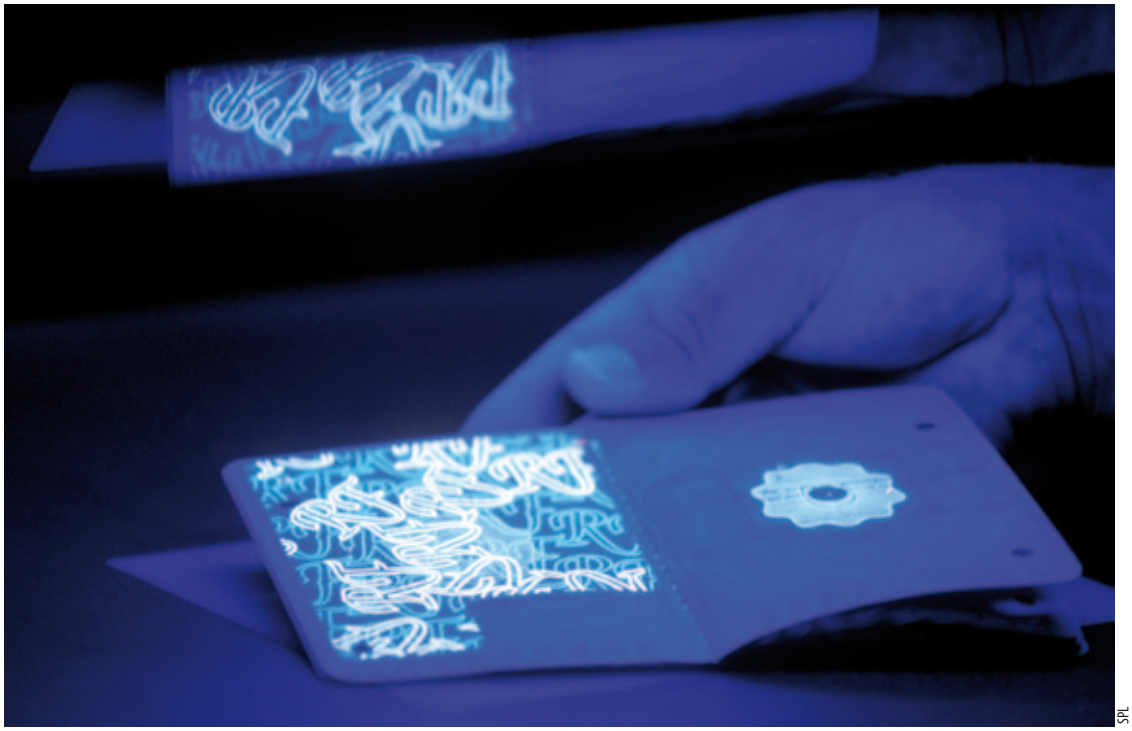
Tarihte steganografinin kullanıldığı ilk örneklerden biri milattan önceki çağlara aittir. Yunanlı tarihçi Herodotos'un bildirdiğine göre, MÖ V. yüzyılda Pers saldırısı sırasında, Yunan komutan Histiaeus, Susa Kralı Darius tarafından göz hapsine alındığı sırada, Anadolu'da bulunan Milet şehrindeki damadı Aristagoras'ı durumdan haberdar etmek için ona gizli bir mesaj göndermek ister. Tabii, bu mesajın Kral Darius fark etmeden Aristagoras'a ulaştırılması gerekmektedir. Bunu gerçekleştirmek için komutan Histiaeus bir kölenin saçını kazıtır ve mesajı kölenin başına dövme olarak yazdırır. Saçları uzayan köle Anadolu'ya gönderilir. Kimse tarafından dikkat çekmeden Aristagoras'a ulaşan kölenin saçları tekrar kazınır ve Aristagoras mesajı okur. Bu olay, gizli haberleşme sanatı olan steganografinin tarihte ilk kez kullanıldığı örneklerden biridir. Tarihte tahta tabletlere mesaj kazıyıp tabletin üzerini mumla kaplamak ve gizli mesajı okumak için daha sonra mumu eritmek, morötesi boya ile yazı yazabilen kalemlerle mektup yazmak ve gizli mesajı okumak için mektubu morötesi ışığa tutmak, yazılı bir metnin içindeki bazı harfleri, üzerlerine çok küçük bir delik delerek işaretlemek, böylece o harflerden gizli bir mesaj oluşturmak ve bu mesajı okumak için mektubu ışığa tutmak gibi yöntemler de kullanılmıştır. Tarihten bir başka örnek de, II. Dünya Savaşı sırasında Almanya'nın mikro-nokta teknolojisi kullanılarak geliştirdiği gizli haberleşme yöntemidir. Bu yön-

>>>



Wikipedia

Resmin içindeki sır: Steganografi ve sayısal damgalama yöntemleri ile herhangi bir resmin içerisine gizli bir bilgi yerleştirilebilir. Resmin içerisine gizli bilgi yerleştirme işlemi genellikle gözün algılayamayacağı frekans bileşenlerinin gizli bir anahtar kullanılarak değiştirilmesi suretiyle yapılmaktadır. Bu gizli bilgiye ise ancak gizli anahtara sahip olan kişiler özel bir damga çıkarma yöntemi kullanarak erişebilir.



SPL

Sayısal damgalama sistemlerinin genel süreçleri: Sayısal damgalamanın iki ana süreci vardır. Bunlardan ilki damga (gizli bilgi) gömme süreci, diğeri ise damga (gizli bilgi) çıkarma sürecidir. Resmin içerine gömülen damga alıcıya ulaşana kadar çeşitli saldırılara ve/veya bozulmalara uğrayabilir. Hatta bu gizli damgayı silmek ya da değiştirmek isteyen üçüncü kişiler de olabilir.

Resimde bir pasaportun içerisine gömülmüş olan gizli damgaların ultraviyole ışık altında ve belli bir algılayıcı cihaz kullanılarak ortaya çıkarılması gösteriliyor.

temde, gizli mesajların çeşitli teknolojiler yardımıyla nokta kadar küçültülüp mektuptaki sözcüklerde bulunan noktalı harflerin ve noktalama işaretlerinin üzerine yapıştırılarak saklandığı bilinmektedir. Aşağıda, yine II. Dünya Savaş'ında kullanılan başka bir steganografi örneği verilmiştir.

"Apparently neutrals protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretex for embargo on by-products, ejecting suets and vegetable oils."

Yukarıda verilen paragrafta her kelimenin ikinci harfi yan yana getirildiğinde *"Pershing sails from NY June 1."* cümlesi, yani *"Füze New York'tan 1 Haziran'da denize açılacak"* mesajı okunur.

İngiltere Başbakanı Margaret Thatcher'ın, 1981 yılında kabinesindeki bir bakan tarafından basına bazı belgeler sızdırılmasından sonra, bu olayın sorumlusunun kim olduğunu bulmak için her bakana verilen belgelerdeki yazıların boşluklarını bakanları tanımlamak için özel olarak ayarlatması, böylece bakanlara içeriği aynı ama biçimi farklı yazılar dağıtılması, bu sayede de gizli bilgileri basına veren bakanın yakalanması yakın geçmişten verebileceğimiz bir örnektir.

Günümüzde resim, video ve ses/müzik gibi çoklu ortam ürünlerinin kullanımının yaygınlaşmasıyla gizli mesajlar artık bu tip verilerin içerisine saklanıyor. Bilgi ve haberleşme teknolojilerinin gelişmesine paralel olarak bilgi saklama yöntemlerinin de gelişmesiyle, çok daha karmaşık matematiksel formüllere dayanan bilgi saklama yöntemleri geliştirildi. Örneğin, piksellerden oluşan sayısal bir imgenin piksel değerlerinde gözün fark edemeyeceği kadar küçük değişiklikler yaparak sayısal imgelerin içlerine gizli mesajlar saklanabiliyor. İmgenin büyüklüğü arttıkça daha fazla bilgi saklama şansı doğuyor. Aynı şekilde sayısal ortamdaki bir sesin ya da bir müzik parçasının içine, ses veya müzik bileşenlerini insan kulağının fark edemeyeceği şekilde değiştirerek gizli mesajlar saklanabiliyor. Burada dikkat edilmesi gereken nokta, gizli mesajın yetkisi olmayan kişilerce fark edilmesini engellemek. Bunu gerçekleştirmek için hem özgün veriyle içine bilgi gizlenmiş veri arasındaki farkın insan beyni tarafından algılanamaz olmasını, hem de aralarındaki farkın matematiksel olarak bulunamıyor olmasını sağlamak gerekir.

SPL

Sayısal damgalama ve steganografi gizli bilgiyi saklama teknolojileridir. Bu yöntemlerde amaç gizli bilgiye sadece gizli anahtara sahip olan yetkili kişiler tarafından erişilebilmesi ve diğerleri tarafından fark edilememesidir.

Tabii işin içine güvenliğin girdiği bazı durumlarda bu gizli haberleşmenin ortaya çıkarılması gerekir. İşin bu kısmında çeşitli steganaliz yöntemleri kullanılır. Steganaliz, steganografik yöntemler kullanılarak saklanmış gizli bilgilerin çeşitli matematiksel yollarla ortaya çıkarılması işine verilen addır. Günümüzde çok kolay bir şekilde kullanılabilecek birçok ücretsiz ve paylaşıma açık steganografi yazılımı internet üzerinden rahatlıkla bulunabiliyor. Ancak bu yazılımların yasadışı gruplar ve kötü niyetli kişiler tarafından kullanılması olasılığı ciddi güvenlik problemlerini de beraberinde getiriyor. Yasadışı gruplar steganografik yöntemler kullanarak, internet gibi herkese açık elektronik ağlar üzerinden çoklu ortam ürünlerinin (resim, şarkı, film gibi) içerisine gömdükleri bilgiler aracılığıyla gizlice haberleşebilirler. İnternet üzerindeki yoğun e-posta trafiği içindeki şifrelenmiş mesajlar dikkat çekebilirken, gizli mesajlar saklayan görüntü, müzik ve film dosyaları hiçbir şüphe uyandırmayabilir. Bu nedenle, steganaliz algoritmaları geliştirerek bu gibi gizli ve yasadışı haberleşmeleri deşifre etmek, ülke ve sivil halk güvenliği açısından çok büyük önem taşır.

Sayısal Damgalama: Telif Haklarının Yeni Koruyucusu

Son yıllarda internetin ve sayısal teknolojinin kullanımının hızla yaygınlaşması, çoklu ortam ürünlerinin üretimi, saklanması ve dağıtımı sorunlarını da beraberinde getirdi. Bu eğilim e-ticaret, e-sağlık, sayısal kütüphaneler ve izle-öde video sistemleri gibi pek çok gelişmiş sayısal ortam uygulamasının kullanımının gittikçe yaygınlaşmasıyla da artarak sürmeye devam edecek. Bu uygulamaların insan hayatına birçok rahatlık getirmenin yanı sıra sayısal ortamda oluşturulan ses, video ve resim gibi çoklu ortam ürünlerinin yasa dışı çoğaltılması, değiştirilmesi ve dağıtılması gibi pek çok telif hakkı problemini de beraberinde getirdiği gerçek. Son yıllarda imge, video ve ses/müzik gibi çoklu ortam ürünlerinin üreticilerini/dağıtıcılarını ve bu ürünlerin fikri haklarını ellerinde bulunduran hak sahiplerini en çok tehdit eden güvenlik konusu "analog geri dönüşüm problemi". Bu sorun ilk olarak Amerikan Sinemacılar Birliği (*Motion Picture Association of America*) tarafından 2002 yılında "analog delik" olarak adlandırıldı. Burada kullanılan "analog delik" terimiyle, aslında sayısal ortam ürününün insan gözünün görebileceği analog bir formata çevrildikten sonra yasa dışı olarak yeniden kaydedilmesi ifade ediliyor; diğer bir deyişle, sinemalarda kaçak çekim yapıp bunu CD'ye veya DVD'ye kaydeden kişilerin ve buna izin veren sinemaların tespit edilmesi sorunu. Aynı durum günümüzde müzik CD'leri için de geçerli. Bugün ülkemizde pek çok yerde yasa dışı CD satıcıları görmeye maalesef alışmış olmamız, bu sorunun ne kadar büyük olduğunun kanıtı.

Son yıllarda telif hakkı problemini çözebilmek için "sayısal damgalama" adı verilen yeni bir yöntem kullanılıyor. Sayısal damgalama, sayısal verilerin izinsiz kişiler tarafından kullanımını engellemek için önerilmiş yeni bir teknoloji. Sayısal damgalama yöntemlerinde, "aidiyet bilgisi" sayısal ortamda bulunan imge, video veya ses verisi içine, bu verilerin kalitesini bozmayacak ve insan beyni tarafından fark edilemeyecek şekilde saklanır. Örneğin, bir imgenin frekans spektrumundaki frekans bileşenlerinden gözün en az fark edeceği bileşenler değiştirilerek onların yerine saklanmak istenilen bilgiler yerleştirilir. Böylece, bu değişim insan beyni tarafından algılanamaz. Böyle bir imgenin telif haklarının kime ait olduğu, bilginin içine saklanmış sayısal damganın ortaya çıkarılmasıyla anlaşılır. Bu noktada, kullanılacak sayısal damganın korsanlar tarafından silinemez ve değiştirilemez olması çok önemlidir.

Sayısal damgalamanın kullanılabileceği diğer bir alan ise medikal görüntülerin elektronik ağlar üzerinde dağıtıldığı e-sağlık uygulamalarıdır. Bu ağlarda, medikal görüntülerin korunması, tanınması ve asıllanması gibi çeşitli güvenlik ve mahremiyet sorunları ortaya çıkıyor. Örnek bir uygulama alanı, bir medikal imgeye, hasta ile ilgili çeşitli kişisel bilgilerin sayısal damgalama yöntemleri kullanılarak gizlenmesidir. Bu uygulama sayesinde farklı hastaların çeşitli medikal görüntülerinin karışması önlenebilir; hasta bilgilerinin izinsiz kişilerce görülmesi ve kullanılması gibi istenmeyen durumların önüne geçilebilir. Geçmişte, medikal görüntüleri başkalarınınkiyle karıştığı için mağdur olmuş pek çok insan vardır.

Çağatay Karabat, İstanbul Üniversitesi Elektronik Mühendisliği Bölümü'nden 2005'te bölüm birincisi olarak mezun oldu. Sabancı Üniversitesi Elektronik ve Bilgisayar Bilimleri Bölümü'nde yüksek lisansını yaptı ve öğrenimi boyunca burada araştırma görevlisi olarak çalıştı. 2007'den beri TÜBİTAK UEKAE 'de araştırmacı olarak çalışıyor. Sayısal damgalama, steganografi, steganaliz, kriptolojik protokol tasarımı, RFID ve biyometrik güvenlik sistemleri alanlarında çalışmalar yapıyor. Ayrıca, çoklu ortam güvenlik sistemleri hakkında Avrupa Birliği projelerinde hakem olarak da yer alıyor.

Kaynaklar

Cox, Ingemar, Miller, Matthew L., Bloom, Jeffrey A., "Digital Watermarking", The Morgan Kaufmann Series in Multimedia Information and Systems, 2002.
Cox, Ingemar, Miller, Matthew L., Bloom, Jeffrey A., Fridrich, Jessica, Kalker, Ton, "Digital Watermarking and Steganography", The Morgan Kaufmann Series in Multimedia Information and Systems, 2007.
Karabat, Çağatay, "Robust Blind and Non-Blind Detection for Digital Watermarking", Sabancı Üniversitesi, Master Tezi, 2007.
Karabat, Çağatay, Keskinoz, Mehmet, "Watermark Detection Using Channel Estimation in the Quantization Based Watermarking System", IEEE International Information Hiding and Multimedia Signal Processing Conference, IIHMSP, Harbin, Çin, 2008.
Karabat, Çağatay, Keskinoz, Mehmet, "Robust Non-Blind Detection for Spread Spectrum Watermarking System", IEEE International Information Hiding and Multimedia Signal Processing Conference, IIHMSP, Harbin, Çin, 2008.
Karabat, Çağatay, "Adaptive Threshold Based Robust Watermark Detection Method", International Workshop on Digital Watermarking, IWDW, s. 139-151, Pusan, Güney Kore, 2008.
Karabat, Çağatay, "Space Time Block Coding for Spread Spectrum Watermarking Systems", International Workshop on Digital Watermarking, IWDW, s. 266-277, Pusan, Güney Kore, 2008.