# Görsel Zeka (VISINT) Panoraması 2025: OSINT Görüntü Analizinde En İyi 10 Teknik ve Trend

## Yönetici Özeti

Bu rapor, 2025 yılı ve sonrası için Açık Kaynak İstihbaratı (OSINT) alanında fotoğraf ve video analizine yönelik en etkili on teknik ve trendi derinlemesine incelemektedir. Bulgular, Yapay Zeka (YZ) odaklı analiz, gelişmiş jeolokasyon (coğrafi konumlandırma), özgünlük krizi ve operasyonel ölçeklenebilirlik olmak üzere dört ana tematik kategori altında toplanmıştır. Yapay Zeka, hem yeni yeteneklerin birincil sağlayıcısı hem de dezenformasyon gibi en önemli zorlukların kaynağı olarak bu dönüşümün merkezinde yer almaktadır. Analizler, görsel zekanın (VISINT) artık OSINT'in niş bir alt disiplini olmaktan çıkıp, özel araçlar, ileri düzey eğitim ve yeni bir analitik zihniyet gerektiren temel bir istihbarat alanına dönüştüğünü göstermektedir. Bu değişim, istihbarat toplulukları, güvenlik kuruluşları ve gazeteciler için hem benzeri görülmemiş fırsatlar hem de ciddi zorluklar sunmaktadır.

### 2025 VISINT Trendlerine Stratejik Bakış Tablosu

| Trend/Teknik | Temel Teknoloji | Birincil İşlev | Temel 2025 Uygulama Alanları | İlişkili Risk/Zorluk | Ana Referanslar |
| --- | --- | --- | --- | --- | --- |
| **1. Anlamsal ve Bağlamsal Arama** | CLIP+FAISS | Kavramsal Arama | Etiketlenmemiş veri setlerinde tehdit avcılığı, tematik istihbarat toplama | Anahtar kelime sınırlamalarını aşma | SANS OSINT Zirvesi, Ultralytics |
| **2. YZ Destekli Bağlamsal Zeka** | Multimodal Modeller | Bütünsel Anlam Çıkarma | Olay tespiti (protesto, çatışma), sosyo-politik analiz | Algoritmik önyargı, jeopolitik yanlış yorumlama | Roboflow, Google AI |
| **3. Jeolokasyon için 3B Sahne Rekonstrüksiyonu** | NeRF/Gaussian Splatting | Fotogerçekçi Sahne Rekonstrüksiyonu | Hassas bölgelerin sanal keşfi, suç mahalli yeniden oluşturma | Yüksek hesaplama maliyeti ve uzmanlık | Bellingcat, ArXiv |
| **4. Çok Modlu Jeo-uzamsal Üçgenleme** | Veri Füzyon Platformları | Kanıt Birleştirme | Çoklu zayıf sinyallerden konum doğrulama, ağ analizi | Tek bir "altın" ipucuna bağımlılığın azalması | ShadowDragon, Neotas |
| **5. Yeni Nesil Deepfake Tespiti** | GAN/Difüzyon Modelleri | Sahtecilik Tespiti | Hukuki süreçlerde kanıt doğrulama, dezenformasyonla mücadele | "Yalancının Temettüsü" (Liar's Dividend) | SANS Enstitüsü, Facia.ai |
| **6. İleri Düzey Metadata Adli Bilişimi** | Karşı-Adli Bilişim Analizi | Metadata Gizleme Analizi | Gelişmiş aktörlerin tespiti, niyet analizi | Adli bilişim araçlarına yönelik karşı saldırılar | ResearchGate, CameraForensics |
| **7. Otonom YZ Ajanları ile Veri Triage'ı** | Bilgisayarlı Görü Pijamaları | Büyük Ölçekli Tarama | Büyük veri akışlarından ilgili görsellerin filtrelenmesi | Veri zehirlenmesi, ölçekli manipülasyon | SANS Enstitüsü, Webasha |
| **8. Entegre OSINT Platformları ile Birleşik Analiz** | Bağlantı Analizi Grafikleri | İlişki Haritalama | Karmaşık suç ağlarının ortaya çıkarılması, kurumsal risk yönetimi | Yüksek maliyet, yetenek eşitsizliği | Maltego, ShadowDragon |
| **9. Gelişmiş Tersine Görüntü ve Yüz Tanıma** | Evrişimli Sinir Ağları (CNN) | Kişi ve Nesne Tanımlama | Şüpheli takibi, pratik anonimliğin sonu | Gizlilik ihlalleri, etik kaygılar | Lenso.ai, PimEyes |
| **10. Gerçek Zamanlı ve Tahmine Dayalı VISINT** | Edge AI / Akış Analizi | Olay Tahmini | Kriz yönetimi, kamu güvenliği, proaktif müdahale | "Suç öncesi" analiz, etik ikilemler | RTInsights, Group-IB |

## Bölüm I: Görüntü Zekasında Yapay Zeka Odaklı Paradigma Değişimi

Bu bölüm, VISINT'teki en temel değişimi ele almaktadır: pikselleri analiz etmekten anlamı kavramaya geçiş. Yapay Zeka artık sadece bir otomasyon aracı değil, analistlerin görsel verilerle nasıl etkileşim kurabileceğini yeniden tanımlayan bilişsel bir ortak haline gelmiştir.

### 1. Anlamsal ve Bağlamsal Arama: Anahtar Kelimelerle Değil, Kavramlarla Sorgulama

Geleneksel tersine görüntü arama—öncelikli olarak tam veya benzer kopyaları bulmaya odaklanan bir yöntem—yerini anlamsal aramaya bırakmaktadır.1 Bu yeni paradigma, bir görüntüdeki

*anlamı*, *bağlamı* ve *ilişkileri* anlamak için yapay zeka modellerini kullanır. Bu sayede analistler, etiketlenmemiş devasa görüntü veri setlerini doğal dil sorguları veya kavramsal olarak benzer içerik bulmak için tek bir referans görüntü kullanarak arayabilirler.3

Bu teknolojinin merkezinde OpenAI'nin CLIP (Contrastive Language-Image Pre-training) gibi modelleri ile Meta'nın FAISS (Facebook AI Similarity Search) gibi verimli arama kütüphanelerinin birleşimi yatmaktadır.3 CLIP, hem görüntüleri hem de metinleri ortak bir "gömme uzayına" (embedding space) haritalamak için bir görüntü kodlayıcı ve bir metin kodlayıcı kullanır. Bu uzayda, "günbatımında kumlu bir plaj" görüntüsü ile "günbatımında kumlu bir plaj" metni, sayısal olarak birbirine yakın vektörlerle temsil edilir.3 FAISS ise bu görüntü gömme vektörlerinden oluşan son derece verimli ve aranabilir bir dizin oluşturarak, bir metin sorgusunun gömme vektörüne en yakın komşuların milyonlarca görüntü arasından bile gerçek zamanlı olarak getirilmesini sağlar.3 Bu modellerin "sıfır atış" (zero-shot) yeteneği kritik bir öneme sahiptir. Devasa ve çeşitli veri setleri üzerinde önceden eğitildikleri için, herhangi bir özel ince ayar gerektirmeden yeni, daha önce görülmemiş ve etiketlenmemiş görüntü koleksiyonları üzerinde arama yapabilirler. Bu, yeni durumlarla karşılaşan OSINT analistleri için büyük bir avantajdır.3

Bu teknolojik ilerleme, OSINT alanında iki önemli etki yaratmaktadır. İlk olarak, geleneksel tersine görüntü aramanın birincil işlevi değişmektedir. TinEye gibi araçlar belirli bir görüntünün kökenini izlemek için hala kullanışlı olsa da 1, anlamsal arama, farklı ve etiketlenmemiş kaynaklar arasında tematik keşif ve istihbarat toplama gibi yeni bir yetenek sunmaktadır. Geleneksel araçlar, "Bu görüntü başka nerede göründü?" sorusunu yanıtlarken, anlamsal arama, "Bu görüntü veya metinle aynı fikri temsil eden başka hangi görüntüler var?" sorusuna cevap verir.3 Bu, bir analistin tek bir kanıtı doğrulamaktan kapsamlı bir istihbarat resmi oluşturmaya geçebileceği anlamına gelir. Örneğin, bir analist, tanımlanamayan bir askeri teçhizatın görüntüsünü kullanarak, modeller, boya şemaları veya ortamlar farklı olsa bile benzer

*sınıftaki* teçhizatı içeren diğer görüntüleri arayabilir.

İkinci olarak, "görsel istem mühendisliği" (visual prompt engineering) olarak adlandırılabilecek yeni bir beceri ortaya çıkmaktadır. Tıpkı metin tabanlı Büyük Dil Modelleri (LLM'ler) için istem mühendisliğinin kritik hale gelmesi gibi, görsel arama için de benzer bir beceri gerekecektir. Bir analistin sorguyu nasıl ifade ettiği ("çölde bir askeri konvoy" ile "kurak bir bölgede zırhlı araçlardan oluşan bir sütun") farklı sonuçlar doğuracaktır. Bellingcat'in sıfır atış sınıflandırma rehberi, en iyi sonuçlar için belirgin, bağlamsal ve net etiketler kullanmanın önemini vurgulamaktadır.5 Bu, anlamsal bir aramanın etkinliğinin, analistin kesin, açıklayıcı ve bağlamsal olarak farkında olan metin sorguları oluşturma yeteneğine büyük ölçüde bağlı olacağını göstermektedir.

### 2. YZ Destekli Bağlamsal Zeka (VISINT): Nesne Tanımanın Ötesinde

Bu trend, bir görüntüdeki nesneleri basitçe tanımlamanın ("bu bir araba") ötesine geçerek, bütünsel bağlamı anlamaya yönelir ("bu, bir protestoda hasar görmüş sivil bir araba, sivil huzursuzluğa işaret ediyor"). Bu, görsel verilerden ilişkileri, faaliyetleri, duygusal tonu ve sosyo-politik önemi analiz edip çıkarabilen yapay zeka sistemlerini içerir.6 Bu, temel görüntü analizinden gerçek Görsel Zekaya (VISINT) evrimin merkezinde yer alır.

Bu yetenek, çeşitli bilgisayarlı görü görevlerini entegre eden gelişmiş, çok modlu yapay zeka modelleri aracılığıyla elde edilir.6 Bu modeller, kapsamlı bir resim oluşturmak için nesne tespiti, sahne anlama, eylem tanıma ve görsel ilişki analizini birleştirir.6 Daha da önemlisi, bu sistemler görsel verileri, eşlik eden sosyal medya gönderisindeki metin, zaman damgaları ve jeolokasyon verileri gibi diğer veri akışlarıyla birleştirerek daha zengin ve doğru bir bağlamsal anlayış üretir.10 Örneğin, Google'ın Gemini Pro Vision ve Imagen gibi modelleri, altyazılar oluşturabilir, görsel içerikle ilgili soruları yanıtlayabilir ve bir görüntü içindeki yapılandırılmış içeriği anlayabilir.9 Bu yapay zeka, etkileşimin veya soruşturmanın bir "hafızasını" tutarak, önceki bulgulara ve kullanıcı girdilerine göre analizini uyarlayabilir ve durum bilgisi olmayan bir araçtan dinamik bir analitik ortağa dönüşebilir.7

Bu gelişmeler, analistin rolünü temelden değiştirmektedir. VISINT araçları, istihbarat döngüsünün ilk aşamalarını (toplama ve işleme) ve hatta analiz aşamasının bazı kısımlarını otomatikleştirmeye başlamaktadır. Görüntüleri sadece nesneleri etiketlemek için değil, aynı zamanda öğrenilmiş bağlamsal kalıplara dayanarak potansiyel ilgi çekici olayları (örneğin, toplanmalar, çatışmalar, silahların varlığı) işaretlemek için ön işleme tabi tutabilirler. Bir insan analistin bir çatışma bölgesinden bir fotoğrafa bakarken gerçekleştirdiği zihinsel adımlar—nesneleri tanımlama, durumlarını analiz etme, mekansal ilişkilerini yorumlama ve olayı çıkarma—artık modern yapay zeka tarafından büyük ölçüde otomatikleştirilebilir.6 Bu nedenle, insan analistin rolü, bu zaman alıcı ilk analizi yapmaktan, YZ'nin çıkarımlarını doğrulamaya ve daha üst düzey stratejik düşünmeye kayacaktır: "YZ tarafından tanımlanan bu olay, hedeflerimiz için ne anlama geliyor?"

Ancak bu yetenek, önemli bir risk taşır: jeopolitik analizde algoritmik önyargı. Yapay zeka, politik olarak hassas görüntüleri yorumlamak için kullanıldıkça, eğitim verilerindeki doğal önyargılar tehlikeli yanlış yorumlamalara yol açabilir. Yapay zeka modellerinin, belirli grupları belirli kavramlarla ilişkilendiren (örneğin, "Müslüman" ile "terörist") önyargılar geliştirdiği gösterilmiştir.13 Sağcı siyasi gruplar, belirli kültürel ve nostaljik anlatıları pekiştiren görüntüler üretmek için şimdiden yapay zekadan yararlanmaktadır.15 Bu temel önyargılara sahip bir OSINT aracı, politik olarak yüklü bir görüntüyü analiz etmek için kullanıldığında, tarafsız değil, belirli bir politik veya kültürel bakış açısını yansıtan bir açıklama üretebilir.16 Bu analize güvenen bir istihbarat kurumu için bu, hatalı, algoritmik olarak oluşturulmuş bir yoruma dayanarak gerilimleri tırmandıran kritik bir jeopolitik durumun yanlış okunmasına yol açabilir.

## Bölüm II: Jeolokasyonun Yeni Ufukları

Bu bölüm, bir fotoğrafın nerede çekildiğini bulma sanatını ve bilimini dönüştüren, 2B harita eşleştirmesinden etkileşimli 3B sahne keşfine geçen devrim niteliğindeki teknolojileri kapsamaktadır.

### 3. Jeolokasyon için 3B Sahne Rekonstrüksiyonu: NeRF, Gaussian Splatting ve Fotogrametri

Bu alan, geleneksel 2B jeolokasyondan (bir fotoğraftaki simge yapıları uydu veya sokak seviyesi görüntülerle eşleştirme) bir dizi 2B görüntüden bir sahnenin tam 3B modellerini oluşturmaya doğru bir geçişi temsil etmektedir. Bu, sanal keşfe ve hassas bakış açısı eşleştirmesine olanak tanıyarak jeolokasyonun güvenilirliğini ve doğruluğunu önemli ölçüde artırır.18

Bu yetenek, birkaç temel teknoloji tarafından desteklenmektedir. Fotogrametri, fotoğraflardan 3B modeller oluşturmanın yerleşik tekniğidir. Bellingcat, sosyal medya fotoğraflarından perspektifi ve manzarayı eşleştirerek Burj Khalifa'daki bir dairenin tam katını belirlemek için Blender'da bir 3B model oluşturarak kullanımını göstermiştir.20 Daha yeni bir yapay zeka tabanlı teknik olan Neural Radiance Fields (NeRF), bir dizi 2B görüntüden ve kamera pozlarından bir sahnenin sürekli bir 3B temsilini öğrenmek için bir sinir ağı kullanır. NeRF'ler, herhangi bir açıdan fotogerçekçi "yeni görünümler" oluşturmada mükemmeldir ve bir analistin, bir fotoğrafın çekildiği tam noktayı bulmak için yeniden oluşturulmuş sahnede sanal olarak uçmasına olanak tanır.19 Daha da yeni bir teknik olan Gaussian Splatting, bir sahneyi 3B Gauss'ların bir koleksiyonu olarak temsil eder. NeRF'e benzer fotogerçekçi render kalitesi elde eder, ancak önemli ölçüde daha hızlı eğitim ve gerçek zamanlı render hızları ile hızlı OSINT analizi için daha pratik hale gelir.18 CaLiSa-NeRF gibi yeni araştırmalar, son derece ayrıntılı, çok katmanlı kentsel 3B modeller oluşturmak için yer seviyesi görüntüleri, LiDAR nokta bulutlarını ve uydu görüntülerini birleştirmektedir.23

Bu teknolojiler, jeolokasyonun doğasını temelden değiştirmektedir. Analistler artık sadece 2B bir fotoğrafı 2B bir haritayla karşılaştırmıyorlar. Artık 3B çevreyi yeniden oluşturabiliyor ve ardından kameranın konumunu bu ortam içinde simüle edebiliyorlar. Geleneksel jeolokasyon, bir fotoğraftaki referans noktalarını bulmayı ve bunları Google Earth gibi bir haritada eşleştirmeyi içerir; bu, 2B'den 2B'ye veya 2B'den 2.5B'ye bir karşılaştırma sürecidir.12 NeRF ve Gaussian Splatting gibi teknikler ise açık kaynaklı görüntülerden (örneğin sosyal medya, emlak listeleri) tam, gezilebilir bir 3B model oluşturur.20 Analistin görevi daha sonra, hedef görüntüde görülen perspektifi, görüş alanını ve örtüşmeleri mükemmel bir şekilde kopyalamak için bu simüle edilmiş 3B ortamına sanal bir kamera yerleştirmek haline gelir. Bu, konumu basit bir simge yapı eşleştirmesinden çok daha yüksek bir kesinlik derecesiyle doğrular.

Bu araçların birçoğunun açık kaynaklı olması (Blender, NeRF/Splatting uygulamaları), bir zamanlar yalnızca devlet düzeyindeki istihbarat teşkilatlarının uydu ve hava görüntüleme yetenekleriyle sahip olduğu gelişmiş saha keşfini, devlet dışı aktörler, gazeteciler ve hatta kötü niyetli gruplar için erişilebilir kılmaktadır. Bir konumun ayrıntılı 3B modellerini oluşturmak tarihsel olarak karmaşık ve pahalı bir süreçti. Şimdi ise, bir konumun (örneğin halka açık bir meydan, hassas bir binanın dışı) yeterli sayıda halka açık 2B görüntüsü sosyal medyadan toplanabilir ve yüksek kaliteli bir 3B model oluşturmak için kullanılabilir.18 Bu, bir aktivist grubun lojistiği planlamak için bir protesto rotasını modelleyebileceği, bir gazetecinin tanık ifadelerini doğrulamak için bir suç mahallini yeniden oluşturabileceği 24 ve bir terörist grubun saldırı planlaması için potansiyel bir hedefin sanal keşfini yapabileceği anlamına gelir.18

### 4. Çok Modlu Jeo-uzamsal Üçgenleme: Görselleri Farklı Veri Kümeleriyle Birleştirme

Bu trend, bir görüntüyü tek başına analiz etmenin ötesine geçerek, yüksek güvenilirlikli jeolokasyon elde etmek için onu birden fazla, farklı açık kaynaklı veri akışıyla gerçek zamanlı olarak birleştirmeyi içerir. Bir görüntü görsel bir çapa sağlar, ancak konumu, ipuçlarının ağ verileri, kamu kayıtları, ticari veriler ve diğer jeo-uzamsal bilgilerle çapraz referanslanmasıyla doğrulanır.25

Bu süreç, tek bir teknolojiden çok, entegre OSINT platformları tarafından sağlanan bir metodolojiye dayanır. Süreç, klasik görüntü analiziyle başlar: simge yapılar, işletme adları, sokak tabelaları, benzersiz mimari, araç türleri vb. tanımlanır.12 Bu görsel ipuçları daha sonra diğer veritabanlarında sorgu olarak kullanılır. Örneğin, bir işletme adı OpenCorporates gibi şirket sicillerinde kontrol edilir 28; kısmi bir plaka, araç tescil verileriyle çapraz referanslanır; veya metadatada yakalanan Wi-Fi BSSID'leri, WiGLE gibi veritabanlarında aranarak kesin bir konum belirlenebilir.25 Babel X, Maltego ve OSINT Industries gibi jeo-uzamsal platformlar, bu farklı veri türlerini tek bir harita üzerinde birleştirerek analistlerin kanıtların birleştiği noktayı görmelerini sağlar.26

Bu yaklaşım, OSINT'in doğasındaki bir değişimi yansıtmaktadır. Düşmanlar OSINT tekniklerinin (örneğin, tabelaları bulanıklaştırma, metadatayı temizleme) daha fazla farkına vardıkça, bir görüntüde tek ve kesin bir ipucu bulma olasılığı azalmaktadır. Jeolokasyonun geleceği, farklı veri modalitelerinden gelen çok sayıda zayıf sinyalin bir araya getirilmesine dayanmaktadır. Erken jeolokasyon başarıları genellikle tek, net bir bilgi parçasına dayanıyordu.31 Ancak düşmanlar artık bu ipuçlarını ortadan kaldırmak için aktif olarak karşı-adli bilişim teknikleri kullanıyor.33 Bu nedenle, gelecekteki başarı, bir "mozaik" yaklaşımına bağlı olacaktır. Bir analist, tek bir nokta yerine bir konum için bir "olasılık konisi" oluşturmak amacıyla belirsiz bir mimari stili (görsel veri), gölgelerden çıkarılan günün saati (görsel veri), kısmen gizlenmiş tabelalardaki baskın dil (görsel veri) ve o bölgedeki sosyal medya duyarlılığını (metinsel veri) birleştirebilir.

Ayrıca, geleneksel OSINT kamu verilerine odaklanırken, ticari veri setleriyle (örneğin, iş analitiği, emlak verileri) birleşme, iyi kaynaklara sahip kuruluşlar için önemli bir ayırt edici özellik haline gelmektedir. Kamu veri kaynakları OSINT'in temelini oluşturur.28 Ancak, ticari veri sağlayıcıları genellikle daha ayrıntılı ve yapılandırılmış veri setlerine sahiptir.28 Bir jeolokasyon görevinde, bir analist bir fotoğrafta yapım aşamasında olan bir bina tespit edebilir. Kamu kayıtları yavaş güncellenirken, ticari emlak ve inşaat endüstrisi veritabanları o projenin tam konumuna, planlarına ve zaman çizelgesine sahip olabilir. Kamu görsel verilerinin bu özel ticari verilerle birleştirilmesi, önemli bir analitik avantaj sağlar.

## Bölüm III: Bütünlük ve Özgünlük Silahlanma Yarışı

Bu bölüm, VISINT için varoluşsal bir tehdidi ele almaktadır: gördüğünüz şeye güvenememe durumu. Giderek daha karmaşık hale gelen sahtecilikler ve bunlarla mücadele etmek için geliştirilen ileri adli bilişim tekniklerinin ikili eğilimlerini inceleyecektir.

### 5. Yeni Nesil Deepfake ve YZ Üretimi İçerik Tespiti

Bu bölüm, sentetik veya manipüle edilmiş medyayı (deepfake'ler, "ucuz sahtecilikler" ve diğer YZ tarafından oluşturulmuş görüntüler) tespit etmek için gelişmiş tekniklerin kritik ihtiyacına ve geliştirilmesine odaklanmaktadır. Üretken yapay zeka araçları yaygınlaştıkça, otantik görsel kanıtları fabrikasyon olanlardan ayırt etme yeteneği, tüm OSINT çalışmalarının bütünlüğü için hayati önem taşımaktadır.37

Tespit süreci, çok katmanlı bir adli bilişim yaklaşımını içerir. YZ liderliğindeki adli analiz, üretken modellerin (GAN'lar, Difüzyon modelleri) geride bıraktığı ince artefaktları ve tutarsızlıkları tespit etmek için eğitilmiş özel YZ modellerini kullanmayı içerir. Bu, aydınlatma, gölgeler, yansımalar, dokulardaki (özellikle cilt ve saçta) doğal olmayan desenleri ve arka planlardaki veya çevresel figürlerdeki garip anatomik hataları içerebilir.37 Köken ve kaynak takibi, sadece görüntünün piksellerini analiz etmek yerine, görüntünün kökenine odaklanır. Bu, orijinal, manipüle edilmemiş sürümü bulmak için tersine görüntü aramayı 37 ve otantik medya için doğrulanabilir bir gözetim zinciri oluşturmak amacıyla blokzincir tabanlı dijital imzaların veya filigranların potansiyel kullanımını içerir.37 Trend, otomatik deepfake tespit araçlarını doğrudan OSINT iş akışlarına ve platformlarına entegre etmeye, şüpheli medya hakkında gerçek zamanlı uyarılar sağlamaya yöneliktir.37

Bu gelişmeler, "Yalancının Temettüsü" (Liar's Dividend) olarak bilinen kavramı operasyonel bir gerçekliğe dönüştürmektedir. Deepfake'lerin varlığının bile gerçek kanıtları itibarsızlaştırmak için kullanılabileceğini tanımlayan bu terim, düşmanlar tarafından standart bir taktik haline gelecektir. Suçlular zaten gerçek bir görüntünün sahte olduğunu iddia edebilir ve doğru araçlar olmadan bunu çürütmek zordur.42 Son derece gerçekçi deepfake'lerin yayılması, ne kadar otantik olursa olsun, herhangi bir tehlikeli video veya görüntünün, deepfake olduğu iddia edilerek makul bir şekilde inkar edilebileceği anlamına gelir.37 Bu durum, analistin rolünü tersine çevirir. Kanıt bulma saldırısından, kendi kanıtlarını doğrulama savunmasına geçer. Bu, daha yüksek bir ispat yükü gerektirir.

Ayrıca, tek bir "evrensel" deepfake dedektörünün etkinliği azalacaktır. Tespitin geleceği, sahteyi oluşturmak için kullanılan YZ modelinin belirli "parmak izini" veya karakteristik artefaktlarını tanımlamayı içerecektir. Farklı üretken modeller farklı mimarilere ve eğitim süreçlerine sahiptir 39, bu da ürettikleri görüntülerde modele özgü ince artefaktlara neden olur. Bir SANS sunumu, özellikle

*belirli* üretken YZ modelleri tarafından yapılan hataları tespit etmeye odaklanmaktadır.40 Bu nedenle, gelişmiş adli bilişim araçları sadece ikili bir "gerçek/sahte" yanıtı vermekle kalmayacak, aynı zamanda "bu görüntünün bir Midjourney v7 modeli tarafından üretilme olasılığı %85" gibi olasılıksal bir değerlendirme sunabilecektir. Bu, sadece görüntüyü çürütmekle kalmaz, aynı zamanda onu yaratan düşmanın araçları ve yetenekleri hakkında istihbarat da sağlayabilir.

### 6. İleri Düzey Metadata Adli Bilişimi ve Karşı-Adli Bilişim Farkındalığı

Bu trend, görüntü dosyalarına gömülü gizli verilerdeki artan "silahlanma yarışını" kapsamaktadır. Bir yanda, metadatadan (EXIF, IPTC vb.) kritik istihbarat çıkarmak için gelişmiş araçların kullanımı, diğer yanda ise analistlerin bu verileri silmek, değiştirmek veya tahrif etmek için kullanılan karşı-adli bilişim tekniklerini anlama ve tespit etme ihtiyacının artması yer almaktadır.33

ExifTool gibi araçlar kullanılarak, analistler GPS koordinatları, tarih/saat damgaları, kamera markası/modeli ve hatta düzenleme için kullanılan yazılım gibi zengin bilgileri çıkarabilirler.25 Karşı-adli bilişim (anti-forensics) ise adli analizi kasıtlı olarak engelleme eylemidir. Teknikler arasında metadata silme, belirli kameralar veya yazılımlar tarafından bırakılan istatistiksel izleri (PRNU parmak izleri gibi) ortadan kaldırmayı amaçlayan iz bastırma ve en aldatıcı olanı, bir düşmanın izleri sadece kaldırmakla kalmayıp aktif olarak taklit ettiği özgünlük sentezi bulunur.33

Bu dinamik, iki önemli sonuç doğurur. İlk olarak, metadatanın yokluğu artık bir istihbarat göstergesi haline gelmiştir. Geçmişte, eksik metadata genellikle tarafsız bir veri noktasıydı. 2025'te, yüksek riskli bir soruşturmada, tüm metadatanın ve dijital parmak izlerinin *kasıtlı* ve *kapsamlı* bir şekilde kaldırılması, saklayacak bir şeyi olan sofistike bir düşmanı düşündüren bir kırmızı bayrak olacaktır. Sıradan kullanıcıların görüntülerindeki metadata, sosyal medya platformları tarafından otomatik olarak kaldırılır.45 Ancak, karşı-adli bilişimle uğraşan sofistike bir aktör, sadece EXIF verilerini silmekle kalmaz, aynı zamanda PRNU gürültüsü gibi daha ince artefaktları da kaldırmaya çalışır.33 Sadece EXIF değil, aynı zamanda dijital bir görüntünün beklenen istatistiksel gürültü desenlerinden de yoksun olan "çok temiz" bir görüntüyü inceleyen bir analist, görüntünün kasıtlı olarak temizlendiği sonucuna varabilir. Bu, analizi "hangi veriler mevcut?" sorusundan "hangi veriler

*eksik* ve neden?" sorusuna kaydırır.

İkinci olarak, adli bilişim araçlarının "güven modeli" çökmektedir. Analistler artık tek bir adli bilişim aracının çıktısına körü körüne güvenemezler. Bulguları çapraz doğrulamak için birden fazla araç kullanan katmanlı bir yaklaşım zorunlu hale gelecektir, çünkü düşmanlar sahteciliklerini en popüler adli bilişim algoritmalarını aldatmak için özel olarak tasarlayacaklardır. Karşı-adli bilişim araştırmaları, açıkça "görüntü adli bilişimine saldırmaya" ve "adli analizlerin belirli bir sonucunu tetiklemeye" odaklanmaktadır.33 JPEG sıkıştırması, yeniden örnekleme ve diğer yaygın adli bilişim belirteçleri için dedektörleri aldatmak üzere özel olarak tasarlanmış teknikler geliştirilmektedir.33 Bu nedenle, 2025 için sağlam bir metodoloji, herhangi bir çelişkinin ortaya çıkıp çıkmadığını görmek için bir görüntüyü birden fazla, farklı türde analiz aracından (örneğin, biri sıkıştırma artefaktlarını, diğeri gürültü desenlerini, üçüncüsü renk filtresi dizisi tutarlılığını kontrol eden) geçirmeyi gerektirecektir.

## Bölüm IV: Ölçekte Otomasyon ve Entegrasyon

Bu bölüm, istihbarat ekiplerinin ezici görsel veri seliyle başa çıkmalarını sağlayan operasyonel eğilimleri incelemekte ve yapay zeka destekli otomasyon ile entegre platformların nasıl temel güç çarpanları haline geldiğine odaklanmaktadır.

### 7. Büyük Ölçekli Görsel Veri Triage'ı için Otonom YZ Ajanları

Her gün petabaytlarca yeni görsel veriyle karşı karşıya kalındığında, insan analizi artık ölçeklenebilir değildir. Bu trend, görüntü ve videoların ilk, büyük ölçekli triage'ını (önceliklendirme ve ayıklama) gerçekleştirmek için otonom veya yarı otonom YZ ajanlarının konuşlandırılmasını içerir. Bu ajanlar, devasa veri akışlarından ilgili içeriği tarayabilir, özetleyebilir, kategorize edebilir ve işaretleyebilir, böylece daha derinlemesine araştırma için insan analistlere yönetilebilir bir alt küme sunabilirler.46

Bu ajanlar, SANS Enstitüsü web seminerinde açıklandığı gibi, yüzlerce gigabaytlık görüntü ve video arasında özetleme ve arama yapabilen, böylece veri aşırı yüklenmesi sorununu çözen YZ destekli özetleme ve arama yetenekleri kullanır.47 Bu sistemler, temel unsurları tanımlamak için bir nesne algılama modeli, sahneyi tanımlamak için bir altyazı modeli ve son olarak görüntüyü kategorize etmek için bir sınıflandırma modeli gibi bir bilgisayarlı görü modelleri ardışık düzeni kullanır.6 SpiderFoot ve Sintelix Harvester gibi araçlar, yüzlerce kaynaktan görsel ve ilgili verilerin toplanmasını otomatikleştirerek, manuel müdahale olmaksızın analiz ardışık düzenine besler.36

Bu gelişmeler, "Hizmet Olarak İstihbarat" (Intelligence-as-a-Service) modelinin ortaya çıkmasına yol açmaktadır. Kuruluşlar, kendi büyük ölçekli triage sistemlerini kurmak yerine, küresel açık kaynaklı görüntü akışını işlemek için zaten YZ ajanlarını kullanmış olan özel, önceden analiz edilmiş görsel istihbarat akışları sağlayan hizmetlere giderek daha fazla güvenecektir. Büyük ölçekli bir YZ triage sistemi kurmak ve sürdürmek, önemli teknik uzmanlık ve hesaplama kaynakları gerektirir.47 Babel X ve Dark Owl gibi ticari şirketler, belirli veri kaynaklarının YZ destekli analizini zaten bir hizmet olarak sunmaktadır.26 Bu hizmetlerin görsel verilere genişlemesi, örneğin "Güney Çin Denizi'ndeki denizcilik faaliyetleriyle ilgili tüm coğrafi konumlandırılmış görüntülerin, gemi türü ve anormallikler için önceden analiz edilmiş" bir abonelik tabanlı akış sunması doğal bir evrimdir.

Ancak bu otomasyon, yeni bir güvenlik açığı olan "veri zehirlenmesi" riskini de beraberinde getirir. Kuruluşlar triage için otomatik YZ ajanlarına bağımlı hale geldikçe, düşmanlar tek bir analisti aldatmaktan ziyade, bu ajanları eğitmek için kullanılan verileri "zehirlemeye" odaklanacak ve böylece tüm kuruluşların istihbarat akışlarını ölçekli olarak manipüle edecektir. YZ modelleri, eğitim setine kötü niyetli verilerin eklenmesiyle belirli şekillerde yanlış davranmaya neden olan "veri zehirlenmesine" karşı savunmasızdır.51 Bir düşman, binlerce görüntüyü ustaca manipüle edebilir—örneğin, kendi askeri donanımının tüm görüntülerine belirli, neredeyse görünmez bir artefakt ekleyerek—ve bunları OSINT araçlarının veri topladığı halka açık sitelere yükleyebilir. Bu zehirli verilerle eğitilmiş otomatik YZ ajanı, bu donanımı görmezden gelmeyi veya zararsız bir şey olarak yanlış sınıflandırmayı öğrenebilir. Bu, o modeli kullanan herhangi bir kuruluşun otomatik triage sisteminde etkili bir şekilde bir kör nokta yaratır.

### 8. Entegre OSINT Platformları ile Birleşik Analiz

Bu trend, tek amaçlı araçların dağınık bir koleksiyonunu kullanmaktan uzaklaşıp, çok modlu verileri tek bir ortamda alabilen, analiz edebilen ve görselleştirebilen kapsamlı, entegre platformlara geçişi işaret etmektedir. Maltego, ShadowDragon ve Palantir Gotham gibi platformlar, analistlerin görsel kanıtlar, ağ verileri, kamu kayıtları ve sosyal medya istihbaratı arasında sorunsuzca geçiş yapmalarını ve karmaşık ilişkileri görsel olarak haritalamalarını sağlar.30

Bu platformlar, sosyal medyadan karanlık ağ forumlarına ve ticari veri sağlayıcılarına kadar yüzlerce farklı veri kaynağına bağlanmak için API'ler ve "Dönüşümler" (Transforms) kullanır.28 Temel özellikleri, tüm veri noktalarını (kişiler, resimler, IP adresleri) bir grafikte düğümler ve ilişkilerini bağlantılar olarak temsil etme yeteneğidir. Bu görsel temsil, bir elektronik tabloda veya metin belgesinde görünmez olacak gizli bağlantıları, faaliyet kümelerini ve kritik yolları tespit etmeyi kolaylaştırır.30 Bir analist, tek bir platform içinde bir görüntüyle başlayabilir, bir yüzü çıkarabilir, yüz tanıma araması yapabilir, bir sosyal medya profili bulabilir, kullanıcının ortaklarını ve bilinen konumlarını çıkarabilir ve hepsini aynı grafikte haritalayabilir.52

OSINT'in bu "platformlaşması", iki katmanlı bir yetenek sistemi yaratmaktadır. Bu güçlü ve pahalı entegre platformları karşılayabilen ve düzgün bir şekilde uygulayabilen kuruluşlar, ücretsiz, açık kaynaklı araçlar koleksiyonuna dayananlara göre önemli bir analitik avantaja sahip olacaktır. Maltego ve Palantir gibi platformlar açıkça kurumsal, hükümet ve kolluk kuvvetleri müşterilerini hedeflemektedir ve ucuz değildir.26 Bu platformlar, 120'den fazla veri sağlayıcısının sorunsuz entegrasyonu gibi, bireysel ücretsiz araçlarla çoğaltılması son derece zor olan yetenekler sunar.44

Bu entegrasyon aynı zamanda yeni bir analist becerisi ihtiyacını da beraberinde getirir: "Veri Füzyonisti". Bu platformlardaki en etkili analistler, tek bir alanda (örneğin, görüntü analizi) uzman olanlar değil, bir cevabı bulmak için hangi soruları soracağını ve hangi farklı veri setlerini birleştireceğini bilen genelciler olacaktır. Bu platformların gücü, farklı veri türlerini bağlama yeteneklerinde yatmaktadır.30 Karmaşık bir vakayı çözmek için bir analistin, bir görüntünün EXIF verilerini (görsel adli bilişim) arka planda görülen bir web sitesinin WHOIS kaydına (ağ adli bilişimi), ardından kayıt sahibinin sosyal medya profiline (sosyal medya istihbaratı) ve son olarak karanlık bir ağ forumunda bulunan kripto para işlemlerine (finansal istihbarat) bağlaması gerekebilir.28 Temel beceri, bu alanlardan herhangi birinde derin uzmanlık değil, hepsinin geniş bir anlayışına ve bunları nasıl ilişkilendirebileceğini görme yaratıcılığına sahip olmaktır.

## Bölüm V: Temel Soruşturma Tekniklerinin Evrimi

Bu bölüm, özellikle tersine görüntü ve yüz tanıma araması gibi temel OSINT yöntemlerinin, yukarıda tartışılan trendler tarafından nasıl güçlendirildiğini ve yeni, daha güçlü uygulamalara yol açtığını incelemektedir.

### 9. Gelişmiş Tersine Görüntü ve Yüz Tanıma Araması

Bu trend, daha önce ayrı olan iki yeteneğin birleşmesini ve geliştirilmesini temsil etmektedir. Tersine görüntü arama artık sadece kopyaları bulmak için değil; güçlü, büyük ölçekli yüz tanıma ve nesne tanıma motorlarıyla entegre edilmektedir. Bu, analistlerin web genelinde insanları, nesneleri ve hatta kısmi görüntüleri artan bir doğrulukla aramasına olanak tanır.2

Modern tersine görüntü arama motorları, bir görüntüden benzersiz görsel özellikleri (şekiller, renkler, dokular) çıkarmak için özellikle Evrişimli Sinir Ağları (CNN'ler) olmak üzere gelişmiş yapay zeka kullanır ve dijital bir "parmak izi" oluşturur.2 PimEyes ve FaceOnLive gibi özel yüz tanıma arama motorları, bir yüzün vektör temsilini oluşturmak ve açık web, sosyal medya ve diğer kaynaklarda eşleşmeleri aramak için yüksek düzeyde ayarlanmış algoritmalar kullanır.55 Lenso.ai gibi araçlar, bu yetenekleri entegre ederek bir kullanıcının bir görüntü yüklemesine ve ardından sonuçları "İnsanlar", "Yerler", "Kopyalar" ve "Benzerler" olarak kategorize edilmiş şekilde görmesine olanak tanır, bu da yüz tanıma, jeolokasyon ipuçları ve standart tersine görüntü aramasını tek bir süreçte etkili bir şekilde birleştirir.54

Bu gelişmelerin en önemli sonuçlarından biri, halka açık olarak paylaşılan görüntülerde pratik anonimliğin sona ermesidir. Güçlü yüz tanıma arama araçlarının artan doğruluğu ve halka açık olması, halka açık bir fotoğraf veya videoda görünen herhangi bir yüzün potansiyel olarak tanımlanabileceği ve diğer çevrimiçi kimliklere bağlanabileceği anlamına gelir. PimEyes gibi araçlar, tek bir yüklenmiş fotoğraftan bir kişinin yüzünü çok sayıda web sitesinde zaten bulabilmektedir.55 Veritabanları büyüdükçe ve algoritmalar geliştikçe, önemli bir çevrimiçi varlığı olan herkes için başarılı bir eşleşme olasılığı kesinliğe yaklaşmaktadır.

Bir sonraki evrim, sadece tam bir görüntü veya bir yüz için değil, bir görüntü *içindeki* belirli bir nesne için arama yapma yeteneği olacaktır. Mevcut araçlar zaten bir görüntü içindeki nesneleri tanımlamada iyidir.6 Apple'ın Görsel Zeka'sındaki özelliklerin ima ettiği gibi mantıksal bir sonraki adım 57, bir kullanıcının bir fotoğraf içindeki bir nesneyi (örneğin, benzersiz bir sırt çantası, belirli bir dövme, bir üniforma üzerindeki bir şirket logosu) seçmesine ve web genelinde sadece o nesne için tersine arama yapmasına olanak tanımaktır. OSINT için bu, oyunun kurallarını değiştiren bir gelişmedir. Bir analist, gizlenmiş olabilecek yüzüyle değil, sürekli giydiği benzersiz bir giysi veya teçhizatla bir kişiyi takip edebilir. Tek bir fotoğraftan alınan benzersiz birlik yamalarını arayarak belirli bir askeri birliğin tüm üyelerini tanımlayabilirler.

### 10. Gerçek Zamanlı ve Tahmine Dayalı Görsel Zeka

Bu ileriye dönük trend, yukarıdaki tüm tekniklerin halka açık web kameraları, sosyal medya canlı yayınları ve drone görüntüleri gibi *canlı* görsel veri akışlarına uygulanmasını içerir. Bu, gerçek zamanlı izleme, olay tespiti ve hatta gelişen durumların tahmine dayalı analizini mümkün kılar.8

Bu yetenek, Maltego Monitor gibi platformların ve GDELT gibi hizmetlerin haber ve sosyal medyadan gerçek zamanlı veri akışlarını alıp işlemesiyle mümkün olur.28 Analizin etkili olabilmesi için neredeyse gerçek zamanlı olarak gerçekleşmesi gerekir. Bu, görsel verilerin merkezi bir buluta gönderilmek yerine, gecikmeyi azaltmak için "uçta" (veriyi yakalayan cihaza yakın veya üzerinde) işlenmesini gerektirir.8 Tarihsel ve gerçek zamanlı görsel verileri analiz ederek, YZ modelleri belirli olaylardan önce gelen kalıpları belirleyebilir. Örneğin, binlerce saatlik protesto görüntülerini analiz ederek, bir model belirli bir kalabalık yoğunluğunun ve hareket modelinin yakın bir şiddet olayının güçlü bir göstergesi olduğunu öğrenebilir ve önleyici uyarılara olanak tanıyabilir.38

Bu paradigma değişimi, OSINT analistinin rolünü de dönüştürmektedir. Gerçek zamanlı bir ortamda, insan "döngünün içinde" olmak için çok yavaştır. Rolleri, "döngünün üzerinde" olmaya kayacaktır; yani, izleme sistemlerini tasarlamak, YZ için uyarı parametrelerini ayarlamak ve otomatik istihbarat toplamayı yönetmek, bunu kendileri yapmaktan ziyade. Binlerce video akışının gerçek zamanlı analizi bir insan ekibi için imkansızdır.58 YZ ajanları ve entegre platformlar, bu akışları önceden tanımlanmış tetikleyiciler için izlemek üzere gereklidir.9 Analistin işi artık kamera yayınlarını izlemek değil, YZ için "angajman kurallarını" tanımlamak, doğru soruları sormak ve otomatik sistemin ürettiği uyarıların önemini yorumlamaktır.

Ancak bu yetenek, "suç öncesi" analizin etik açıdan sorunlu alanına girmektedir. Görsel verilere dayanarak olayları tahmin etme yeteneği, OSINT'i bu hassas alana itecektir. Bu tahmine dayalı modellerdeki önyargı ve hata potansiyeli, ciddi gerçek dünya sonuçlarına yol açabilir. YZ, tarihsel verilere ve tehdit aktörü davranışlarına dayanarak gelecekteki siber saldırıları tahmin etmek için kullanılabilir 38; aynı ilke görsel göstergelere dayanarak fiziksel olaylara da uygulanabilir. Kalabalık görsellerinin gerçek zamanlı analizine dayanarak yüksek bir isyan olasılığını tahmin eden bir sistem düşünün. Kolluk kuvvetleri bu tahmine göre hareket edebilir ve aksi takdirde barışçıl kalacak bir durumu potansiyel olarak tırmandırabilir. Tahmine dayalı modelin önyargıları varsa (Trend 2'de tartışıldığı gibi), belirli etnik veya politik grupların protestolarını "yüksek riskli" olarak işaretleme olasılığı daha yüksek olabilir ve bu da ayrımcı polisliğe yol açabilir.

## Sonuç

2025 yılına doğru ilerlerken, görsel istihbarat alanı, yapay zekanın dönüştürücü gücüyle yeniden şekillenmektedir. Bu raporun ortaya koyduğu on trend, sadece teknolojik ilerlemeleri değil, aynı zamanda OSINT pratiğinde temel bir paradigma değişimini de göstermektedir. Anlamsal arama ve bağlamsal zeka, analistleri anahtar kelimelerin kısıtlamalarından kurtararak, daha önce erişilemeyen içgörülerin kapısını aralamaktadır. 3B sahne rekonstrüksiyonu ve çok modlu jeo-uzamsal üçgenleme, bir fotoğrafın nerede çekildiğini belirleme görevini basit bir eşleştirmeden, yüksek kesinlikli bir simülasyon ve veri füzyonu sürecine dönüştürmektedir.

Ancak bu yeni yetenekler, ciddi zorlukları da beraberinde getirmektedir. Deepfake'lerin ve karşı-adli bilişim tekniklerinin yaygınlaşması, görsel kanıtların bütünlüğüne yönelik varoluşsal bir tehdit oluşturmakta ve analistleri sadece kanıt bulmakla değil, aynı zamanda buldukları kanıtların gerçekliğini ispatlamakla da yükümlü kılmaktadır. Algoritmik önyargı ve tahmine dayalı analizin etik sonuçları, bu güçlü araçların sorumlu bir şekilde kullanılmasını sağlamak için dikkatli bir gözetim gerektirmektedir.

Sonuç olarak, VISINT artık OSINT'in bir alt dalı değil, kendi başına temel bir istihbarat disiplinidir. Başarı, sadece en yeni araçlara erişime değil, aynı zamanda bu araçları yönlendirecek eleştirel düşünme, "veri füzyonisti" becerileri ve sağlam etik çerçevelere de bağlı olacaktır. Geleceğin analisti, büyük ölçekli otomasyonu yöneten, YZ'nin çıktılarını doğrulayan ve makinenin sağlayamayacağı stratejik içgörüyü sunan bir "gözetmen" rolünü üstlenecektir. Bu yeni ortamda yol almak, hem teknolojik adaptasyon hem de analitik titizlik gerektirecektir.

#### Alıntılanan çalışmalar

1. Reverse Image Search | Bellingcat's Online Investigation Toolkit - GitBook, erişim tarihi Haziran 24, 2025, <https://bellingcat.gitbook.io/toolkit/categories/image-video/reverse-image-search>
2. Reverse Image Search: The Ultimate Guide - W3era.com, erişim tarihi Haziran 24, 2025, <https://www.w3era.com/blog/seo/reverse-image-search/>
3. Semantic Image Search with OpenAI CLIP and Meta FAISS, erişim tarihi Haziran 24, 2025, <https://docs.ultralytics.com/guides/similarity-search/>
4. A Quick Guide to Semantic Image Search (with Examples) - Nyckel, erişim tarihi Haziran 24, 2025, <https://www.nyckel.com/blog/semantic-image-search/>
5. Easy AI: Classifying Images with AI Models - Bellingcat, erişim tarihi Haziran 24, 2025, <https://www.bellingcat.com/resources/how-tos/2024/08/15/easy-ai-zero-shot-ai-image-classification-smart-image-sorter/>
6. AI Image Analysis: Use Cases, Models & Real-World Examples - Roboflow Blog, erişim tarihi Haziran 24, 2025, <https://blog.roboflow.com/ai-image-analysis/>
7. Why Context Matters in Artificial Intelligence - testRigor AI-Based Automated Testing Tool, erişim tarihi Haziran 24, 2025, <https://testrigor.com/blog/ai-context/>
8. The Power of Contextual Decisions for Real-Time Visual Intelligence - RTInsights, erişim tarihi Haziran 24, 2025, <https://www.rtinsights.com/the-power-of-contextual-decisions-for-real-time-visual-intelligence/>
9. Vision AI: Image and visual AI tools | Google Cloud, erişim tarihi Haziran 24, 2025, <https://cloud.google.com/vision>
10. What Is Contextual AI and How Does It Work - Yonyx, erişim tarihi Haziran 24, 2025, <https://corp.yonyx.com/knowledgebase/what-is-contextual-ai-and-how-does-it-work/>
11. Visual Intelligence - AlertMedia, erişim tarihi Haziran 24, 2025, <https://www.alertmedia.com/platform/visual-intelligence/>
12. Image Analysis and Geolocation with OSINT, erişim tarihi Haziran 24, 2025, <https://www.osintcombine.com/post/from-images-to-intelligence>
13. Understanding and evaluating harms of AI-generated image captions in political images, erişim tarihi Haziran 24, 2025, <https://www.frontiersin.org/journals/political-science/articles/10.3389/fpos.2023.1245684/full>
14. Understanding and evaluating harms of AI-generated image captions in political images - mediaTUM, erişim tarihi Haziran 24, 2025, <https://mediatum.ub.tum.de/doc/1730478/1730478.pdf>
15. The Role of Artificial Intelligence in Shaping Collective Imagination and Reinforcing Cultural and Social Bias - TrIBES, erişim tarihi Haziran 24, 2025, <https://tribes.hypotheses.org/4080>
16. KnowAI The Impact of AI on Political Knowledge, Opinion, and Democracy - UiO, erişim tarihi Haziran 24, 2025, <https://www.hf.uio.no/imk/english/research/projects/ai-political-knowledge-opinion-democracy/>
17. Researchers show how AI tools can be tuned to reflect specific political ideologies, erişim tarihi Haziran 24, 2025, <https://www.brown.edu/news/2024-10-22/ai-bias>
18. Space-Based 3D Reconstruction: Advancing Object ... - Scout Space, erişim tarihi Haziran 24, 2025, <https://www.scout.space/news/3d-reconstruction>
19. We're launching photorealistic Neural Radiance Fields (NeRF) at Mapillary!, erişim tarihi Haziran 24, 2025, <https://forum.mapillary.com/t/were-launching-photorealistic-neural-radiance-fields-nerf-at-mapillary/7878>
20. Exploring the Skyline: How we Located an Alleged Cartel Member in ..., erişim tarihi Haziran 24, 2025, <https://www.bellingcat.com/resources/2024/07/16/dubai-uae-cartel-organised-crime-geolocation-open-source-guide-technique-tools/>
21. NeRF capture instructions - Mapillary, erişim tarihi Haziran 24, 2025, <https://help.mapillary.com/hc/en-us/articles/12769328936476-NeRF-capture-instructions>
22. The NeRFect Match: Exploring NeRF Features for Visual Localization - arXiv, erişim tarihi Haziran 24, 2025, <https://arxiv.org/html/2403.09577v2>
23. CaLiSa-NeRF: Neural Radiance Field with ... - CVF Open Access, erişim tarihi Haziran 24, 2025, <https://openaccess.thecvf.com/content/WACV2025W/GeoCV/papers/Han_CaLiSa-NeRF_Neural_Radiance_Field_with_Pinhole_Camera_Images_LiDAR_point_WACVW_2025_paper.pdf>
24. Forensic Photogrammetry: A Case Study - PhotoModeler, erişim tarihi Haziran 24, 2025, <https://www.photomodeler.com/forensic-photogrammetry-case-study/>
25. OSINT Techniques: Complete List for Investigators (2025 ..., erişim tarihi Haziran 24, 2025, <https://shadowdragon.io/blog/osint-techniques/>
26. Top 9 OSINT Tools | Wiz, erişim tarihi Haziran 24, 2025, <https://www.wiz.io/academy/osint-tools>
27. OSINT Tools And Techniques | OSINT Technical Sources - Neotas, erişim tarihi Haziran 24, 2025, <https://www.neotas.com/osint-tools-and-techniques/>
28. The Top OSINT Data Sources | Venntel, erişim tarihi Haziran 24, 2025, <https://venntel.com/blog/osint-data-sources>
29. OSINT Industries | Powerful Tools For Online Investigations, erişim tarihi Haziran 24, 2025, <https://www.osint.industries/>
30. OSINT with Maltego - Home - ParadigmIT Cybersecurity, erişim tarihi Haziran 24, 2025, <https://paradigmitcyber.com/osint-with-maltego/>
31. OSINT Challenge: Marina Geolocation - YouTube, erişim tarihi Haziran 24, 2025, <https://m.youtube.com/watch?v=mQDawXmBqsQ>
32. Finding a Location from an Image | Geolocation, OSINT Challenge | Episode No. 1, erişim tarihi Haziran 24, 2025, <https://www.youtube.com/watch?v=CWMF8Bx_Lyk&pp=0gcJCdgAo7VqN5tD>
33. Counter-Forensics: Attacking Image Forensics - ResearchGate, erişim tarihi Haziran 24, 2025, <https://www.researchgate.net/publication/285348215_Counter-Forensics_Attacking_Image_Forensics>
34. A quick guide to digital image forensics | CameraForensics, erişim tarihi Haziran 24, 2025, <https://cameraforensics.com/blog/2020/03/06/a-quick-guide-to-digital-image-forensics-in-2020/>
35. Open Source Intelligence Market Trends 2025-2034: Growth, Strategic Insights, and Opportunities Ahead, erişim tarihi Haziran 24, 2025, <https://blog.tbrc.info/2025/05/open-source-intelligence-market-analysis/>
36. Best OSINT Tools | Sintelix, erişim tarihi Haziran 24, 2025, <https://sintelix.com/best-osint-tools/>
37. Deepfakes and Disinformation: The Rapidly Growing Threat to OSINT, erişim tarihi Haziran 24, 2025, <https://facia.ai/blog/deepfakes-and-disinformation-the-rapidly-growing-threat-to-osint/>
38. AI-Enhanced Data Collection for OSINT Investigations | How Artificial Intelligence is Transforming Open-Source Intelligence and Cybersecurity - Web Asha Technologies, erişim tarihi Haziran 24, 2025, <https://www.webasha.com/blog/ai-enhanced-data-collection-for-osint-investigations-how-artificial-intelligence-is-transforming-open-source-intelligence-and-cybersecurity>
39. Open Source Intelligence (OSINT): This Person Doesn't Exist (Deep Fakes and AI), erişim tarihi Haziran 24, 2025, <https://hackers-arise.com/open-source-intelligence-osint-this-person-doesnt-exist-deep-fakes-and-ai/>
40. Detecting AI in OSINT Investigations - SANS Institute, erişim tarihi Haziran 24, 2025, <https://www.sans.org/webcasts/detecting-ai-in-osint-investigations-oct-2024/>
41. Unmasking Digital Deception: Deepfake Detection in OSINT Investigations - Carahsoft, erişim tarihi Haziran 24, 2025, <https://www.carahsoft.com/learn/event/65270-unmasking-digital-deception-deepfake-detection-in-osint-investigations>
42. Unpacking image forensics: what it is and why it matters - CameraForensics, erişim tarihi Haziran 24, 2025, <https://www.cameraforensics.com/blog/2024/01/18/unpacking-image-forensics-what-it-is-and-why-it-matters/>
43. Metadata Forensics: Uncovering Hidden Truths in Digital Files | Ironhack Blog, erişim tarihi Haziran 24, 2025, <https://www.ironhack.com/us/blog/metadata-forensics-when-files-can-speak-and-reveal-the-truth>
44. Best OSINT Tools for Advanced Intelligence Gathering (2025 ..., erişim tarihi Haziran 24, 2025, <https://shadowdragon.io/blog/best-osint-tools/>
45. OSINT Sources: Geolocation OSINT And Investigation Techniques - Neotas, erişim tarihi Haziran 24, 2025, <https://www.neotas.com/osint-sources-geolocation-osint/>
46. AI-Powered OSINT Tools in 2025 | How Artificial Intelligence is ..., erişim tarihi Haziran 24, 2025, <https://www.webasha.com/blog/ai-powered-osint-tools-in-2025-how-artificial-intelligence-is-transforming-open-source-intelligence-gathering>
47. OSINT at Scale: Using AI Computer Vision Agents to Assist ..., erişim tarihi Haziran 24, 2025, <https://www.sans.org/webcasts/osint-scale-using-ai-computer-vision-agents-assist-investigations/>
48. OSINT: Open Source Intelligence, Frameworks, and Cybersecurity Applications - Group-IB, erişim tarihi Haziran 24, 2025, <https://www.group-ib.com/resources/knowledge-hub/osint/>
49. Top 15 OSINT Tools for Powerful Intelligence Gathering - Cyble, erişim tarihi Haziran 24, 2025, <https://cyble.com/knowledge-hub/top-15-osint-tools-for-powerful-intelligence-gathering/>
50. Breaking Down AI Image Analysis - Cloudinary, erişim tarihi Haziran 24, 2025, <https://cloudinary.com/guides/ai/ai-image-analysis>
51. The Impact of AI with OSINT - YouTube, erişim tarihi Haziran 24, 2025, <https://www.youtube.com/watch?v=zgIteU4jEZs>
52. Maltego | OSINT & Cyber Investigations Platform for High-Stakes Cases, erişim tarihi Haziran 24, 2025, <https://www.maltego.com/>
53. Harnessing OSINT in Criminal Investigations: A Case Study on the Fugitive Emmanuel Edokpolor - ESPY, erişim tarihi Haziran 24, 2025, <https://espysys.com/blog/harnessing-osint-in-criminal-investigations-a-case-study-on-the-fugitive-emmanuel-edokpolor/>
54. Top 5 Best Image Recognition Software in 2025 - Tech Times, erişim tarihi Haziran 24, 2025, <https://www.techtimes.com/articles/309265/20250202/top-5-best-image-recognition-software-2025.htm>
55. Free Reverse Image Search Tools Ranked: The Best Options in 2025 [Updated] - FaceOnLive : On-Premises ID Verification & Biometrics Solution Provider, erişim tarihi Haziran 24, 2025, <https://faceonlive.com/free-reverse-image-search-tools-ranked-the-best-options-in-2025-updated/>
56. Top 10 Platforms for Reverse Image Search by Photo in 2025, erişim tarihi Haziran 24, 2025, <https://www.pageon.ai/blog/visual-search-by-photo>
57. Apple Intelligence gets even more powerful with new capabilities across Apple devices, erişim tarihi Haziran 24, 2025, <https://www.apple.com/newsroom/2025/06/apple-intelligence-gets-even-more-powerful-with-new-capabilities-across-apple-devices/>
58. Real Time Visual Intelligence Resources - RTInsights, erişim tarihi Haziran 24, 2025, <https://www.rtinsights.com/hubs/real-time-visual-intelligence-resources/>
59. What is OSINT [Open-Source Intelligence]? Complete Guide - ShadowDragon.io, erişim tarihi Haziran 24, 2025, <https://shadowdragon.io/blog/what-is-osint/>