Journal of Architecture, Engineering & Fine Arts

2019 1(1): 25-35

Available online at http://dergipark.gov.tr/artgrid

Review

PRINTER STEGANOGRAPHY, YELLOW DOT ANALYSIS - A MINI SURVEY

Faruk Takaoğlu[1], Mustafa Takaoğlu[2,*]

[1] TÜBİTAK, BİLGEM, Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü, Kocaeli.
[2] İstanbul Aydın Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, İstanbul.

ORCID ID[1]: 0000-0003-0828-2017
ORCID ID[2]: 0000-0002-1634-2705

***** Corresponding Author: mustafatakaoglu@aydin.edu.tr; Tel.: 444 1 428 (22109)

Received: 23 May 2019; Accepted: 21 June 2019; Published: 28 June 2019

Abstract

Nowadays, with the rapid development of technology, color laser printers, scanner, and imaging devices have become ubiquitous devices in our daily use. Distributed system architectures and logic are becoming increasingly popular. The products that we buy through printers, scanners, and similar devices in our common use area are marked by physical steganography method to follow the illegal activities. These markings are not known by most of society. This data hiding method, which was processed as yellow dots, was discussed in our study, and information about the subject was shared.

Keywords: Yellow Dot Analysis; Counterfeit Protection System; Machine Identification Code; Printer Steganography.

Please cite this article as: Takaoğlu, F. ve Takaoğlu, M. (2019), Yazıcı steganografisi, sarı nokta analizi – bir mini derleme. *ArtGRID-Journal of Architecture, Engineering & Fine Arts, 1*(1), 25-35.

Derleme

YAZICI STEGANOGRAFİSİ, SARI NOKTA ANALİZİ – BİR MİNİ DERLEME

Özet

Günümüzde teknolojinin hızlı gelişmesi ile renkli lazer yazıcı, tarayıcı ve görüntüleme cihazları günlük kullanımımızda çokça rastlanılan cihazlar haline gelmiştir. Dağıtık sistem mimarileri ve mantığı giderek yaygınlaşmaktadır. Ortak kullanım alanımızda bulunan yazıcılar, tarayıcılar ve benzeri cihazlar vasıtasıyla aldığımız ürünlerin en temelinde illegal aktivitelerin takip edilmesi amacı ile fiziksel steganografi yöntemi ile işaretleme yapılmaktadır. Bu işaretlemeler toplumun çoğu tarafından bilinmemektedir. Sarı noktalar olarak işlenen bu veri gizleme yöntemi çalışmamızda ele alınmış ve konu ile ilgili bilgiler paylaşılmıştır.

Anahtar Kelimeler: Sarı Nokta Analizi; Sahtecilik Koruma Sistemi; Makina Kimlik Kodu; Yazıcı Steganografisi.

1. GİRİŞ

Aitlik günümüzde birçok alanda kesinleştirilmesi gereken bir konu olarak karşımıza çıkmaktadır. Gelişiminin başından bu zamana kadar içinde bulunduğumuz internet çağının etkisi ile üretilen çeşitli dijital ve fiziksel ürünlerin kime ait olduğunun sorgulanması için çeşitli yöntemler geliştirilmiştir. Günümüzde geliştirilen aitlik ispatlama yöntemlerinin ve uygulamalarının çoğu kullanıcılar tarafından farkına varılamayacak şekilde geliştirilmiştir. Farkına varılarak yapılan aitlik ispatlama yöntemleri genellikle ticari kaygı güdülen unsurlarda tercih edilmektedir. Böyle bir uygulamanın yapılmasının sebebi üretilen unsurun başkaları tarafından kullanılmasının ve gelir elde edilmesinin engellenmesidir. Dijital ürünlerde kullanılan bu tarz yöntemlere filigran veya "Watermark" denilmektedir (Sönmez, Kaynar ve Takaoğlu, 2018). Şahısların farkına varamayacakları şekilde üretilen aitlik ispatları ise genellikle, sadece sahibinin bildiği imza niteliğindeki bir dijital veya fiziksel bilginin eser üzerine gizlenmesi ile yapılmaktadır. Bilim dünyasında bir unsuru başka bir masum unsur içerisinde gizleme işlemlerinin bütününe steganografi denilmektedir. Bu kelime antik yunan dilindeki gizli anlamına gelen "steganos" ve yazma anlamına gelen "graphein" kelimelerinin birleşiminden türetilmiştir (Takaoğlu, 2016).

Günümüzde dijital ve fiziksel aitlik bilgilerinin gizlenmesinde kullanılan steganografi aynı zamanda gizli haberleşme çalışmalarının da en önemli uygulama alanlarından biridir. Steganografinin kullanıldığı alanların stratejik önem arz etmesinden dolayı yaygın olarak kullanılmakta ancak aynı oranda içeriği bilinmemektedir. Bilişim sektöründe mesai harcayan kimselerin haberdar olduğu alanlardan biri olan steganografinin, fiziksel uygulama alanlarından çokça bilinenleri; kıymetli evraklar ve banknot paraların üzerindeki filigran görselleridir. Son dönemlerde renkli lazer yazıların fiziksel steganografi uygulaması yaptıkları EFF-Electronic Frontiers Foundation tarafından tespit edilmiştir. Bu tespit üzerine ilk kez 2007 tarihli Chaos Communication Camp'de detaylı bir bilgilendirme yapılmıştır (Beusekom, Shafait ve Breuel, 2013). 1980 yıllarda renkli lazer yazıcıların, renkli tarayıcıların ve yüksek çözünürlüklü görüntüleme sistemlerinin hayatımıza girmesi ile birlikte evrak ve banknot para sahteciliğinde vb. illegal aktivitelerde artış gözlemlenebileceği

için buna önlem alınmak istenmiştir. Önlem olarak renkli lazer yazıcılarda çıplak insan gözü ile gözlemlenmesi çok zor boyutlarda olan ve yansıtma özelliği beyaz kâğıt üzerinde en az olan sarı renkteki noktalardan bir desen eklenmiştir. Bu desen temel olarak yazıcının marka, model, seri no, baskısının yapıldığı tarih ve saati evrak üzerine bir mantık ile işlemektedir (Beusekom, Schreyer ve Breuel, 2010). Bu desen her model yazıcıda farklılık göstermektedir. EFF Xerox marka yazıcıların sarı nokta desenlerini çözebilmeyi başarmıştır.

Günümüzde piyasada çoğunlukla kullanılan yazıcıların sarı nokta desen verilerini tanımlayıp çözebilen bir yazılımı, "Japanese Business Machine Association - JBMA" Japon iş makinaları birliği tarafından geliştirilmiştir ve sadece belirli ülkelere satış işlemi yapılmaktadır (Beusekom, Shafait ve Breuel, 2013). Bu uygulamanın 2000'li yıllarda bu kadar duyulmasının sebebi, Amerikan Ulusal Güvenlik Ajansı (NSA-National Securtiy Agency)'nın bir çalışanının kurum içerisindeki gizli bir belgenin fiziksel çıktısını alarak bir haber kurumu "The Intercept"e iletmesidir (Buck, 2018). Gizlilik çerçevesinde paylaşılan haberde kaynak belirtilmemiştir ancak NSA sarı nokta analizi kullanarak alınan çıktıların hangi tarihte, hangi saatte ve hangi yazıcıdan alındığını tespit ederek bilgiyi sızdıran kişinin işine son vermiştir. Bu ve benzer yazılımın bulunduğu inceleme laboratuvarlarında gönderilen delil ya da örnek kâğıttan, evrak üzerindeki sarı noktaların tanıtım kodu elde edilir. Bu kod üzerinden cihazın markası ve üreticisi elde edilebileceği gibi üretici firmaya kod iletilerek veri tabanından hangi bayi ve/veya son kullanıcıya satıldığı bilgisi elde edilebilir. Daha sonrasında insanlar güvenlik unsuru olarak tasarlanan sarı nokta analizlerinin aynı zamanda evlerimizde bulunan çoğu yazıcı tarafından kullanıldığını ve bu durumun kişisel ve özel hayatın gizliliğinin ihlalini doğurduğunu savunmaktadır. MIT Media Lab.'da CCCG, Computer Counter Culture Group Sahtecilikten Koruma Sistemi, SKS, kodlarının kullanılmasının engellenmesi için bir kampanya başlatmıştır. Farklı bir bakış açısı ile kullanılan bu SKS kodlarının illegal ve terörist aktiviteleri engelleyebileceği için kullanılması taraftarı olan gruplarda bulunmaktadır.

Bu yöntem ve tekniklerin anlaşılıp çözülebilmesinin faydalı olduğu alanlara örneğin fatura yazım işlemlerinde sahte faturanın başka bir yazıcıdan çıktığının veya üzerine tekrar basım yapılarak var olan sarı nokta desenlerinde bozulmalara sebep verdiğini ispat edebilir. Bir başka örnekle; eğer incelenen belge hakkında araştırma yapılıyorsa ve ortamdaki yazıcının SKS kodu biliniyorsa evrak incelenerek SKS kodu üzerinden yazıcı hakkında bilgi edinilebilir. Eğer evrak başka bir SKS kod içeriyorsa bu durumda evrakın dışarıdaki başka bir yazıcıdan yazıldığı anlaşılabilir ve evrak üzerinde başka bir inceleme yapmaya gerek kalmaz. Sarı nokta desenlerinde evrakın çıktı veya kopya olup olmadığını anlamak için desen içerisinde bir grup sarı nokta bulunur. Bu noktaların değişimi incelenerek evrakın yazıcıdan baskı yapıldığı yâda gerçek evraktan kopya alınarak baskılandığı anlaşılabilir. Bu konu üzerinde farklı görüşler olmasını bir kenara bırakarak, çalışmamızda sarı nokta analizlerinin teknik detayları hakkında bilgi verilmiştir.

2. TEKNİK ALAN

Sarı nokta analizi veya "YellowDots" yukarıdaki giriş bölümünde bahsedildiği üzere evrak üzerine gözle görülmesi zor olan sarı noktalardan oluşan bir desen basılarak yazıcı ve eğer varsa kopyalandığı belge hakkında bilgi vermektedir. Bu sistem her yazıcıda farklı tür ve şekillerde görülmektedir. Kullanılan desenler yazıcıdan yazıcıya göre değişebileceği gibi aynı zamanda sarı nokta yerine mavi nokta kullanılabilir. Ayrıca kullanılan tüm desenlerin evrak üzerindeki yayılmaları farklılık gösterebilmektedir. Sarı noktalar teknik terminoloji olarak sahteciliği ve illegal aktiviteleri engellemek amacı ile tasarlandıkları için Sahtecilikten

Koruma Sistemi, SKS, olarak tanımlanmaktadırlar. Bu noktaların oluşturduğu desen çözülebilmesi için tekrar eden alt desenin tespit edilmesi gereklidir. Bu alt desenden çıkarılan bilgilere ise Makine Kimlik Kodu, MKK, denilmektedir. Bazı desenler çoğu kesim tarafından çokça bilinmekte ve bazı desenlerin markalara göre karakteristik özellikleri bulunmaktadır. Örneğin Hp markalı yazıcıların desenlerin genellikle "L" harfine benzer sarı nokta alt desenleri ile başlamaktadır (Buck, 2018).

Farklı şekil ve formlarda evrak üzerine işlenebilen sarı noktalar 0.006 inç 0,1524 milimetre boyutlarındadır. 600 dpi çözünürlükte her nokta 4 piksele denk gelmektedir. Noktalar beyaz evrak üzerinde yansıtma özelliği en düşük olan renklerden biri olduğu için sarı renklerde basılmış böylelikle insan gözü ile görüntülenmesi zorlaştırılmıştır. Sarı renkli noktaları net görüntüleyebilmek için KYM-Kırmızı/Yeşil/Mavi formatındaki resimlerin mavi renkli bandında inceleme yapılması gereklidir. Sarı nokta varlığı incelenmek istendiğinde resmi bantlarına ayırmaksızın UV-Ultraviyole ışık kullanılarak görüntülenmesi sağlanabilir. Görüntülenen desenlerin evrak üzerindeki dağılımı değişiklik göstermektedir. Sarı noktalar incelendiğinde belirli bir desen formunun evrak içerisinde belirli aralıklarla ayrık olarak tekrar edildiği görülebilir. Birbiri ardına bitişik tekrar eden desenler görülebilir veya anlaşılması zor olması için geliştirilen birbirinden bağımsız, bitişik, karmaşık ve kaotik desenler içerebilir (Khanna, Mikkilineni, Chiu, Allebach ve Delp, 2008). Şekil 1'de sarı nokta Steganografisi örneği verilmiştir.

Şekil 1. Sarı Nokta Steganografisi Örneği.

Sarı noktaların anlamlandırılması ve oluşturulmuş desenlerin arkasında yatan mantığın zor olması ve detaylı incelemelere gereksinim duymasından dolayı, ilgili çalışmalarda bir kısım araştırmacı sarı noktaların analiz edilmesi ve tanımlanması için çalışırken diğer araştırmacılar

ise sarı nokta analizinin sonucu olan yazıcı tanımlama işlemini sarı noktaları incelemeden yapmak istemiştir.

Nitin Khanna ve arkadaşlarının yapmış oldukları çalışmada kamera tanınması için kullanılan sensör gürültüsünün tanınmasından esinlenerek yazıcılar için uyarlanmıştır. Amaç yazıcının fiziksel parçaları ve üretiminden kaynaklanan temel gürültü unsurlarının karakteristiğini bulmak ve bu gürültüyü tanıyarak yazıcının marka ve modelinin belirlenmesidir. Gürültüyü tanıyabilmek için yazıcıdan çıkan evrak üzerindeki PRNU-Photo Response Non-Uniformity değerleri analiz edilmiştir. Evrak üzerinden elde edilen özellikler Destek Vektör Makinesi Algoritması, DVM, kullanılarak evrakın hangi yazıcıdan çıktı tahmin edilip sınıflandırması tamamlanmıştır. DVM modelinde yapılan bu sınıflandırma ve tanıma çalışması yazıcı ve tarayıcı için ayrı ayrı yapılmıştır. DVM yönteminde %92,3'lük bir başarı oranı yakalanmıştır. Bu çalışma ve benzeri çalışmalarda cihazın seri numarası, evrakın yazıldığı tarih ve saat gibi bilgilerin kesin olarak elde edilmesi mümkün değildir. Aynı zamanda yazıcının seri numarası bilinemediği için bu yöntemle cihazı satan mağaza ve alıcı müşteriye ulaşmak imkânsızdır (Khanna ve diğerleri, 2008).

Sarı nokta analizi ile yazıcıdan çıktısı alınan bir evrak ile tarayıcıdan kopyalanan bir evrakın farkı desen içerisindeki değişimlerle gözlemlenebilmektedir. Schreyer ve arkadaşları ayrık kosinüs dönüşümü özellik değerlerini evrak üzerinde analiz ederek 400dpi çözünürlükte yazıcıdan alınmış ve kopyalanmış evrakların birbirilerinden ayırt edilebilmesini başarmışlardır (Schreyer, 2009, Schulze, Schreyer, Stahl, ve Breuel, 2008, Schulze, Schreyer, Stahl, ve Breuel, 2009). Jaing ve arkadaşları DCT özelliklerini kullanarak SVM sistemi eğitmiş ve yazıcı marka model tahmini yapılamasını sağlamışlardır. Ancak veri setleri ufaktır 6 adet yazıcı modeli bulunmaktadır (Jiang, Ho, Treharne, ve Shi, 2010).

Sarı noktalar kullanılmadan da yazıcıların marka ve modellerinin tahmin edilmesi çalışmaları yapılmıştır. Bu yaklaşımla ilgili olarak Gazi N. Ali ve arkadaşlarının yapmış oldukları çalışmada (Ali, Mikkilineni, Chiang, Allebach, Chiu, ve Delp, 2003) yazıcıların kâğıtları bükme ve/veya ana yazıcı rulosuna alma frekanslarından faydalanılarak tanınmasını amaçlamışlardır. Yazıcılardan çıkan çıktıları farklı lazer tarayıcılarda en az 3 kez tarayarak elde edilen görüntülerdeki çizgilerin değişimlerine Fourier analizi yapılmıştır. Sonuçta çıkan frekans-absorbans çizelgesine göre yazıcı modelleri birbirilerinden ayrıştırılmaya çalışılmaktadır.

Yazıcıların istatistiksel ve/veya piksel tabanlı özellikleri kullanılarak tahmin edilmesi mümkün olabilmektedir. Mikkilineni ve arkadaşlarının yapmış oldukları çalışmada (Mikkilineni, Chiang, Ali, Chiu, Allebach ve Delp III, 2005) evrakların aitliğinin ispatlanması için Gray Level Co-Occurance Matrix-GLCM yöntemi kullanılmıştır. Makalede iki farklı açıdan evrak aitliğinin ispatlanması amaçlanmıştır. Bunlardan ilki pasif olarak adlandırılan bu yöntem doküman içerisindeki "intrinsict" parametrelerin bulunup yazıcı hakkında bilgi sahibi olunmasını amaçlar. İkinci olan aktif yöntemde ise "extrasinct" parametre/imza eklenmesidir. Bu işlem yazıcının işlem mekanizmalarına modülasyon getirilerek cihazın evrakı yazdığı zaman tarih ve model seri no gibi bilgilerini evrak üzerine kodlaması sağlanmaktadır.

Diğer bir taraftan sarı noktaların analiz edilerek çözülmeye çalışıldığı çalışmalarda olmuştur. Bu çalışmalarda daha öncesinde EFF'in yaptığı gibi sarı nokta desenlerinin diziliş şemasını çözmek yerine daha çok EFF'in oluşturduğu veri tabanı kullanılarak bu verilerden elde edilen sarı nokta desenleri ile evrakların ait oldukları yazıcılar tahmin edilmeye çalışılmaktadır.

Buna örnek olarak bir diğer çalışmada J.van Beusekom ve arkadaşları (Beusekom, Schreyer, ve Breuel, 2010) tarafından Janis S.Tweedy'nin geliştirdiği method kullanılarak sarı nokta alt desenleri evrak içerisinde bulunarak yatayda ve düşeyde birbirilerine karşı aralarında bulunan mesafelerinin ölçülerek yazıcıların kümelenmesi sağlanmaktadır. Yapılan çalışmada 13 adet farklı Sahtecilikten Koruma Sistemi, SKS, kümesi oluşturulmuş ve incelenen sarı nokta desenlerinin bu küme içerisinde yer alan farklı yazıcı türlerine ve üreticilerine atama yapılabildiği belirtilmiştir.
Peter'in yapmış olduğu bir diğer sarı nokta hakkında bilgilendirme içeren çalışmada sarı nokta desenleri ve bu desenlerin içeriği, markalara göre desen karakteristik farklılıkları ve bu desenlerin tanımlama yaparken nasıl kullanılacağı ve içerisindeki fenomenlerin anlamlandırılması hakkında detaylı bir çalışması olmuştur (Buck, 2018).

3. SARI NOKTA ANALİZİ ÇÖZÜM ADIMLARI

Bir MIC kodunun fiziksel ve dijital olarak anlaşılması ve daha sonrasında çözülümünün sağlanması için temel olarak aşağıdaki adımların tamamlanması gereklidir:

- İdeal görüntüleme sisteminin oluşturulması
- Desen tanımlama işlemlerinin yapılması
- Bilgi / Veri çıkarımı işlemlerinin yapılması

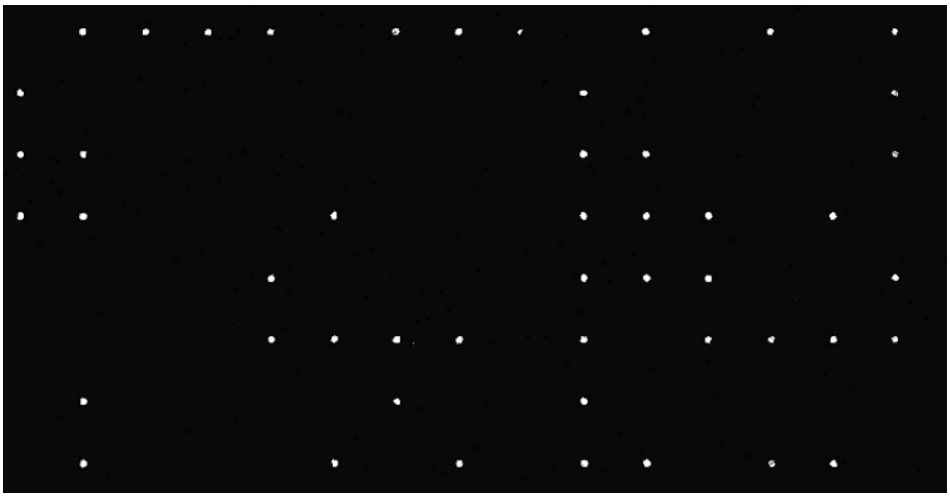
3.1. İdeal Görüntüleme Sisteminin Oluşturulması

Görüntüleme sistemi daha öncesinde bahsedildiği gibi sarı noktaların insan gözü ile görülemeyecek kadar ufak ve farkına varılmalarının zor olması istendiği için sarı renklerde basılmasından dolayı uygun görüntüleme ortamının oluşturulması ile alakalıdır. Nokta boyutlarında olan yaklaşık 0.006 inç veya 600dpi çözünürlükte 4 piksel boyutuna denk gelen sarı noktaların incelenmesi için mikroskop vb. yakınlaştırma cihazlarının kullanılması ilk işlemlerden biri olabilir. Normal gözle görülebilmesi için sarı rengin en çok yansıtılırlık özelliği gösterdiği ultraviyole ışık türü tercih edilerek farkına varılabilir. Dijital olarak sarı noktalar analiz edilmek istenildiğinde renkli görüntü formatında uygun yakınlık değerinde veya büyütme oranında elde edilen görüntülerin mavi renk bandında inceleme yapılması gereklidir. Bazı yazıcı marka ve modellerinde sarı noktalar yerine mavi noktalarda kullanılmıştır. Bu noktaların analizi için renkli görüntünün yeşil renk bandında incelme yapılarak baskı yapılan noktaların varlığına ulaşılabilir. Şekil 2'de gri formatta sarı nokta analizi paylaşılmıştır.

Şekil 2. Gri Formatta Sarı Nokta Analizi.

3.2. Desen Tanımlama İşlemlerinin Yapılması

Uygun görüntüleme sistemi oluşturulduktan sonra yapılması gereken desenin tanımlanabilmesi işlemleridir. Temel görüntü işleme ve morfolojik işlemleri içeren bu alanda yapılması gereken kâğıt ön yüzü ve arka yüzünün birbirinden ayırt edilebilmesidir. İncelenen evrak üzerinde birbirinden farklı bölgeler, yazılar, gürültüler ve şekiller sarı noktalarla kesişebilir veya iç içe geçebilir. Böyle durumlarda sarı noktaların diğer tüm etmenlerden olabildiğince düzgün bir şekilde ayrıştırılması gereklidir. Renkli resmin mavi bandından elde edilen görüntü gri tonlarında bir görüntüdür. Bu görüntüyü sadece siyah ve beyaz renklerin olacağı "binary form" 0-sıfır veya 1-bir 'lerden (0 ve 255 'de olabilir) oluşan bir görüntüye çevrilmelidir. Bu tarzda bir dönüşüm ile görüntünün arka ve ön planı birbirinden ayrışmış olur. Bunun sağlanabilmesi için "binarization" olarak adlandırılan eşikleme yöntemleri kullanılmaktadır. Bu yöntemler eşikleme değerlerini hesaplama türlerine göre ikiye ayrılmaktadırlar. İlk kategori küresel eşikleme içeren metotlardır. İkinci kategori ise yerel eşikleme içeren metotlardır. Teknik alanda bahsedildiği üzere yazıcıların evrak üzerinde bıraktıkları gürültü ve lekeler bilinmektedir. Bu lekeler ve gürültüler boyut olarak sarı noktalar ile aynı veya daha büyük boyutlarda olabilmektedirler. Lekelerin böyle durumlarda sarı nokta olarak algılanması veya uygun eşikleme değeri seçilemediği durumlarda gürültü olarak nitelendirilebilecek sarı noktaların arka plan rengi olarak sınıflandırılarak kaybolması söz konusu olabilir. Bu ve benzeri negatif olaylar göz önünde bulundurulduğunda Sauvola'nın "local adaptive binarization" yöntemlerinin (Sauvola ve Pietikainen, 2000) işlemsel olarak daha hızlı ve daha güvenilir bir tercih olduğu Beusekom ve arkadaşları tarafından belirtilmiştir (Beusekom, Shafait ve Breuel, 2013). Ancak incelenen evrakın üzerinde yer alan yazı, şekil ve bölgelere göre OTSU algoritması (Otsu, 1979) tercih edilebilir. Şekil 3'de OTSU algoritması sonucu elde edilen sarı nokta analizini görebilirsiniz.

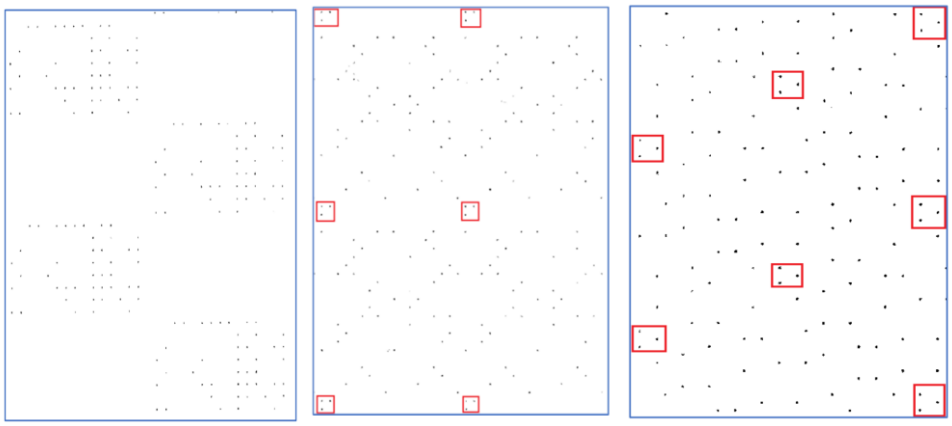


Şekil 3. OTSU Sonucu Sarı Nokta Analizi.

Bu aşama tamamlandıktan sonra elde edilen resim sadece siyah ve beyaz bölgelerden oluşan bir haldedir. Bu resmin gürültülerden temizlenmesi için morfolojik ve temel görüntü işleme metotlarından geçirilir. Morfolojik olarak sırasıyla "dilation" ve "erosion" işlemleri uygulanarak "quadratic" maskeleme yapılabilir. Daha sonrasında resim içerisinde bulunan 4 pikselden büyük noktalar sarı nokta harici olarak kabul edilerek temizlenebilir. Birbiri üzerine geçmiş veya şekil olarak nokta boyutundan farklı olan resim içi görseller sarı nokta harici olarak resimden kaldırılarak resim içerisinde sadece sarı nokta bölgeleri bırakılabilir.
Elde edilen bu görüntüden sonra desen tanımlama işleminin yapılması gereklidir. Literatürdeki çalışmalarda desenleri görsel olarak kullanıcı tarafından tanınması ve belirlenmesi (Buck, 2018) olduğu gibi aynı zamanda RAST-Recognition by Adaptive Subdivision of Transformation Space ve Optimal Branch ve Bound algoritmaları kullanılmıştır (Beusekom, Shafait ve Breuel, 2013). Bu işlemler sonucunda tüm evrak içerisinde tekrar eden alt desenler bulunabilir. Bu alt desenler evrak üzerinde farklı formatlarda tekrar ederek tam bir desen oluştururlar. Alt desenlerin birbirilerine karşı olan mesafeleri, konumları ve doğrultularına göre desenler tanımlanabilir;

- Seyrek Desen: Alt desenlerin tüm evrak üzerinde geniş aralıklarla tekrar edildiği tür desenlerdir.
- İzole Desen: Desenin tepe ve dip noktalarının birer desen mesafesi boşluk bırakılarak tekrar edildiği desen türü.
- Dağınık Desen: Alt desenlerin birbirileri arasında yatayda ve düşeyde mesafe farklılıklarının bulunduğu desenlerdir. Mesafe farklılıklarından dolayı alt desenler farklı doğrultularda olabilir bu yüzden alt desenin takip edilmesi veya toplu bir desen içerisinde fark edilmesi zor olmaktadır. Aynı zamanda kaotik desen olaraktan adlandırılabilir.
- Düzenli Desen: Bu desen türünde alt desenler birbiri ardına yakın mesafeli konumlanmış ve hizalı olarak tüm evrak içerisinde tekrar eder. Aynı zamanda Grid-Izgara desen olarak adlandırılabilirler.
- Diagonal Desen: Alt desenin yatayda çapraz yönlü sürekli olarak tekrarlandığı desen türüdür.

Genel olarak sarı noktalar A4 boyutlarındaki bir kâğıt üzerinde yaklaşık olarak 150 kez tekrarlanmaktadır. Şekil 4'te izole desen, grid-ızgara desen ve çapraz desen görselleri paylaşılmıştır (Buck, 2018).



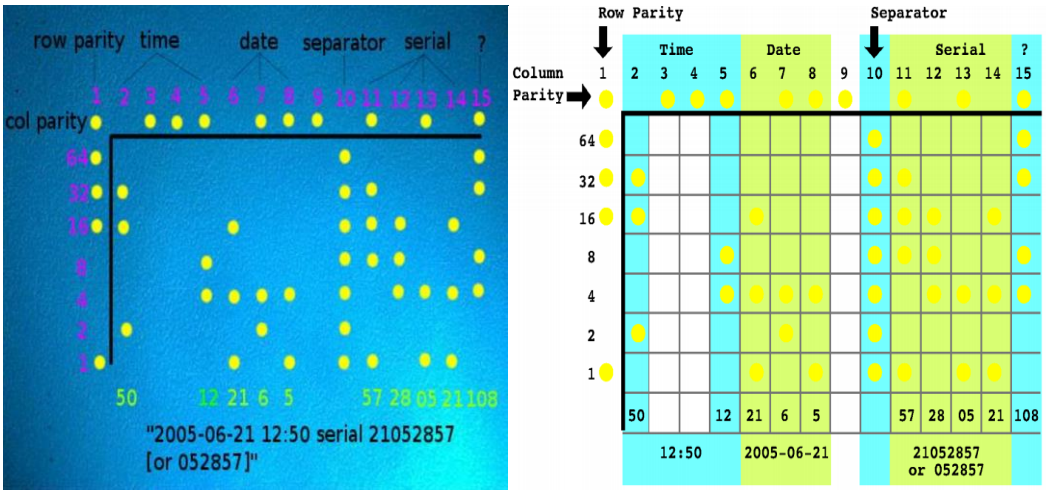
(a) (b) (c)

Şekil 4. (a) ile ifade edilen görsel izole deseni, (b) ile ifade edilen görsel grid–ızgara deseni, (c) ile ifade edilen görsel çapraz deseni göstermektedir.

3.3. Bilgi / Veri Çıkarımı İşlemlerinin Yapılması

Günümüzde tüm herkes tarafından sadece XEROX marka yazıcıların deseni anlamlandırılarak EFF tarafından çözümlenebilmiştir. Çalışmanın bu kısmında EFF'in XEROX marka yazıcılarının desenlerinin anlaşılması anlatılacaktır.

Elimizdeki sarı nokta desenlerinin bulundukları konum ve/veya birbirilerine göre bulundukları konumlara göre bir sayı sisteminde gösterilebilmektedir. Desenin sayı sisteminde gösterilmesi sadece bir yöntemdir, sayı sisteminde anlam kazanıp kazanmayacağı eldeki tek desenin bulunduğu görüntü karesinde kapladığı yere göre belirlenir. Eğer desen eldeki alanın %50'sini kaplıyorsa, yüksek ihtimalle desen tanımlaması yapmak için desenin sayısal gösterimde yazılması gereklidir diyebiliriz. Sayısal gösterim için "binary", "hexadecimal", "octal" veya "decimal" vb. sayı sistemleri ve/veya bunların kombinasyonları tercih edilebilir. Örneğin bir "A" karakteri 0041 (Unicode), 10 (Morse), 1000001 (binary) veya A(hexadecimal) değer olarak tanımlanabilir. Elde edilen sarı noktalar bir ızgara hücresi içerisine alınarak satır ve sütün değerlerine göre çıkarımlarda bulunulabilir. En ideal sayı sistemi tercih edilebilir. Yapılması gereken, sarı noktaların konumlarından faydalanarak saat, tarih, yazıcı seri numarası bilgileri elde etmektir (Khanna ve diğerleri, 2008).



(a) (b)

Şekil 5. (a) ile ifade edilen görselde veri çıkarım örneği 1, (b) ile ifade edilen görselde veri çıkarım örneği 2 gösterilmektedir.

Yukarıda bahsedilen adımların haricinde araştırmacılar makinaların oluşturdukları desenlerin arasındaki uzaklıklardan daha öncesinde ellerinde olan veri tabanı ile karşılaştırmalar yaparak cihaz model tanımaya işlemini yapmışlardır. Şekil 5'de veri çıkarımlarının örnekleri paylaşılmıştır (Buck, 2018).

4. SONUÇ

Steganografi çok eski ancak bir o kadar da popüler bir çalışma alanıdır. Bu alanda yapılan çalışmaların farkındalığı arttırılarak genişletilmesi gerekmektedir. Çalışmamız bu bilinç ile öncelikle yazıcı steganografisi ve sarı nokta analizi hakkında taranan literatürden elde edilen genel bilgiler açıklanmıştır. Sarı nokta analizinin teknik aşaması hakkında bilgiler paylaşılmıştır. Ayrıca sarı nokta analizinin çözüm aşamalarında; ideal görüntüleme sisteminin oluşturulması, desen tanımlama işlemlerinin yapılması ve bu işlemler sonucunda elde edilen çıktıdan bilgi ve veri çıkarımı yapabilmemizi sağlayan işlemlerden bahsedilmiştir.

KAYNAKÇA

Ali, G.N., Mikkilineni, A. K., Chiang, P. J., Allebach, J. P., Chiu, G. T. ve Delp E. J. (2003). Intrinsic and Ectrinsic Signatures for Information Hiding and Secure Printing with Electrophotographic Devices. Conference: NIP19: International Conference on Digital Printing Technologies.

Beusekom, J., Schreyer, M. ve Breuel T. M. (2010). Automatic counterfeit protection system code classification, Proc. SPIE 7541, Media Forensics and Security II, 75410F (27 January 2010); doi: 10.1117/12.840253; https://doi.org/10.1117/12.840253

Beusekom J., Shafait F. ve Breuel T. M. (2013). Automatic Authentication of Color Laser Print-Outs Using Machine Identification Codes. Pattern Analysis and Applications, November 2013, Volume 16, Issue 4, pp 663–678.

Buck, P. (2018). Reverse Engineering the Machine Identification Code. 10.13140/RG.2.2.28980.76169.

Jiang, W., Ho, A. T. S., Treharne, H. ve Shi. Y. Q. (2010) A novel multi-size block benford's law scheme for printer identification. PCM'10 Proceedings of the 11th Pacific Rim conference on Advances in multimedia information processing: Part I Pages 643-652 Shanghai, China September 21 - 24, 2010

Khanna, N., Mikkilineni, A. K., Chiu, G. T. C., Allebach, J. P. ve Delp, E. J. (2008). Survey of Scanner and Printer Forensics at Purdue University. IWCF 2008 LNCS 5158 pp.22-34.

Mikkilineni, A. K., Chiang, P. J., Ali, G. N., Chiu, G. T. C., Allebach, J. P. ve Delp III, E. J. (2005). Printer identification based on graylevel co-occurrence features for security and forensic applications, Proc. SPIE 5681, Security, Steganography, and Watermarking of Multimedia Contents VII, (21 March 2005)

Otsu, N. (1979). A threshold selection method from gray-level histograms. IEEE Trans. Sys., Man., Cyber. 9 (1): 62–66. doi:10.1109/TSMC.1979.4310076.

Sauvola, J. ve Pietikainen, M. (2000). Adaptive document image binarization. Pattern Recognition 33(2), 225–236.

Schreyer, M. (2009). Intelligent printing technique recognition and photocopy detection for Forensic document examination. In Proc. of Informatiktage 2009, volume S-8, pages 39-42,

Schulze, C., Schreyer, M., Stahl, A. ve Breuel, T. M. (2008). Evaluation of graylevel-features for printing technique classification in high throughput document management systems. In Proc. of the 2nd Int. Workshop on Computational Forensics, volume 5158 of Lecture Notes in Computer Science, pages 35-46, Washington, DC, USA, August 2008.

Schulze, C., Schreyer, M., Stahl, A. ve Breuel T. M. (2009). Using DCT features for printing technique and copy detection. In Proc. of the 5thInt. Conf. on Digital Forensics, pages 95-106, Orlando, FL, USA, January 2009

Sönmez, F., Kaynar, O. ve Takaoğlu F. (2018). İdeal Steganografi Senaryosu: Taşıyıcı Resimlerin Kapasitelerinin Hesaplanması, Frekans Tabanlı Steganografide OPA Yöntemi. [Ideal Steganography Scenario: Calculation of Capacities of Carrier Images, OPA Method in Frequency-Based Steganography] ACTA INFOLOGICA, 2018; 2(1): 12-21.

Takaoğlu, F. (2016). DWT ve DCT Steganografide Performans Analizi [Performance Analysis in DWT and DCT Steganography](Yüksek Lisans Tezi).