e-Journal of New Media / Yeni Medya Elektronik Dergi - eJNM
ISSN: 2548-0200, September 2020 Volume 4 Issue 3, p.176-184

YAZICI STEGANOGRAFİSİ VE SARI NOKTA ANALİZİNİN GÜNÜMÜZDE GEÇERLİLİĞİ

Faruk TAKAOĞLU
İstanbul Aydın Üniversitesi, Türkiye
faruktakaoglu@gmail.com
https://orcid.org/0000-0003-0828-2017

Mustafa TAKAOĞLU
İstanbul Aydın Üniversitesi, Türkiye
mustafatakaoglu@aydin.edu.tr
https://orcid.org/0000-0002-1634-2705

ÖZ

Çalışmamızda fiziksel bir steganografi yöntemi olan yazıcı steganografisi ve sarı nokta analizi üzerinde durulmuştur. Günümüzde satılan tüm yazıcılar evrakta gözle görülemeyen bir tahrifat yapmaktadır. Genellikle sarı ve mavi renklerle yapılan bu tahrifat ile evrakta sahtecilik önlenmeye çalışılmaktadır. Ancak gelişen teknoloji sayesinde, örneğin blokzincir teknolojisi gibi yenilikçi uygulama alanlarının yaygınlaşması ve hayatlarımızda daha geniş alanlarda yer bulması durumunda, evraktaki orijinalliğin korunması ve sahteciliğin önüne geçilmesinde alternatif çözümler sağlanabilecek olup, günümüzde kullanılan sarı nokta desenlerinin gerekliliğini sorgulanır bir hale getirmektedir. Ayrıca steganografi bilginin gizlenmesi amacıyla yapılmaktadır. Bu sebeple yazıcı steganografisi uygulanarak tutulan bilgilerin ne olduğu tam olarak bilinmemektedir. Bu sebeple kişisel veri gizliliği konusunda bir güvenlik açığı ihtimali ortaya çıkmaktadır. Yapmış olduğumuz araştırmada yazıcı steganografisi sistemleri, sarı nokta analizi ve gelişen teknoloji karşısında ortaya çıkabilecek sorunlar hakkında bir farkındalık oluşturulması amaçlanmıştır. Bu doğrultuda steganografi hakkında teknik bilgiler paylaşılmış ve sarı nokta analizinin ne olduğu ve nerelerde uygulandığı açıklanmıştır. 1980'li yıllarda geliştirilmiş olan Sahtecilikten Korunma Sistemi'ne dikkat çekilmiş ve kapsamı açıklanmıştır. Evrakta sahtecilik nasıl yapılır açıklanmıştır. Çeşitli örnekler ile yazıcı steganografisinin kişisel veri güvenliğini nasıl tehdit ettiği ifade edilmiştir

Anahtar Kelimeler: *Sarı Nokta Analizi, Sahtecilik Koruma Sistemi, Yazıcı Steganografisi, Veri Güvenliği*

TODAY'S VALIDITY OF PRINTER STEGANOGRAPHY AND YELLOW DOT ANALYSIS

ABSTRACT

In our study, printer steganography and yellow point analysis, which is a physical steganography method, was emphasized. All printers sold today make an invisible falsification on the paperwork. With this falsification, which is usually made with yellow and blue colors, the documents are tried to be prevented. However, thanks to the developing technology, if innovative application areas such as blockchain technology become widespread and are found in wider areas in our lives, alternative solutions can be provided in order to preserve the originality of the documents and prevent fraud, making the question of the necessity of the yellow dot patterns used today. In addition, steganography is performed to hide information. For this reason, it is not known exactly what information is kept by applying printer steganography. For this reason, there is a possibility of a security vulnerability regarding personal data privacy. In our research, it is aimed to raise awareness about printer steganography systems, yellow dot analysis and problems that may arise in the face of developing technology. In this direction, technical information about steganography was shared and it was explained what the yellow

Research Article - Submit Date: 24.04.2020, Acceptance Date: 10.08.2020
DOI NO: 10.17932/IAU.EJNM.25480200.2020/ejnm_v4i3004

spot analysis was and where it was applied. Attention was drawn to the Anti-Fraud System developed in the 1980s and its scope was explained. How to counterfeit documents is explained. It has been stated with various examples how printer steganography threatens personal data security.

Keywords: *Yellow Dot Analysis, Counterfeit Protection System, Printer Steganography, Data Security*

GİRİŞ

Teknolojinin hızla gelişmesi sonucunda insanların günlük hayatında kullandığı ve yaşamlarının sıradan bir parçası haline gelmiş birçok ürün bulunmaktadır. Bu ürünlerin özellikleri ve kabiliyetlerinin farkında olunmadan gün içerisinde defalarca kullanıldığı görülmektedir. Ev ve iş yerlerinde kullanılan yazıcı ve tarayıcı cihazları buna örnek olarak verilebilir. 1980'li yıllarda kullanımı artan, siyah beyaz ve renkli lazer yazıcılar ve optik tarayıcılar sundukları teknik kabiliyet ve avantajlarla insanlar tarafından kabul görmüş ve çokça kullanılmıştır. Ancak her ne kadar bu ürünler hatayı kolaylaştırsa da beraberinde yasal olmayan işlerde kullanıldığı görülmüş ve bunun sonucu olarak yerel ve evrensel tehlikeleri de beraberinde getirmiştir. Yazıcıların ilk olarak sahte para basımında kullanılmasının tespit edilmesinden sonra 1980'li yıllarda lazer yazıcıların içerisine görünmesi zor olan fiziksel filigran veya fiziksel steganografi yöntemi geliştirilerek uygulanmıştır. Geliştirilen bu yönteme Sahtecilikten Koruma Sistemi (SKS) adı verilmiştir. Bu sistem, bastırılan evrak üzerine yardımcı bir görüntüleme sistemi olmadan farkına varılması çok zor kabul edilen sarı noktalar yerleştirilmesini esas almaktadır (Khanna vd 2008: 24).

Böylesine önemli bir konunun toplumun geniş kesimleri tarafından bilinmemesinin sebebi; hem yapılan işlemin hem de bu işlemin yapımında kullanılan bilim alanının stratejik önem arz etmesidir. Sarı noktaların evrak üzerinde ilk bakışta anlaşılması zor şekilde tasarlanarak basılması aslında fiziksel bir steganografi bilimi örneğidir. Steganografi antik Yunancada gizli anlamına gelen "steganos" ve yazma anlamına gelen "graphein" kelimelerinin birleşiminden meydana gelmektedir (Takaoğlu, 2016: 35). Kelime anlamı olarak gizli yazma anlamına gelen bu bilim çok eski dönemlerden bu yana gizli mesajlaşma işlemlerinde veya var olan kıymetli bir unsurun saklanarak iletilmesi veya korunmasında kullanılmaktadır. Daha sonra bilimin ve teknik kabiliyetlerin gelişmesi ile bu bilimin alt dalları ve uygulama alanları genişlemiştir. Dilimizde filigran olarak kullanılan bu bilim, steganografinin bir alt dalı veya uygulama alanıdır (Sönmez vd 2019: 16). Filigran normal hayatımızda banknot para birimlerinde görmekte olduğumuz bir uygulamadır. Dijitalleşme ve internet çağı ile birlikte çoklu medya unsurlarının ticari değer ve/veya adli sorumluluk içermesi ile birlikte aitliklerinin ispatlanması için filigran kullanılmaya başlanmıştır. Evrakların kimin tarafından yazıldığı ve aitliklerinin ispatlanması için ise steganografinin bu alt dalı filigranlar yani sarı noktalar kullanılmaktadır (Beusekom vd 2013: 665).

Massachusetts Teknoloji Enstitüsü Medya Laboratuvarı Bilgisayar Kültür Grubu'nun yapmış olduğu bir çalışmada (URL-1) evrak üzerine yerleştirilen ve yukarıda bahsettiğimiz bu sarı noktaların Amerikan resmi makamlarınca ve yazıcı üreten firmalar arasında alınan bir karar doğrultusunda yapıldığı öne sürülmüştür. Evrak üzerine insan gözünün farkına varamayacağı şekilde yerleştirilen bu sarı noktalar daha sonrasında yetkili kişilerce cihazın markası, modeli, seri numarası, evrakın yazıldığı tarih ve zamanı hakkında net bilgiler verir hale getirilmiştir. İlk olarak Elektronik Sınırlar Vakfı (ESV) tarafından XEROX marka bir yazıcının SKS sistemi çözülerek yazıcılarda SKS varlığı ispatlanarak kamuoyuna duyurulmuş ve toplumun ilgisi çekilmeye çalışılmıştır. 2007 yılında Kaos İletişim Kampı (KİK) organizasyonunda ilk defa katılımcılarla SKS kodlarının kullanımı üzerine bir söyleşi gerçekleştirilmiştir (Beusekom vd 2010: 3).

Yapılan bu çalışma ile amacımız ülkemizde farkındalığı düşük bir konu olan steganografinin ve kullanım alanlarından biri olan sarı nokta analizinin farkındalığını arttırmaktır. Yazıcı steganografisi gibi fiziksel steganografinin günlük hayatımızın içinde yer aldığı aktif kullanım alanlarına dikkat çekilerek, bu yöntemin farkındalığının oluştuğu yerlerdeki toplumsal tepkilere ve önerilere yer verilmiştir. Bu doğrultuda çalışmamızın devam eden bölümlerinde sarı noktaların teknik özellikleri, evrak üzerine yerleştirilme aşamaları hakkında alanyazın taramasında elde edilen teknik bilgilere ve

Research Article - Submit Date: 24.04.2020, Acceptance Date: 10.08.2020
DOI NO: 10.17932/IAU.EJNM.25480200.2020/ejnm_v4i3004

kullanımlarına yer verilmiş ve farkındalığın sağlanması amaçlanmıştır. Ayrıca sarı noktaların kullanımının gelişen teknoloji ışığında gerekliliği, konu hakkındaki görüşlerimizi yansıtacak şekilde aktarılmış ve öneriler paylaşılmıştır. Yapılan bu çalışmanın, konu hakkında bilgilenmek isteyen araştırmacı ve öğrencilere yardımcı olabileceğini düşünmekteyiz.

ALANYAZIN İNCELEMESİ

Sarı noktalar 1980'li yıllarda renkli lazer yazıcılar kullanılarak sahte para basımının engellenmesi amacı ile tasarlanmıştır. Amerikan Sorgulanan Belge İnceleyicileri Derneği (ASBİD)'ne göre üzerinde tahrifat yapılmış evrak ve sahte banknot para vakalarında artış gözlenmektedir. Evrak tahrifatı ve sahtecilik vakalarının temel araçları olarak renkli lazer yazıcı ve tarayıcı cihazları görülmektedir. Bu cihazların içerisindeki sistemle evrak üzerine yerleştirilen SKS kodları takip edilerek sahtecilik olayları çözülmeye çalışılmaktadır. SKS kodları bize evrakın yazıldığı tarih ve saati vererek adli vakalarda ispat olarak kullanılmakta, aynı zamanda cihaz model ve seri no vererek sahteciliğin tespiti ve ispatı olarak kullanılmaktadır. SKS kodlarındaki bozulmalar incelenerek evrak üzerinde yapılan tahrifatlar takip ve tespit edilmektedir (Gazi vd 2003: 513).

SKS kodları cihaz ve evrak hakkında bize bilgi veren bir sistemdir. Bu sistem evrak içerisine fiziksel filigran veya fiziksel steganografi örneği olarak sarı noktalardan oluşan bir desen olarak işlenmektedir. Bu noktalar çıplak insan gözü ile görülmesinin zor ve hatta imkânsız olması için sarı renklerde ve ufak boyutlarda üretilmektedir. Her biri 0.006 inç olan bu sarı noktalar 600 dpi çözünürlükte yaklaşık 4 piksellik bir boyuttadırlar (Beusekom vd 2010: 5). Renklerinin sarı olarak tercih edilmesinin sebebi beyaz arka plan renk üzerinde sarı rengin yansıtılırlığının düşük olmasıdır. Bazı yazıcı modelleri sarı renk yerine mavi renkte noktalar da tercih etmektedirler. Tespit edilmiş sarı nokta içeren yazıcıların listesi ESV'nin internet sayfasından elde edilebilir (URL-3). Sarı noktaların evrak üzerinde nasıl göründüğü hakkında bilgi sahibi olunması amacıyla Şekil1'de sarı nokta işlenmiş bir evrak görüntüsü paylaşılmıştır.

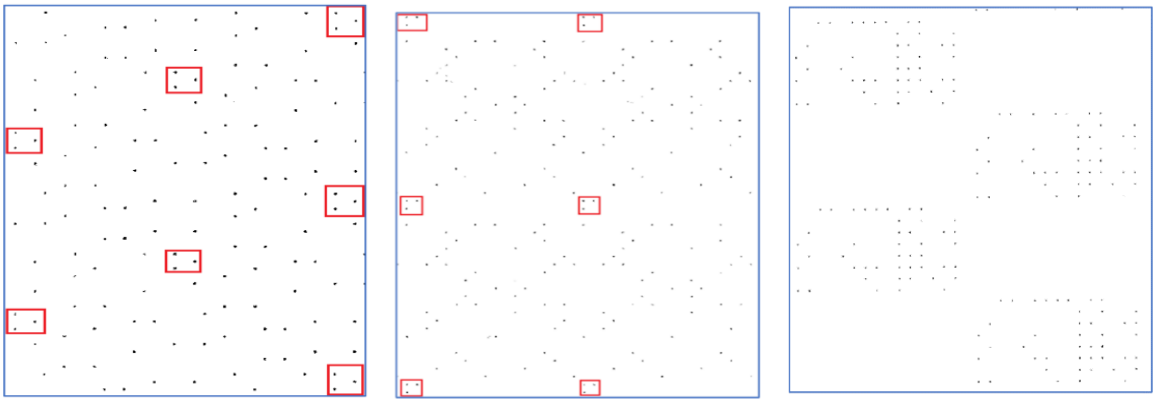
Resim 1: Sarı Noktaların Evrak Üzerinde Yakın Çekim Görünümü (URL-2)

Sarı noktalar evrak üzerinde gözükmeleri zor olduklarından öncelikle mikroskop veya yakınlaştırma kapasitesine sahip kameralar ile bakılması gereklidir. Eğer böyle bir imkân söz konusu değil ise evrak üzerine morötesi ışık kaynağı yansıtmak gereklidir. Sarı noktalar morötesi ışıkta en yüksek yansıtılırlık değerine ulaşacaklarından görülmeleri kolaylaşmaktadır (Peter, 2018: 16). Sarı noktaların görünürlükleri sağlandıktan sonra yapılması gereken sarı noktaların oluşturdukları desenlerin tespit edilmesidir.

Evrak üzerine işlenen sarı noktalar bir desen oluşturarak kâğıt üzerine yerleştirilmektedir. Genellikle ufak bir alt desen evrak içerisinde sürekli tekrar ederek büyük ve tam deseni oluşturmaktadır. A4 boyutlarındaki bir evrakta 150 kez alt desen tekrar etmektedir. Var olan bu tüm desen kendi içerisinde tekrar eden alt desenlerin evrak üzerindeki dizilişine göre farklı adlandırılabilir. Eğer alt desen bir desen boyu kadar aralıklarla yatayda ve düşeyde tekrar ediliyorsa izole desen denir. Alt desenler birbirilerinin peşi sıra ve ızgara şeklinde diziliyor ise buna ızgara desen denir. Alt desenler yatayda ve düşeyde belirli aralıklarla çaprazda hizalı şekilde sıralanmışlar ise buna çapraz desen denir. Son olarak alt desenler

Research Article - Submit Date: 24.04.2020, Acceptance Date: 10.08.2020
DOI NO: 10.17932/IAU.EJNM.25480200.2020/ejnm_v4i3004

birbirine oldukça yakın ve belirli bir hizası olmayan kaotik şekilde dizilmişler ise buna dağınık veya kaotik desen denilir (Kotipalli ve Suthaharan, 2014: 77). Şekil 2'de izole, ızgara ve çapraz desen görüntüleri paylaşılmıştır.



Resim 2: İzole Desen, Izgara Desen, Çapraz Desen

Desenler çeşitli algoritmalar kullanılarak tespit edilebileceği gibi kullanıcılar tarafından inceleme sonucunda da tespit edilebilir. Yazıcı marka ve modellerine göre desenler belirli karakteristik özellikler içermektedir. Örneğin HP marka yazıcıların çıkarmış oldukları desenlerde "L" veya ters "L" deseni tekrar eden alt desende ilk başta bulunmaktadır (Peter, 2018: 22).

SARI NOKTA ANALİZİ KULLANIM ÖRNEKLERİ

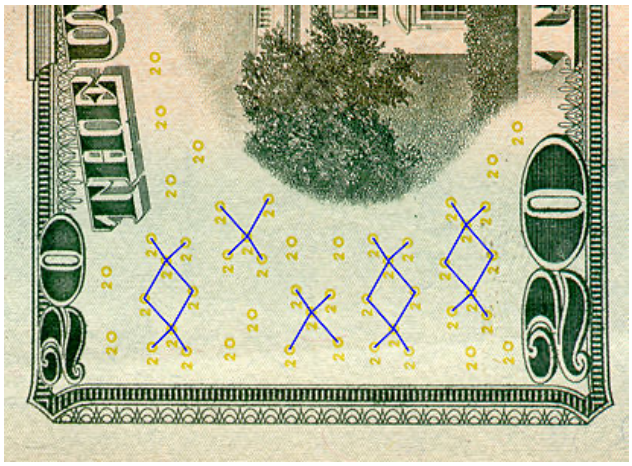
Çalışmamızın bu bölümünde sarı noktaların toplumun faydasına kullanılan yöntemlerinden bahsedilecektir. SKS kodları, yani sarı noktalar, daha öncesinde bahsedildiği gibi evrakta tahrifat yani sahtecilik ve sahte parayı engellemek amacıyla üretilmişlerdir. SKS kodlarından yazıcı modeli, seri numarası, tarih ve saat bilgileri elde edilerek yazıcıdan çıktı alan kişilerin tespit edilebilmesi farklı bir kullanım alanıdır. ESV yayınlarında ABD haber alma teşkilatları örneği temel alınarak 1100 'den fazla yazıcılardan çıktı olarak alınan dokümanların izlendiği ve takip edildiği bildirilmiştir (URL-5).

Bir evrak baskı yapıldıktan sonra farklı veya aynı yazıcı kullanılarak üzerinden geçilerek değişiklik yapılabilir. Bu durumun farkına varabilmek için SKS kodlarına yani sarı noktaların evrak üzerindeki dağılımlarına bakmak ilk düşünülebilecek çözüm olabilir. Her yazıcının evrak üzerine yerleştirmiş olduğu sarı nokta deseni kendine özel bir desen tasarımı olduğu için bir evrak ikinci kez farklı bir yazıcıdan yazdırıldığında bu sarı noktaların birbirine geçmesi ve karışması söz konusudur. Evraktaki sarı noktalar incelendiğinde birbiri içerisine geçmiş, çakışmış sarı noktalar görüldüğü takdirde evrakta sahtecilik yapıldığına karar verilebilir (Aravind vd 2005: 436). Aynı zamanda birbiri ile dip dibe bulunan veya aynı sarı nokta deseni noktalarının yan yana tekrar edildiğinin görülmesi durumunda da incelenen davanın durumuna bağlı olarak bu evrak ikinci kez aynı yazıcıdan geçirilerek üzerinde işlem yapılmıştır kanısına varılabilir.

Her zaman sarı noktaların desenlerindeki değişimleri incelemek gerekli değildir, bazı durumlarda üzerinde sarı nokta olmaması gereken bir doküman da sarı nokta desenlerinin varlığına rastlanıldığında evrakın taklit veya kopya evrak olduğunun kanısına varılabilir. Bazı durumlarda sarı nokta desenleri içerisindeki farklılıkları inceleyerekten evrakın kopyalanmış olup olmadığını anlanabilir. Dilimizde eşlik veya eşitlik bitleri olarak geçen bu bitlerdeki değişim kontrol edilerek evrakın tarayıcıdan kopyalanarak basıldığını anlayabiliriz. Bu durum bir desen içerisinde yer alan bir kolondaki nokta grubunun değişimini incelemeye dayanır. Marka ve modele göre bu kolon içerisindeki noktaların varlığı veya diziliş şekli değişebilmektedir. İncelenen desenlerde sadece bir adet boş nokta yeri bulunan veya sadece bir noktanın dolu olduğu desen kolonunun kopyalama işleminden sonra yazıcıdan yazdırıldığı takdirde, sarı nokta analizi yapıldığında, bu kolon bölgelerinde tam tersi şekilde değişiklik gözlemlenmiştir.

Research Article - Submit Date: 24.04.2020, Acceptance Date: 10.08.2020
DOI NO: 10.17932/IAU.EJNM.25480200.2020/ejnm_v4i3004

Temel uygulama alanı olan banknot paralarda gözle görülebilir ve birbirileri ile mesafe açısından ilişkili sarı nokta deseni bulunmaktadır. EURion takımyıldızı adı verilen bu desen birçok ülkenin banknot para birimlerinde kullanılmaktadır. Amerikan doları üzerindeki sarı noktalar bunlara örnek olarak verilebilir (URL-4). Bu sarı noktalar haricinde banknot üzerinde bir sarı nokta deseni görüldüğü zaman banknotta sahtecilik düşünülebilir. Şekil 3'te kâğıt para üzerinde uygulanmış EURion desenli sarı nokta örneği paylaşılmıştır.



Resim 3: EURion Desenli Sarı Noktalar

Banknot para birimleri üzerinde çokça kullanılan SKS kodları ve sarı nokta analizi günümüzde birçok alanda kullanılan ve pek fazla eleştirilmeyen sistemlerdir. Ancak ilerleyen dönemlerde kripto para birimlerinin, daha doğrusu blokzincir teknolojilerinin birçok alanda yaygınlaşabileceği göz önüne alınarak düşünüldüğünde, banknot para birimlerinin kullanımının şekil değiştireceği ve banknotların tedavülden kalkabileceğini söylemek afaki değildir (Takaoğlu vd. 2019: 289). Çünkü ekonominin blokzincirine çekilmesi çalışmaları meyvesini vermeye başladığında ve ayrıca insanlığın şahit olduğu Covid19 gibi küresel salgınlar sebebiyle nakit paranın virüs taşıma riskinin insanlığı süratle kredi kartı kullanımına sevk etmeye başlaması sonucunda, sarı nokta desenlerinin para birimlerinde kullanılmasının ilerleyen dönemlerde sonlanacağına şahit olabiliriz.

Günümüzde e-imza uygulamalarının arttığı dikkate alınırsa kâğıt evrakların imzalanarak kurumlar veya kişiler arasında paylaşılarak gönderilmesi süratle şekil değiştirebilir ve dolayısıyla tamamen tarihe karışabilir. Bir dijital belgenin herhangi bir yazıcıdan çıktısının alınarak bir başka makam veya kuruma iletilinceye kadar birçok fiziki hasar ve tahrifattan geçmesi mümkündür. Tüm bu sorunların ortadan kaldırılabilmesi için güvenli ağlar ile veya internet üzerinden e-imza kullanarak bir başka kurum veya kişiye iletilebilir. Eğer güvenli bir teknolojik altyapı oluşturulabilirse ve toplum bireyleri arasında da evrak ve belge gönderimi kullanımı sağlanabilirse kâğıt evrakların sosyal hayatta da kullanımı azalabilir. Böylelikle evraklar ve bunlardan kaynaklanan adli vaka ve davaların azalacağı ve kamu kurumlarındaki iş yükünün azalacağı düşünülebilir.

BULGULAR VE TARTIŞMA

Kurum, kuruluş ve şahısların ürettikleri evrakların analiz ve takip edilmesi hususunda, bu alanda çalışan uzmanların farklı görüşleri bulunmaktadır. Ulusal güvenlik ve anti terörizm önlemleri açısından bakıldığında; verilerin üzerine herhangi bir yöntem ile tehlike arz eden bilgilerin gizlenmesi yahut sahte banknot ya da çek, senet, tapu senedi gibi değerli kâğıtların üzerinde yapılabilecek işlemler sonucunda devletlere ve insanlara zarar verebilecek her türlü eylemin engellenmesi için takip ve önlem mekanizmalarının geliştirilmesi ve uygulanması kabul edilebilir görülmektedir.

Ancak bahsettiğimiz sistemler marifetiyle yapılan analiz ve takip işlemlerinin terör ve illegal örgütlerin takip edilmesinden ziyade Greenpeace ve United for Peace and Justice gibi şiddet ve kamu zararına

Research Article - Submit Date: 24.04.2020, Acceptance Date: 10.08.2020
DOI NO: 10.17932/IAU.EJNM.25480200.2020/ejnm_v4i3004

eylemlerde bulunmayan organizasyonların takibinde kullanılmasına şahit olunması da bu alanda çalışan birçok kişi tarafından tepki ile karşılanmıştır (URL5).

İnsanların son zamanlarda SKS kodları ve sarı nokta analizine ilgi göstermesinin bir diğer sebebi ise The Intercept isimli Amerikan yayın kuruluşunda Amerikan Ulusal Güvenlik Teşkilatı'na ait bilgilerin yayınlanmasıdır. Bu yayından sonra Amerikan Ulusal Güvenlik Ajansından veri akışını sağlayan kişinin işine son verilmiştir. Veri aktarımını sağlayan kişinin yayın kurumuna ulaştırdığı evraklardaki sarı nokta analizinden hangi yazıcıdan ve hangi zamanda çıktısının alındığı bilgisine ulaşılarak çıktıyı alan kişi tespit edilmiş ve işine son verilmiştir. Bu olaydan sonra insanlar kendi evlerinde kullandıkları yazıcılardan çıkan evraklar ile takip edilmelerini özel hayatın gizliliğine müdahale olarak gördüklerini paylaşmışlardır. Dile getirilen bu eleştiri çok doğru olmakla birlikte özel hayatın gizliliğine yapılmış bir ihlaldir. Hukuken bu durumun incelenmesi gerekmektedir.

Sarı nokta desenlerinin çözümlerinin bilgisi sadece üreticiler ve Amerikan devletinin ilgili kurumları arasında paylaşılmaktadır. Toplum ESV çalışmaları sayesinde sadece XEROX marka yazıcıların sarı nokta desenin çözümlerini bilmektedir. Bunların haricinde Japon İş Makinaları Üreticileri Birliği (JİMÜB) tarafından üretilen bir yazılım sayesinde sarı nokta desenlerinin çözülümü yapılabilmektedir. Ancak bu kurum yazılımını sadece belirli devletlere satmaktadır (Peter, 2018: 25). Burada temel olarak itiraz edilen sorun, bu bilginin sadece belirli kesimlerce kontrol edilebilmesi ve topluma paylaşılmamasıdır.

Günümüzde kullanılan yazıcılar çok daha karmaşık özellikleri bünyesinde bulundurmaktadır: Tarama, faks, kablosuz bağlantı ve internet bağlantısı gibi özellikleri günümüzde artık sıradan bir yazıcıda olan temel özelliklerdir. The Intercept örneğini göz önünde bulundurduğumuzda, yazdırılan dokümanlara yazıcı steganografisiyle gizlenen bilgilerin neleri kapsadığı hakkında tam bir bilgi bulunmamaktadır. Yukarıda bahsedilen JİMÜB kurumunun sahip olduğu teknolojiyi sınırlı ülkelerle paylaşması da üzerinde durulması gereken ve saklanan bilgilerin düşünülenden fazla olabileceğini gösteren bir diğer göstergedir.

Paylaşılan bilgiler ışığında şu tespiti yapmak gerekir: Kişisel ve kurumsal verilerin korunması büyük bir risk altındadır. Bu riskin sebebi birçoğumuz tarafından önemsenmeyen basit bir yazıcı çıktısının içerisine steganografi vasıtasıyla gizlenmiş ve içeriğini bilmediğimiz bilgilerdir. Ayrıca birçok yazıcıda bulunan internet bağlantısı özelliği ile yaşanabilecek izinsiz veri transferleri de göz ardı edilmemeli ve bu ihtimalin üzerinde durulmalıdır.

Anlaşılacağı üzere sarı nokta analizi konusu, üzerinde disiplinler arası çalışmaların yapılması gerektiği bir çalışma alanıdır. Hukuken gizlenen bilgilerin neleri kapsadığının yahut sarı nokta desenlerinin paylaşılmamasının bir sorun teşkil edip etmediği incelenmelidir. Yazıcılarında steganografi kullanan üreticilerin müşterilerine karşı sorumluluğu bulunmaktadır. Yazıcılardan elde edilecek verilerin kapsamını sınırlayıcı yasal kurallar belirlenmeli ve ürünler denetlenmelidir. Günümüzde satılan hiçbir yazıcının ürün bilgisinde bahsedilen durumu ifade eden bir ibare bulunmamaktadır. Hâlbuki paylaşmış olduğumuz bilgiler ışığında, yazıcılarda kullanılan steganografi ve sarı nokta teknikleri sebebiyle veri güvenliğinin garanti edilemediği anlaşılmaktadır.

Son olarak hızla gelişen teknolojik yenilikler neticesinde yazıcı steganografisinin gerekliliğinin zayıflaması karşımıza şu sorunu çıkaracaktır: Sahteciliğin engellenmesi amacıyla kâğıt üzerinde kasıtlı olarak yapılan tahrifata gerek kalmayacaktır. Bu durumda ilerleyen süreçte gözle görülemeyecek boyutlarda dahi olsa kusurlu bir çıktı veren yazıcılar, ayıplı bir ürün olarak değerlendirilebilir. Ayrıca blokzinciri teknolojisinin internet teknolojisi gibi kullanımının yaygınlaşması ve uygulanabildiği alanların genişlemesiyle para transferlerinin dijital ortama çekilmesi ve değerli tüm evrakların blokzincir sisteminde değiştirilemez bir şekilde kayıt altına alınması durumunda fiziksel yazıcı steganografisi ve sarı nokta analizinin gereksiz ve etik olmayan bir yazıcı özelliği haline geleceği unutulmamalıdır. Bu durumda çok net bir şekilde ilerleyen süreçte üretilecek yazıcılarda yazıcı steganografisinin bulunmaması gerektiğini ifade etmemiz gerekir.

SONUÇ

Research Article - Submit Date: 24.04.2020, Acceptance Date: 10.08.2020
DOI NO: 10.17932/IAU.EJNM.25480200.2020/ejnm_v4i3004

Ülkemizde steganografinin fiziksel kullanım alanlarından biri olan sarı nokta analizleri hakkında çokça veri ve çalışma bulunmamaktadır. Günümüzde steganografi üzerine yapılan araştırmaların neredeyse tamamı dijital steganografi uygulamaları ile ilgilidir. Ancak günlük hayatımızda yer alan fiziksel steganografinin nadir ve güncel uygulama alanlarından biri de sarı nokta analizi olduğu unutulmamalıdır. Çalışmamızda bu konu hakkında gerekli bilgilendirmeler yapılmış ve farkındalık oluşması hedeflenmiştir.

Sarı nokta analizinin ortaya atılmasının arkasındaki sebep 1980'li yıllar düşünüldüğünde çok mantıklı olabilir. Ancak günümüzde teknolojinin geldiği nokta düşünüldüğünde ve steganografinin bir veri saklama sanatı olduğu gerçeğini unutmadan hali hazırda kullanılan sistemlerin sadece evrakta sahtecilik ve sahte para üretilmesine karşı olduğunu savunmak ve elde edilen diğer bilgilerin neler olduğunu sorgulamamak doğru değildir. Bilgi güçtür ve bu güce ulaşmak ucuz değildir. Günümüzde Japon İş Makinaları Üreticileri Birliği tarafından üretilen yazılımın neden sadece belirli ülkelere satıldığının üzerinde düşünülmesi gerekmektedir. Ayrıca yazıcılar sayesinde sahte para üretimi günümüzde yok denecek kadar az yapılan bir sahtecilik yöntemidir. Durum böyleyken ve yazıcıların günümüzde neredeyse her resmi yahut özel kurumda kullanıldığı düşünüldüğünde, böyle bir sistemin varlığından herkesin haberdar olması gerekmektedir.

İnternet bağlantısı olan her yazıcı, Sahtecilikten Korunma Sistemi marifetiyle gerçekleştirilen fiziksel steganografi sonucunda elde ettiği bilgileri ikinci hatta üçüncü şahıslarla paylaşabilir. En büyük sorun steganografi kullanılarak elde edilen bilgilerin ne olduğunun bilinmemesidir. JİMÜB'in geliştirdiği yazılımın tüm yazıcı markalarında işe yaradığı düşünüldüğünde ve bu teknolojinin sadece belirli ülkelerle paylaşıldığı dikkate alındığında, elde edilen verilerin ne denli kapsamlı olduğu akıllara gelmektedir. Sadece şahsi kullanım olarak düşünülmeden, devlet kurum ve kuruluşlarında kullanılan bu tür yazıcıların sızdırabileceği stratejik bilgiler, çok ciddi milli savunma sorunlarına sebebiyet verebilir. Bu sebeple sadece devlet kurumlarında kullanılmak üzere, SKS kurallarından bağımsız, aksine milli menfaatlerin korunması amacıyla yerli SKS kuralları belirlenerek üretilmiş bir yazıcı geliştirilmesi gerekmektedir.

Çalışmamızın önceki bölümlerinde tanıtılan Intercept örneği üzerinde düşünmek gerekmektedir. Amerikan çıkarlarına ters bir bilgi paylaşımı yapan kişinin kullandığı yazıcı sayesinde kimliğine ulaşılması, insanlar üzerinde farklı etkiler yaratabilir. İnsanların bu konu hakkındaki tepkilerinin çok yönlü olarak değerlendirilmesi gerekmektedir. KİK organizasyonunun dikkat çektiği ve kişisel verilerin güvenliğinin sorgulandığı forumlar düşünüldüğünde haklı bir noktaya temas ettikleri görülmektedir. Ancak 11 Eylül ve benzeri terör saldırıları ve sonuçlarında karşılaşılan olumsuzluklar düşünüldüğünde, merkezi otoritelerin sorumlulukları gereği önlem almaya yönelik çalışmalarına şiddetle karşı çıkmak uygun olmayabilir. Bu sebeple kontrol mekanizmalarının çok doğru belirlenmesi ve çok doğru kurumlarca yapılmasının sağlanması gerekmektedir.

Evrak sahteciliği ve sahte para basımı gibi çalışmaların işe yarayabilmesi için merkezi otoritelerce kabul edilmesi ve işleme alınması gerekir. Ancak günümüzde geliştirilen birçok teknoloji bu sorunların çözümünde etkili olarak kullanılmaktadır. Blokzincir teknolojisi çok uygun bir örnektir. Bilindiği üzere günümüzde kullanılan birçok veri tabanı merkezi yapıda olup, saldırılara açık bir durumdadır. Geliştirilen bulut mimarileri karşılaşılan sorunların çözümünde olumlu sonuçlar sunuyor olsa da kesin bir çözüm değildir. Bu sebeple blokzincir temelli dağıtık veri yapıları çözüm olarak ön plana çıkmaktadır. Çünkü blokzincir sistemlerinde veri işleme yönü tek taraflıdır. Sadece okuma ve yazma işlemleri yapılabilir. Kaydedilmiş bir verinin anlaşılmadan silinmesi mümkün değildir. Tabii ki blokzincir teknolojisi yeni bir teknoloji olmakla birlikte her sorunun çözümünde nihai bir yol olarak gösterilemez. Ancak ilerleyen süreçte blokzincir teknolojilerinin hali hazırdaki sistemlere uygulanmasının gerçekleşmesi durumunda, evraklarda yapılması planlanan sahtecilik imkânsız bir hal alacaktır. Ayrıca Bitcoin ve Ethereum gibi kripto paralarının yaratıcı gücü olan blokzincir teknolojisinin dünya ülkelerince kendi para birimlerinde uygulanması ve kendi milli kripto paralarını geliştirmeleri durumunda, kağıt para kullanımının ve doğal olarak da sahte para basımının bir manası kalmayacaktır. Blokzincir teknolojisi ve benzeri yeni gelişmelerin hayatlarımıza hızlı bir şekilde dâhil olması durumunda, SKS sistemlerinin kullanımına devam edilmesinin mantıklı bir açıklaması zorlaşacaktır.

Research Article - Submit Date: 24.04.2020, Acceptance Date: 10.08.2020
DOI NO: 10.17932/IAU.EJNM.25480200.2020/ejnm_v4i3004

Teknolojinin gelişmesi ve dijitalleşmenin hızla yayılması ilerleyen dönemde evrak süreçlerinde geleneksel alışkanlıkların şekil değiştirebileceğini gözler önüne sermektedir. Covid19 sürecinde de görüldüğü üzere, eposta vasıtasıyla ve elektronik imza uygulamalarıyla günümüzde kullanılan ve açıkladığımız güvenlik risklerinin yanı sıra çevreci de olmayan kâğıt kullanımının, kurumların sırtına yüklediği masraflar da düşünüldüğünde, yazıcılara duyulan ihtiyacın her geçen gün azalma eğiliminde olduğu sonucuna varılabilir. Ancak tüm önemli evrak ve kıymetli kâğıtların dijitalleştiği düşünüldüğü durumda dahi karşımıza şu sorun çıkmaktadır: Yazıcılar da kullanılan SKS sistemlerinin gerekliliği tartışma konusudur ve yapmış olduğumuz açıklamalardan da anlaşılacağı üzere bir güvenlik sorunu olarak değerlendirilebilir. Bu sebeple toplumsal farkındalığın artması, stratejik önem arz eden kurumlarda yazıcı özellikleri sınırlı olan cihazların tercih edilmesi ve kişisel kullanımda da bazı önlemler alınması gerekmektedir. Yazıcının kullanılmadığı durumlarda kapalı tutulması ve internet bağlantısının yapılmaması bir çözüm yöntemi olabilir. Ayrıca yazıcıların kullanımının ilerleyen süreçte devam edeceği göz önüne alınarak, yerli üretim ve milli SKS sistemleriyle geliştirilmiş yazıcıların üretilmesine öncelik verilmesinin faydalı olacağı görüşündeyiz. Son olarak JİMÜB kurumunun geliştirdiği gibi SKS sistemlerinin sakladığı bilgileri açığa çıkartacak yazılımların geliştirilmesi gerekmektedir. Bu doğrultuda yapılacak çalışmaların stratejik önemi göz önüne alınarak desteklenmesi gerekmektedir.

KAYNAKÇA

Aravind, K. M., Pei-Ju, C., Gazi, N. A., George, C., Jan, P. A. & Edward, D. (2005). *"Printer identification based on graylevel co-occurrence features for security and forensic applications"*, Proceedings of SPIE - The International Society for Optical Engineering, 5681, 430-440.

Beusekom, J., Schreyer, M. & Breuel, T. (2010). *"Automatic Counterfeit Protection System Code Classification"*, Media Forensics and Security (s. 1-8). San Jose: dblp.

Beusekom, J., Shafait, F. & Thomas M. B. (2013). *"Automatic authentication of color laser print-outs using machine identification codes",* Pattern Anal. Appl., 16, 663-678.

Gazi, N. A., Aravind, K. M., Pei-Ju, C., Jan, P. A., George, C. & Edward, D. (2003). *"Intrinsic and Extrinsic Signatures for Information Hiding and Secure Printing with Electrophotographic Devices",* International Conference on Digital Printing Technologies, 5, 511-515.

Khanna, N., Mikkilineni, A. K., Chiu, G. T. C., Allebach, J. P. & Delp, E. J. (2008). *"Survey of Scanner and Printer Forensics at Purdue University",* In: Srihari S.N., Franke K. (eds) Computational Forensics. Lecture Notes in Computer Science, 5158, 22-34.

Kotipalli, K. & Suthaharan, S. (2014). *"Modeling of class imbalance using an empirical approach with spambase dataset and random forest classification"*, In Proceedings of the 3rd annual conference on Research in information technology (pp.75-80). New York: ACM.

Peter, B. (2018). *"Printer Steganography: Reverse Engineering the Machine Identification Code"*, Saxion University of Applied Science, pp. 1-30.

Sönmez, F., Takaoğlu, F. & Kaynar, O. (2018). *"İdeal Steganografi Senaryosu: Taşıyıcı Resimlerin Kapasitelerinin Hesaplanması, Frekans Tabanlı Steganografide OPA Yöntemi",* ACTA INFOLOGICA, 2(1), 12-21.

Takaoğlu, F. (2016). *"DWT ve DCT Steganografide Performans Analizi"*, Yüksek Lisans Tezi, İstanbul Aydın Üniversitesi, Fen Bilimleri Enstitüsü, İstanbul.

Takaoğlu, M., Özer, Ç. & Parlak, E. (2019). *"Blockchain technology and Possible Implementation Areas in Turkey"*, International Journal of Eastern Anatolia Science Engineering and Design, 1 (2), 260-295.

Research Article - Submit Date: 24.04.2020, Acceptance Date: 10.08.2020
DOI NO: 10.17932/IAU.EJNM.25480200.2020/ejnm_v4i3004

İNTERNET KAYNAKLARI

URL-1: http://seeingyellow.com Erişim Tarihi: 22.05.2019

URL-2: https://compcult.media.mit.edu/2007/07/11/seeing-yellow/ Erişim Tarihi: 22.02.2020

URL-3: https://www.eff.org/pages/list-printers-which-do-or-do-not-display-tracking-dots Erişim Tarihi: 23.02.2020

URL-4: https://en.wikipedia.org/wiki/EURion_constellation Erişim Tarihi: 14.03.2020

URL-5: https://www.eff.org/issues/printers Erişim Tarihi: 20.04.2020

Research Article - Submit Date: 24.04.2020, Acceptance Date: 10.08.2020
DOI NO: 10.17932/IAU.EJNM.25480200.2020/ejnm_v4i3004