Drone ile Nesne Tanıma ve Yayınla/Abone-ol Tabanlı Güvenli Görüntü Aktarımı

Ümmühan TEPEBAŞ[1,1*], Mürvet Nur ŞEN[1,1*], Seda KUL[1,1] and Ahmet SAYAR[1,1†]

Mühendislik Fakültesi,Bilgisayar Mühendisliği Bölümü, Kocaeli Üniversitesi,Kocaeli Türkiye.

*Corresponding author(s). E-mail(s): ummuhantepebas@gmail.com; murvetnursen@gmail.com;
Contributing authors: seda.kul@kocaeli.edu.tr; ahmet.sayar@kocaeli.edu.tr;
†These authors contributed equally to this work.

Abstract

Drone cihazları günümüzde gelişen teknoloji ile kullanım alanı ve yaygınlığı artmıştır. Bu projede temel motivasyon bu denli geniş ölçekli kullanılan elektronik cihazların drone' dan drone'a veya drone' dan yer istasyonuna yapılan veri iletiminde etkili bir güvenlik açığı tespit edilip bu problem için kriptolojik yöntemlerle çözüm sağlanmasıdır. Öncelikle kriptolojik yaklaşım için efektif algoritmalar incelenerek, drone cihazlarının siber güvenlik ve veri aktarımındaki açıkların tespit edilmesi sonrası, iyileştirilmesi için incelenen kriptolojik yaklaşımlar ile çözüm sağlama adımları hedeflenmiştir. Bu hedef, veri iletimi bir yayınla/abone ol dağıtık haberleşme sistemiyle Apache-Kafka kullanılarak gerçekleştirilmiştir. Projenin gereksinimleri haberleşme için: Veri İletimi (Yayınla/Abone ol), dağıtık sistem olarak: Apache Kafka, haberleşecek cihazlar olarak: Drone-Bilgisayar Haberleşmesi, nesne tespiti için kullanılacak model: YOLOv4 veya YOLOv4-tiny, güvenliğin sağlanması için ise Advanced Encrption Standart - Rijndael (AES) tabanlı Cryptocode kütüphanesi kullanılmıştır.

Keywords: Bilgi Güvenliği, Dağıtık ortam, Drone'larla Nesne Tespiti, Kriptoloji, Veri iletimi, AES

1 Giriş

Geçmişi 1. Dünya Savaşına kadar uzanan fiziksel olarak içinde insan bulunmadan uçan bu araçlara Türkçe adıyla İnsansız Hava Aracı (İHA), İngilizce adıyla drone'lar günümüze kadar birçok farklı amaçlarla kullanılmıştır. Kullanımına tekniğine göre bu cihazlar ikiye ayrılırlar: Belirli bir uçuş planı oluşturarak otomatik uçuş yapabilen veya uzaktan kumanda edilerek uçuş yapabilenler. İlk zamanlarında uzaktan kumanda olarak telsiz ile kontrol edilebilen bu cihazlar savaş alanı için önemli bir buluştu. 2010 yılında akıllı telefonların gelişmesi ile bu cihazların kullanımı kullanıcı dostu ve kolay erişilebilir, kolay kullanılabilir hale geldi. Gelişen teknoloji diğer tüm cihazlarda olduğu gibi drone için de yeni sürümler ve yeni teknolojiler ile farklı şekil ebat, işlevsellik eklenerek geliştirildi. Bunun neticesinde günümüzde birçok sektör tarafından aktif olarak kullanılmaktadır. Örnek olarak ünlü e-ticaret şirketi olan Amazon, yaptığı açıklamada, teslimat için geliştirdikleri Prime Air adlı drone için, "Prime Air, insansız hava araçlarıyla paket teslim etme hedefimizi gerçeğe dönüştürmeye kararlıdır, yeni bir zemine öncülük ediyoruz ve paketleri müşterilere güvenli bir şekilde teslim etmek için doğru teknoloji ve alt yapıyı oluşturmak zaman almaya devam edecek [1] " diye belirtmiştir.

Dronelar pilotlar için tehlikeli olabilecek görevlerde kullanılması insan hayatı için bir avantajdır. Örneğin National Oceanic and Atmospheric Administration (NOAA) bir fırtına-kasırga avcısı olarak Aerosonde adlı drone kullanmakta ve bu cihaz gerçekleşen hava olaylarından etkileyici görüntüler almaktadır. Diğer yandan araştırmacılar Dünya dışındaki gezegenlerde de bilimsel araştırmalarda bulunmak için "Entomopter" adlı drone geliştirmekte ve bu çalışma NASA tarafından finanse edilmektedir. Arama, kurtarma, hasar tespiti çalışmalarında da kullanılmak üzere geliştirilen General Atomics MQ-1 Predator adlı drone üzerinde bulunan görsel algılayıcılar ile çektiği başarılı görüntüler bilgisayarlar kullanılarak işaretlenir ve hasar tespiti yapılır. Film sektöründe ise kullanılan sabit kameralar veya kamera rayları, vinçlerinin kısıtlı kullanımı nedeniyle drone kullanımı yeni görüntü perspektifleri sağladığı için yeni yeni tercih edilmektedir. Bahsedildiği üzere dronelar günümüzde birçok sektör tarafından aktif olarak kullanılmaktadır. Bu denli geniş kullanıma sahip bu cihazlar elbette bazı siber saldırılara karşı açık hale gelebilmektedir. Örnek olarak Security Analyst Summit' de güvenlik uzmanı olan Jonathan Andersson' un yayınladığı çalışmaya göre drone kaçırmanın yeterince uzman biri için çok az zamana ihtiyacı olduğunu belirtir [2].

Bu çalışmada temel motivasyon olarak dronelardan elde edilen verilerin "yayınla/abone ol" haberleşme modeli ile iletilmesinde kriptolojik yaklaşımlar ve şifreleme algoritmaları kullanılarak gerçekleşebilecek güvenlik açıklarının önüne geçmek amaçlanmaktadır. Bu güvenlik açığını gidermek için şifreleme algoritmaları ile ilgili literatür taramalarına göre geleneksel metin şifreleme algoritmaları görsel şifreleme için zayıf güvenlikte olduğu anlaşılmıştır.

Bu bağlamda şifreleme metodlarının detaylı performans analizi ve incelemesi yapılmıştır. Dağıtık ortamda "Yayınla/Abone ol" sisteminin kullanılması ile bir üretici dronedan çekilen veri Apache Kafka ekosisteminde yaratılan başlıklarda (topic) belirlenen filtrelere göre veri yayını yapar. Diğer uç sistemde bulunan tüketici cihaz bu yayınlanan veri hakkında bilgi sahibi değildir. Şifreleme algoritması ile güvenli görüntü aktarımı sağlamak için veriyi şifreleyerek dağıtır. Tüketici veri çekmek isterse abone olarak istediği veriyi veya nesneyi şifre çözümleme algoritmasından sonra çeker. Dronelardan elde edilen veriler yayınla/abone ol haberleşme modeli ile iletilmesinde çeşitli şifreleme algoritmaları kullanılarak gerçekleşebilecek güvenlik açıklarının önüne geçmek hedeflenmektedir, böylelikle sektörde drone cihazı kullanımı ile elde edilen verilerin güvenliği daha da artırılmış olacaktır.

Bu makalenin devamında çalışma ile ilgili yapılan çalışmalardan yer aldığı 2. bölüm, projenin detaylı mimarisinin anlatıldığı 3. bölüm, gerçekleştirilen testler ve elde edilen değerlerin yer aldığı 4. bölüm ve son olarak sonuçların yer aldığı 5. bölüm ile devam etmektedir.

2 İlgili Çalışmalar

Daha önce drone ile güvenli görüntü aktarımı ile ilgili akademik araştırmalara ulaşamayınca çalışma için birkaç adımda literatür taraması gerçekleştirilmiştir. Öncelikli olarak drone ile iletişim için protokol taraması gerçekleştirilmiştir. Buna örnek drone ile araç takibi ve güvenlik açıklarının tespit edilmesi için MAVLink protokolü hakkında yapılan çalışmalar bulunmaktadır. Bunlardan biri "Security Analysis of the Drone Communication Protocol [3]" adlı makalede bahsedilen güvenlik açıklarının tespit edilmesi için çalışılmıştır. Bu çalışma fuzzing tekniğini kullanarak yazılım açıklarını belirlemeyi amaçlamaktadır.

Yayınla/abone-ol ile ilgili yapılan çalışmalara Rodriguez [4] ,"Publish/Subscribe data communication in Cyber-Physical Systems oriented to Unmanned Aerial Vehicle" örnek verilebilir. Çalışmanın amacı dronların ve diğer otonom insansız araçların uzaktan kontrolü için Data Distribution Service (DDS) kullanan veri seviyesi iletişimine dayalı bir sistem geliştirmektir.

Bal [5], "İnsansız Hava ve Kara Araçları için Görüntü ile Yer tespiti ve Yönlendirme" adlı araştırmasındaki amaç, farklı bölgelerin görüntü üzerindeki hayali yapısını belirlemek ve nereye ait olduklarını bilmektir. Görüntü üzerindeki işaretler, bitkiler, hava durumu desenleri, yol işaretleri ve mimari detaylar görüntünün çekildiği yer hakkında bilgi verir. Bu bilgi, fotoğrafın nerede çekildiğine karar vermede çok yararlıdır. Görüntü konumlandırma sistemi yardımıyla farklı coğrafi bölgelerin görüntü yapısı görsel olarak tespit edilecek ve hedef çıkarılacaktır. Çıkarılan bu nesne, veri kümesindeki görüntülerle karşılaştırılacak ve eşleşen görüntüler, veri kümesindeki konum

bilgisine göre etiketlenecektir. Konuma özel görüntüler, insansız kara ve hava araçlarını tanımlamak ve yönlendirmek için kullanılabilir. Günümüz savunma sanayiinde çeşitli görevler için ve İHA'lara rehberlik edecek görüntü tabanlı bir konum tespit sistemi geliştirmeyi amaçlamaktadır.

Diğer adımda ise çalışmanın büyük önem içeren bölümü görüntü şifreleme literatür taramalarında ise yöntem, metod ve algoritmalarının çok çeşitli olması sebebiyle öncelikle geleneksel daha sonra görüntü şifreleme alanındaki makaleler incelenmiştir. Krikor ve arkadaşları [6] DCT (Discrete Cosine Transform) adlı bir yöntem önerir. DCT yönteminde Şifreli bloklar rastgele karıştırılmaktadır. Pia ve Karamjeet [7] Blowfish 64 bitlik metodu kullanmıştır. Bu metodda güvenliği ve performansı artırmak için gizli bir anahtar (448 bite kadar değişebilen) bloğu şifresini kullanmıştır. Tang [8] görüntü ve videolarda "Zigzag permütasyon" adlı DCT tabanlı belirli düzeyde gizlilik sağlayan yöntem önermiş ve uygulamıştır. İsmail ve arkadaşları [9] kaos tabanlı şifreleme algoritması üzerine yöntem araştırmaları yapmıştır.

Brindha, Sharma ve Saini [10] görüntü şifreleme için DES algoritmasını yöntem araştırması yapmıştır. DES algoritması iletim anında yüksek güvenlik sağlar. Yazarlar çalışmalarında DES ve AES karşılaştırması yapmışlardır. Zhang ve Wang [11] "Bitişik olmayan eşleştirilmiş harita kafeslerine dayalı yeni bir görüntü şifreleme algoritması" simülasyonlarda algoritmaların güvenlik ve verimlilik değerlerini diğer algoritmalar ile kıyaslamıştır. Ghode [12] anahtarsız bir şifreleme çalışması yapmıştır. Kayıpsız RGB görüntülerinin güvenlik seviyesini artırmanın yanı sıra depolama kapasitesi için de geliştirici çözümler sunmuştur.

İlgili algoritmaların karşılaştırmalı tabloları algoritma performansları hakkında detaylı bilgiye erişmeye ve bu çalışmada kullanılcak şifreleme algoritmasının belirlenmesinde yardımcı olmuştur. Ceyhan YOLAÇAN, "Görüntü Dosyalarının Şifrelenerek Güvenli Şekilde Saklanması" [13] 2021 yılındaki yayınlanan makalesinde de şifreleme algoritmalarına kendi çalışmaları ile değinmiş ve referans olarak kullanılabilecek şifreleme algoritmaları karşılaştırma tablosu oluşturmuştur.

Belirtilen tabloda özet olarak çeşitli şifreleme algoritmalarının kaba Kuvvet (Brute Force) saldırılarına karşı dayanıklılık süreleri ölçülmüştür. AES için yıllarla ölçüm birimiyle Brute Force Saldırısını gerçekleştirmek için geçen süre: x= (anahtar uzunluğu - 1) için 2^x / anahtar sayısı sonucu olarak 6.42711E+23 olarak belirtilmektedir. AES 128(2^7) baytlık bir blok boyutu kullanır. Brute Force saldırısında şifrenin kırılmasını hesaplamak için anahtar uzunluğundan yararlanılmaktadır. Bu nedenle ortalama olarak çok çekirdekli ve yüksek RAM hızına sahip performanslı bir bilgisayar saniyede 2(30-7) = 223 blok şifreleyebileceği ve bu da saniyede 223 farklı şifreleme anahtarını da deneyebileceği anlamına gelmektedir. Bir yıl 31,557,600 (60(saniye)*

60(dakika)* 24(saat)* 365,25(gün)) saniyedir. Çalışma performansı yüksek bir bilgisayar 31,557,660 * blok sayısı kadar şifre denemesi yapabilmektedir.

Bir diğer tabloda da maksimum 6.8MB - minumum 562KB ve renkli yedi yüz görüntü verisi kullanılarak yapılan testte çeşitli şifreleme algoritmalarının şifreleme için harcanan maksimum- minimum ve toplam şifreleme süresi milisaniye cinsinden ölçülerek gösterdiği farklılıklar incelenmiştir. AES-128 için bu değerler maksimum değer için 0.0705 ms, minimum değer için 0.0023 ms ve toplam değer için 17.3441 ms olarak ölçülmüştür. Tüm bu incelemeler sonucunda görüntü şifreleme tekniği olarak AES-128 uygun görülmüştür [13].

Bu çalışma sonucunda diğer çalışmalardan farklı olarak sadece belirli bir kriptolojik algoritma ile görsel şifrelemekten ziyade dronedan alınan görsel verilerin siber saldırı türlerine karşı güvenli aktarabilmek amaçlanmakta. Bunun için ilk adımda halen daha güçlü bir siber atak olan Brute Force' a karşı yüksek performans gösteren AES-128 kullanımına karar verilmiştir. Bu sistemin endüstri alanında da etkili olabilmesi için nesne tespiti adımları da eklenmiştir. Güvenli görüntü aktarımı amacında hem yayınla/abone-ol hem de nesne tespiti yapabilen bir başka çalışmaya literatürde erişilememiştir. Kriptolojik algoritmayı dağıtık ortama entegere ederek güvenli veri aktarımı ile nesne tespiti sağlayarak bu alanda yeni bir çalışma sunulmuştur.

3 Drone ile Nesne Tanıma ve Yayınla/abone-ol ile Güvenli Aktarımı Mimarisi

Dronedan elde edilen görüntü verileri, publish-subscribe dağıtık sistem ortamı olan Apache Kafka ortamında yayınlanır (raw-data topik). Yayınlama işlemi Kafka Broker'ları üzerinden yapılır. Bu alt sistemde topicler vardır ve üretilen topice görüntü yayınlandıktan sonra tüketici taraftan aynı topic üzerinden abone olma yöntemiyle işlem gerçekleşir. Bilgisayara aktarılan görsel veriler YOLO v4-tiny derin öğrenme modeli ile nesne tespiti yapılır. Nesneler (Apache Avro) serialize işleminden sonra şifreleme algoritmaları (DES/3DES/Blowfish/Scan) ile şifreleme işlemi gerçekleştirilir. Son olarak yayınlama (produce), alıcıların (subscriber) veriyi consume etmesi ile sonlanır (Şekil 3). Görüntü işleme yoluyla görüntülerden elde edilen bilgiler, görüntü üzerindeki nesneleri işaretlemenin ötesine geçer. Görüntülerden elde edilebilecek bilgilerin artması ve sürekli gelişen algoritmalar beklentileri ve talepleri artırmıştır. Bu aynı zamanda görüntünün konumunu belirlemek için görüntü işlemeyi kullanma gereksinimlerini de karşılar[2].

Bu çalışmada çeşitli algoritmalar araştırılıp test edilmiş ve uygun şifreleme algoritması çalışmaya entegre edilmiştir. Öncesinde denenen algoritmalar Kaotik haritalandırma yöntemi ile şifreleme ve Scan ile sıkıştırarak şifreleme üzerine çalışmalar yapılmış fakat görüntü iletme adımları ile uyum

sağlayamadığı için AES ile şifreleme sağlanmıştır. AES şifreleme metodolojisi güncel olarak da şifreleme algoritmaları içinde en yaygın kullanılan bu algoritma halen Brute Force saldırısına dayanıklı olduğu için bu çalışmada da tercih edilmiştir. Blok şifreleme algoritmalarının en bilineni AES şifreleme algoritmasında SPN mimarisi ve 4 katmanlı döngü ile güvenlik sağlanır. 128 bitlik girdi veri bloklarını, 128, 192, 256 bit anahtar seçenekleri ile şifreler. Her döngü 4 farklı katmandan oluşur: SubBytes, ShiftRows, MixColumns (Yayılma katmanı), AddRoundKey.

İlk olarak 128 bit veri 4*4 byte durum (state) matrisine dönüştürülür. Durumun her bölmesine 1 byte (8 Bit) veri düşer. AES algoritmasında başlangıçta 128 bitlik açık metin bloğu ana anahtar ile XOR işlemine tabi tutulur. Blok şifrelemenin doğrusal olmayan (non-linear) tek yapısı olan S-kutularını doğrusal hale getirilmesi gerekir. Sonraki devam eden adımlar:

1:Her döngüde sırasıyla byte'ların yer değiştirmesi "SubBytes", S-kutuları

2:Satırların ötelenmesi ShiftRows, Karıştırma "Confusion", sola dairesel

3:Sütunların yer değiştirmesi, MixColumns, Yayılma "Diffusion"

4:Anahtar planlamadan gelen döngü için belirlenen alt anahtar (döngü anahtarı) ile XOR işlemine tabi tutma, AddRoundKey

Veri iletiminde kullanılan dağıtık ortam Kafka, dağıtılmış, bölümlenmiş, çoğaltılmış bir kayıt günlüğü hizmetidir. Bir mesajlaşma sisteminin işlevselliğini sağlar, ancak benzersiz bir tasarıma sahiptir. Kafka bir küme olarak çalışır ve düğümlere brokerlar denir. Brokerlar, yüksek kullanılabilirlik ve hata toleransı sağlamak için liderler veya kopyalar olabilir. Brokerlar, mesajların depolandığı dağıtım birimi olan bölümlerden sorumludur. Bu mesajlar sıralanır ve ofset adı verilen bir dizin tarafından erişilebilir. Bir dizi bölüm, bir mesaj beslemesi olarak bir konu oluşturur. Bir bölümün farklı tüketicileri olabilir ve mesajlara kendi ofsetini kullanarak erişirler. Yayıncılar mesajları Kafka "başlıklarla (topic)" yayınlar.

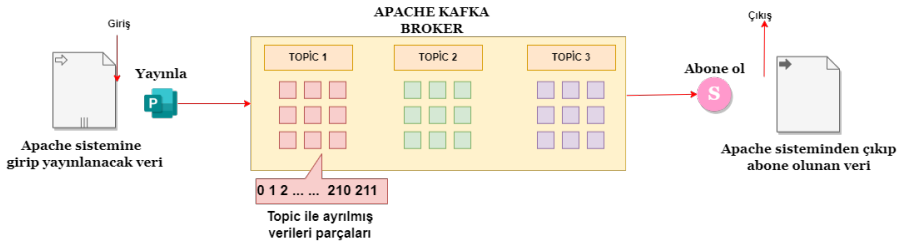

Fig. 1 Yayınla/Abone ol Haberleşmede "Topic" Modeli

Nesne algılama, bir sinir ağının bir görüntüdeki nesneleri tahmin ettiği ve bunları sınırlayıcı kutular biçiminde gösterdiği gelişmiş bir görüntü sınıflandırma biçimidir. Nesne algılama, bu nedenle, önceden tanımlanmış bir sınıf kümesine ait olan bir görüntüdeki nesnelerin algılanması ve yerelleştirilmesi anlamına gelir. Algılama, tanıma veya yerelleştirme gibi

görevler, gerçek dünya senaryolarında yaygın olarak uygulanabilirlik bularak nesne algılamayı (nesne tanıma olarak da anılır) Bilgisayar görüşünün çok önemli bir alt alanı haline getirir. Nesne tespitinde YOLOv4-tiny kullanılmıştır. YOLOv4,, modern düzenleme ve veri artırma yöntemleri arasında metodolojik değişiklikler olarak Ağırlıklı Artık Bağlantılar, Çapraz Mini Toplu Normalleştirme, Aşamalar Arası Kısmi Bağlantılar, Kendi Kendine Düşmanlık Eğitimi ve Mish Aktivasyonu'nun eklenmesini önerir. YOLOv4-tiny, YOLOv4'ün sıkıştırılmış versiyonudur. Ağ yapısını daha basit hale getirmek ve parametreleri azaltmak, böylece mobil ve gömülü cihazlarda geliştirmeyi mümkün kılmak için YOLOv4'e dayalı olarak önerilmiştir. YOLOv4-tiny'yi daha hızlı eğitim ve daha hızlı algılamaya sahip olduğu için bu çalışmada kullanılmıştır. Gerçek zamanlı nesne algılama için YOLOv4-tiny, YOLOv4 ile karşılaştırıldığında daha iyi bir seçenektir, çünkü gerçek zamanlı nesne algılama ortamıyla çalışırken daha hızlı çıkarım süresi kesinlik veya doğruluktan daha önemlidir.

MAVLink, iki varlığın bilgi alışverişinde bulunmasına izin veren noktadan noktaya bir iletişim protokolüdür. MAVLink ve İHA arasında iki yönlü iletişim için kullanılan, Linux [14] tarafından yürütülen "Drone Code" projesinin bir parçasıdır. Model olarak noktadan noktaya yayınla/abone-ol kullanır ve mesajlarını XML dosyasını kullanarak paylaşır. Ağ üzerinde eş zamanlı olmak üzere 255 sistem kullanımına izin verebilir[15]. MAVLink kullanan cihazlar için örnek verilecek olursak, PX4FMU, SmartAP, Armazila, Hexo+, TauLabs. MIT lisansı altında kullanıma açıktır. MAVLink Mesaj, iletişim kanalı aracılığıyla bayt olarak gönderilir, ardından bir sağlama toplamı gelir. Sağlama toplamı eşleşmiyorsa, mesaj hasarlı olup imha edilecektir. Malzeme yetersizliğinden dolayı bu çalışmada gerçek zamanlı görüntü aktarımı için dahili kamera kullanılmıştır. Mavlink protokolü çalışması teoride kalmış deneme gerçekleşmemiştir.

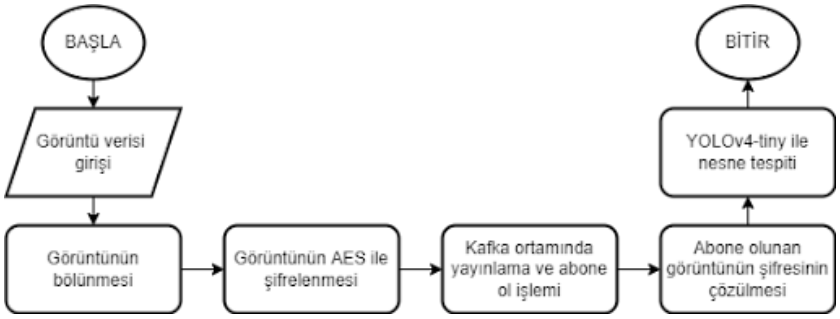

Fig. 2 Algoritmanın Akış Şeması

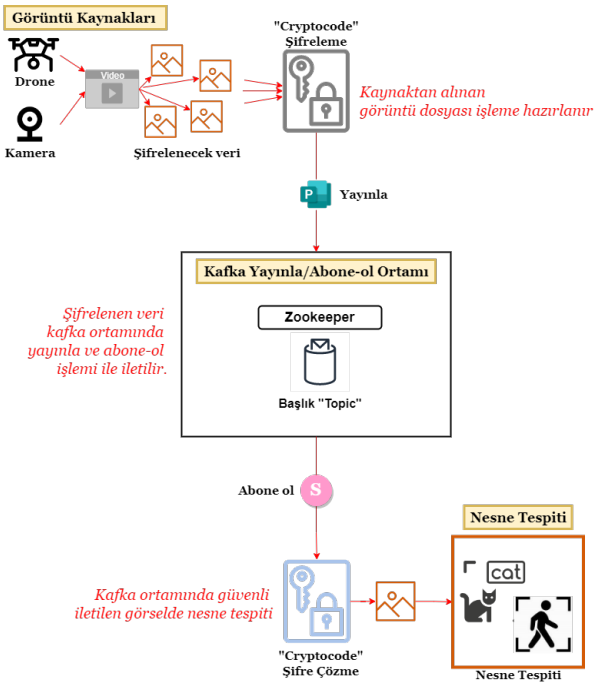

Fig. 3 Algoritmanın Akış Şeması

4 Gerçekleştirilen Testler ve Değerlendirilmesi

Amacımız olan dronedan şifrelemek için alınan görüntüyü dosyasını malzeme eksikliği nedeniyle yine gerçek zamanlı görüntüyü destekleyecek şekilde dahili kamera kullanarak sağlamaktayız. Alınan gerçek zamanlı görüntüyü anlık tek tek çerçevede (frame) işleyebilmek için bir algoritma geliştirilmiştir. Proje çalıştırılmadan önce Kafka ortamı için önceki bölümlerde açıklanan zookeeper ve kafka server komut isteminden ilgili komutlarla aktif hale getirilmelidir.

Birden fazla çerçevelere ayrılan görüntüler şifreleme işlemine hazır hale gelmiştir. Şifreleme işlemi için simetrik anahtarlı AES tabanlı Python “Cryptocode” kütüphanesi kullanılmıştır. Gönderilecek olan görüntünün iletim ortamının Apache Kafka dağıtık sistemde yayınla/abone-ol mimarisi ile gerçekleşeceği daha önceki bölümlerde belirtilmiştir. Bunun için sistem aşağıda verilen kod ile Kafka bootstrap server’ a localhost 9092 portu ile bağlanıp yayınlama (produce) işlemi için hazır hale getirilir.

Proje aslında dronedan çekilen ama kullanımda dahili kamera cihazından alınan anlık canlı görüntü verisi “Opencv” kütüphanesi ile framelere bölünür. Dahili kameradan alınan bu görüntü framelerinin boyutu öğrenilip , bu boyuta göre frame yeniden şekillendirilir. Dikey ve yatay eksenlerden oluşan görüntü matrisi tek boyutlu bir matrise (diziye) çevrildikten sonra liste veri tipine dönüştürülür. Her bir veri(proje kodunda rakamlarla ifade edilmekte) arasına virgül eklenerek bir string haline getirilir. Ayrılan tüm frameler teker teker

şifreleme algoritmasına tabi tutulur. Görüntü verileri byteları şifrelenebilir bir string haline getirilir. Bu string kullanılan şifreleme anahtarı ile şifrelenir. Bu şifreli görsel stringi ortamda yayınlanmaya hazırdır. Yayınlama işlemini gerçeklemek için yaşanacak gecikmeleri önlemek için çözüm yolu karşılaşılan problemlerde belirtilmiştir. Şifreleme işlemi için kullanılan kod ve anahtar yapısı ve örnek olarak anahtar kelimesi "Drone" olarak belirlenmiştir.

Kafka ortamında yayınlanan şifreli görüntü bir başka kaynaktan abone-ol işlemi gerçekleşerek ortamından çekilir. Bu projede local cihazda yayınlama ve abone-ol işlemleri test edilmiş ve kullanılmıştır. İki farklı cihazda kullanım için geliştirme adımlarına ihtiyaç bulunmaktadır. Sistemi abone-ol (consume) işlemine hazırlamak için yeniden Kafka Server'da bootstrap' a localhost 9092 portu ile bağlantı gerçekleştirilir. Abone ol işlemi ile sistemden çekilen şifreli görüntü alıcıya görüntülenebilir bir veri olarak iletilebilmesi için şifre çözme (decryption) işlemine geçilir. String verisi halinde şifrelenen veri iletildikten sonra şifre çözme işlemi ve yeniden boyutlandırma işlemi ile yeniden görsel verisi haline çevrilir. Kullanılan şifreleme kütüphanesi simetrik tabanlı AES algoritması olduğu için mimarinin yayınlama tarafında şifrelendiği anahtar ile abone-ol kısmında şifre çözme işlemi gerçekleşir.

Dahili kameradan alınan görüntünün yaklaşık dokuz yüz bin boyutlu olduğunu saptadık. Projemizde Kafka ile görüntüyü yayınlama işlemi yapılıp ardından consume edilen tarafta bu görüntünün ekrana verilerek üzerinden nesne tespiti yapıldığından her bir frame için gecikmeler yaşanıyor. Yüksek boyutlu bu veriyi tek seferde bir topiğe yayınlamaya çalıştığımızda görüntü alımı gerçek zamanlılıktan şaşıyor ve işlemler eş zamanlı yayınla/abone ol mantığını yürütemiyor. Bundan dolayı yayınlanacak veriyi aşağıda da belirtilen kodla altı parçaya bölerek produce işlemini yavaşlatıp abone olan tarafa zaman kazandırmış oluyoruz. Böylelikle işlemler gerçek zamanlılığa yaklaşarak gecikme beş altı saniyelere kadar indiriliyor.

5 Sonuçlar

Dronelardan alınan görsel verilerinin güvenliği sağlama noktasında araştırmalar sonucu AES algoritması günümüzde yaygın kullanıldığı ve brute force saldırılarına karşı dayanıklı olduğuna erişilmiş ve kullanımına karar verilmiştir. Kullanılan şifreleme algoritması yeniliğe ve güncellemelere açıktır. Şifreleme algoritmaları için kullanılan metrikler ile test denemeleri yapılabilir ve daha iyi bir şifreleme ile güvenlik sağlanabilir. Projenin endüstri için de yararlı olacağı noktada ise nesne tespiti ile proje zenginleştirilmiştir. Mevcut durumda YOLOv4-tiny kullanılarak az sayıdaki veri seti ile birçok nesne tespiti gerçekleşmektedir. Kullanılacak amaca yönelik kullanılan nesne tespiti algoritması ve makina öğrenmesi katkısıyla istenilen tespit gerçekleşebilir. Örnek olarak güvenliğin en önemli olduğu alanlardan biri olan askeriyede, alanına yönelik mühim bilgiler içeren bir veri seti ile bir nesne tespit algoritması eğitilerek dronedan alınan arazi görüntülerinde istenen verilerin hem güvenliği hem de tespiti gerçekleştirilebilir ve böylece savunma sanayisine

veya endüstriye katkı sağlanabilir. Çalışma zamanında iletilen veri ile nesne tespiti adımına kadar geçen sürede 5 saniyelik gecikme gerçekleşmektedir. Bu gecikmenin sebebi ise anlık alınan görüntünün uzun bir süreçten geçmesi ve şifreleme ve tespit algoritmalarının ard arda işleyişinden kaynaklanmaktadır.

References

[1] Austin, P.L.: Amazon Drone Delivery Was Supposed to Start By 2018. Here's What Happened Instead (2021). https://time.com/6093371/amazon-drone-delivery-service/

[2] Perekalin, A.: 11 milisaniyede Drone hacklemek (2017). https://www.kaspersky.com.tr/blog/drone-gone-in-11-ms/3128/

[3] Domin, K., Marin, E., Symeonidis, I.: Security analysis of the drone communication protocol: Fuzzing the mavlink protocol (2016)

[4] Corpas Rodríguez, B.: Publish/Subscribe Data Communication in Cyber-Physical Systems Oriented to Unmanned Aerial Vehicle, (2020)

[5] Bal, B., Erdem, T., SAYAR, A., KUL, S.: İnsansız Hava Araçları Için Görüntü Tabanlı Yer Belirleme Ve Yönlendirme, (2019)

[6] Krikor, L.Z., Baba, S.E.I., Arif, T., Shaaban, Z.: Image encryption using dct and stream cipher. (2009)

[7] Singh, P., Singh, K.: Image encryption and decryption using blowfish algorithm in matlab. (2013)

[8] Tang, L.: Methods for encrypting and decrypting mpeg video data efficiently. In: MULTIMEDIA '96 (1997)

[9] Ismail, I.A., Amin, M., Diab, H.: A digital image encryption algorithm based a composition of two chaotic logistic maps. Int. J. Netw. Secur. **11**, 1–10 (2010)

[10] Brindha, K., Sharma, R., Saini, S.: Use of symmetric algorithm for imageencryption. International Journal of Innovative Research in Computer and Communication Engineering **2**, 4401–4407 (2014)

[11] Zhang, Y.-Q., Wang, X.-y.: A new image encryption algorithm based on non-adjacent coupled map lattices. Appl. Soft Comput. **26**, 10–20 (2015)

[12] Ghode, P.S.: A keyless approach to lossless image encryption. (2014)

[13] Ceyhan, M., Yolaçan, E.N.: Görüntü dosyalarinin Şifrelenerek güvenli Şekilde saklanmasi. (2021)

[14] MAVLink Basics. https://ardupilot.org/dev/docs/mavlink-basics.html

[15] MAVLink Developer Guide. https://mavlink.io/en/