T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

MAKİNA ÖĞRENMESİLE BİYOMETRİK SAHTEKARLIĞA VE AĞ ANORMALLİK TESPİTİNE DAYALI SALDIRI TESPİTİ

DOKTORA TEZİ

Sajad EİNY

Enstitü Anabilim Dalı	**:**	**BİLGİSAYAR VE BİLİŞİM MÜHENDİSLİĞİ**
Tez Danışmanı	**:**	**Prof. Dr. Cemil ÖZ**

Haziran 2021

T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

MAKİNA ÖĞRENMESİLE BİYOMETRİK SAHTEKARLIĞA VE AĞ ANORMALLİK TESPİTİNE DAYALI SALDIRI TESPİTİ

DOKTORA TEZİ

Sajad EİNY

Enstitü Anabilim Dalı : BİLGİSAYAR VE BİLİŞİM MÜHENDİSLİĞİ

Bu tez 09/06/2021 tarihinde aşağıdaki jüri tarafından oybirliği/oyçokluğu ile kabul edilmiştir.

Jüri Başkanı	**Üye**	**Üye**
Üye		**Üye**

BEYAN

Tez içindeki tüm verilerin akademik kurallar çerçevesinde tarafımdan elde edildiğini, görsel ve yazılı tüm bilgi ve sonuçların akademik ve etik kurallara uygun şekilde sunulduğunu, kullanılan verilerde herhangi bir tahrifat yapılmadığını, başkalarının eserlerinden yararlanılması durumunda bilimsel normlara uygun olarak atıfta bulunulduğunu, tezde yer alan verilerin bu üniversite veya başka bir üniversitede herhangi bir tez çalışmasında kullanılmadığını beyan ederim.

Sajad EİNY
16/03/2021

TEŞEKKÜR

Doktora eğitimim boyunca değerli bilgi ve deneyimlerinden yararlandığım, her konuda bilgi ve desteğini almaktan çekinmediğim, araştırmanın planlanmasından yazılmasına kadar tüm aşamalarında yardımlarını esirgemeyen, teşvik eden, aynı titizlikte beni yönlendiren değerli danışman hocam Prof. Dr. Cemil ÖZ'e teşekkürlerimi sunarım.

İÇİNDEKİLER

SİMGELER VE KISALTMALAR LİSTESİ

CLNF	:Conditional Local Neural Fields
DBN	:Deep belief network
DMD	:Dynamic mode decomposition
FA	:Firefly Algorithm
IDS	:Intrusion detection system
IOT	:Internet of things
LBP	:Local Binary pattern
LDP-TOP	:Derivative Pattern from Three Orthogonal Planes
MAN Net	:Mobile Ad-Hoc network
MPOPSO	:Multiple Objective Particle Swarm Optimization
NIDS	:Network Intrusion detection system
RPCA	:Robust principal component analysis
SVM	:Support vector machine
VM	:Virtual machine

ŞEKİLLER LİSTESİ

TABLOLAR LİSTESİ

ÖZET

Anahtar kelimeler: izinsiz giriş tespiti, yüz sahtekarlığı tespiti, anormallik tespiti

Bu çalışmada, sistemlerde saldırı tespiti için dört farklı yeni yaklaşım önerdik. Bilgiye dayalı olarak her çevrimiçi platform farklı şekillerde saldırabilir. Bu projede, biyometrik sahtekarlık tespiti için derin öğrenme algoritmalarını kullandık. Ayrıca, DDOS gibi farklı saldırılar için, ağlarda anormallik tespitine dayalı yeni bir yaklaşım önerdik. bu durumda projemiz iki ana bölüme ayrılmaktadır:

Yüz sahteciliği algılama: Yüz sahtekarlığı saldırıları, izinsiz giriş tespit saldırılarından biridir. yüz sahteciliği tespiti için, iki farklı gruba ayırdığımız iki yeni uygulama önerdik. Birincisi, derin çok renkli özellik öğrenimi ile yüz sahtekarlığı tespiti için IoT-bulut tabanlı platforma önerdik. Ikinci olan, yüz sahtekarlığı tespiti için önerilen ikinci yöntem, Robust ana bileşen analizi ve derin inanç ağı yardımıyla hareket analizine dayanmaktadır.

Ağda izinsiz giriş ve anormallik algılama: Bu bölümde, ağ saldırı tespiti için iki farklı yöntemi inceledik ve önerdik. Üçüncüsü, Çok Amaçlı Parçacık Sürüsü Algoritmasına dayalı Özellik Seçimi ve Hızlı Öğrenme Ağının Kombinasyonunu önerdik. Bu teknikte, özellikleri seçmek, ağı eğitmek ve modeli test etmek için KDD Cup veri setini kullandık. Dördüncü ,hibrit Çıkarım Sistemleri Kullanan Ağ Güvenliği için Anormallik ve İmza Tabanlı IDS'yi önerdik.

INTRUSION DETECTION BASED ON BIOMETRIC SPOOFING AND NETWORK ANOMALY DETECTION WITH MACHINE LEARNING ALGORITHMS

SUMMARY

Keywords: intrusion detection, face spoofing detection, anomaly detection

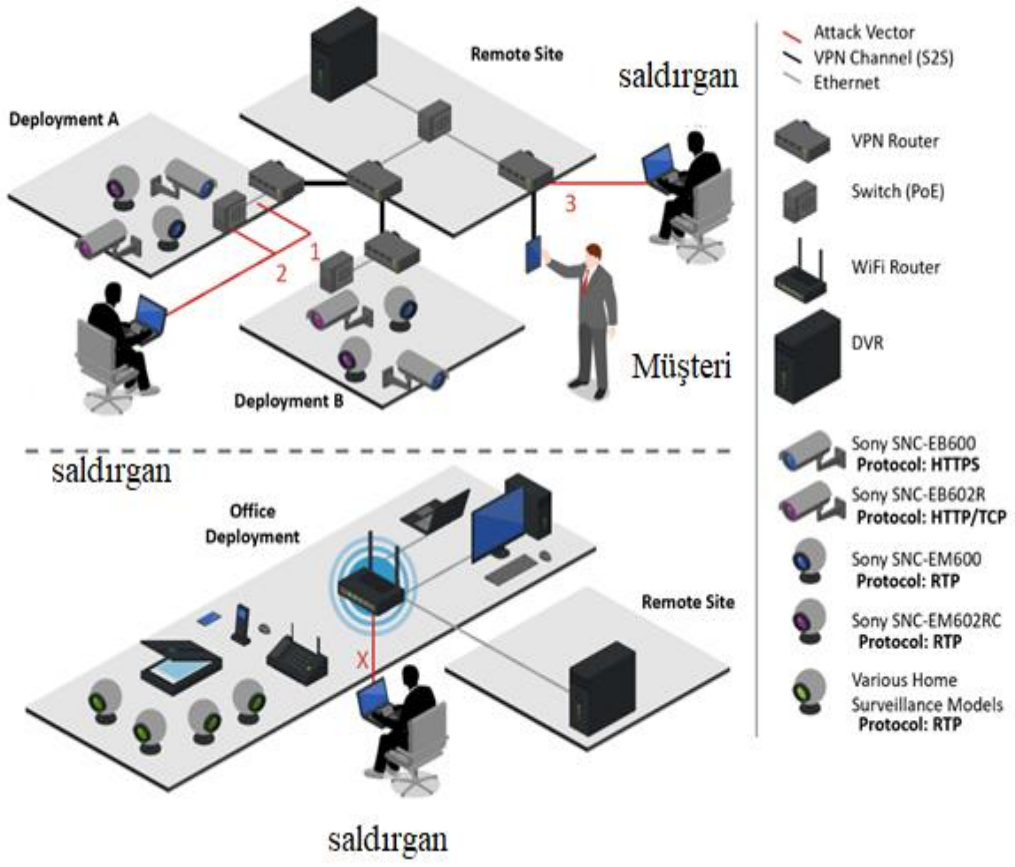
In this study, we proposed four different approaches for intrusion detection in systems. Based on the information, every online platform can attack in different ways. In this project, we used deep learning algorithms for biometric fraud detection. We also proposed a new approach based on anomaly detection in networks for different attacks such as DDOS. In this case, our project is divided into two main parts**:**

Face spoofing detection: Face spoofing attacks are one of the intrusion detection attacks. We have proposed two new applications for face spoofing detection, which we divided into two different groups. The first one, we proposed IoT-cloud based platform for face spoofing detection with deep multicolor feature learning. The second method suggested for face spoofing detection is based on motion analysis with the help of Robust principal component analysis and deep belief network.

Network intrusion and anomaly detection: In this section, we have reviewed and suggested two different methods for network attack detection. The third one, we proposed the Combination of Feature Selection and Fast Learning Network based on the Multipurpose Particle Swarm Algorithm. The forth one, We proposed Anomaly and Signature Based IDS for Network Security Using Hybrid Inference Systems.

BÖLÜM 1. GİRİŞ

Bu projede makine öğrenimi algoritmalarının yardımıyla bir güvenlik platformu tasarlıyoruz. bu platform, online sınav merkezleri gibi herhangi bir online kimlik doğrulama sisteminde kullanılabilir. Bu güvenli platform, biyometrik sahtekarlık ve izinsiz giriş saldırıları gibi farklı saldırı türlerini algılayabilir. Bir öğrencinin online sınava katılmak istediği senaryoyu varsayın. Bu öğrenci farklı saldırı türleri ile sisteme bağlanabilir. Birincisi, yüz sahteciliği saldırısı (Face spoofing attack). Bu saldırıda saldırganlar, kimlik doğrulama için kurbanın bir baskı yüzünü kameranın karşısına ayarlayarak sistemi atlarlar. Bu tür saldırılar biyometrik sahtekarlık saldırısıdır. Aynı şekilde iletişim sırasında saldırganlar, iletişimi atlamak için ağın farklı bölümlerine saldırılar olabilir. Şekil 1.1.'de, üç saldırgan VPN yönlendiricisinden ve SWITCH'ten sunucuya saldırmaya çalışıyor. Bu üç saldırgan, acktiv saldırıları grubundadır.



Şekil 1.1. İzleme ağındaki farklı saldırı türleri [1].

Bu saldırılar sırasında farklı IP kameralardan gelen bilgiler değiştirilebilir veya zarar görebilir. Kullanıcı biyometrik güvenlik kimlik doğrulamasını atlamak için yüz sahteciliği olarak da saldırabilir. bu durumda, her online platform için ağa zarar verebilecek farklı saldırı türleri mevcuttur ve bu projede farklı saldırı türlerini tartıştık ve bunlara çözüm önerdik. bu projenin ana katkısı:

Yüz sahteciliği tespiti için yeni bir derin öğrenme yaklaşımı sunduk izinsiz giriş tespiti için sinir ağına ve bulanık mantığa dayalı yeni yaklaşımı sunduk.

1.1. Yüz Sahteciliği Tespiti

Son yıllarda, yüz tanıma sistemine dayalı biyometrik kimlik doğrulama çok çeşitli uygulamalarda popüler hale gelmiştir. Yaygın yüz tanıma sistemleri, toplanan görüntüdeki yüzleri bir kameradan tanır, ancak canlı olup olmadığını algılayamaz. Bu

nedenle, yüz tanıma uygulamalarının bu yetersizliği, sistemi yüz sahtekârlığı saldırısına karşı savunmasız kılar [2]. Yüz sahtekârlığı saldırılarının dört farklı türü vardır: yüz baskısı, ekran görüntüsü, maske ve videoyu tekrar oynatma. Yüz tanıma sistemlerinin etkisi ve kimlik doğrulama için çeşitli tehditlerin varlığı nedeniyle, yüz sahtekârlığı önleme algoritmaları etkin noktalardan biri haline gelmiştir. Bu çalışmada, yüz sahteciliği tespitinde iki tür model tartışılmıştır: Önce duygu tanımaya dayalı yeni bir yöntem tasarlanıp uygulandı ve ardından nesnelerin interneti için hibrit derin öğrenme modellerine dayalı yeni bir yöntem sunuldu. Bu çalışmada, yüz sahteciliği tespitinde iki tür model tartışılmıştır. Önce hareket tanımaya dayalı yeni bir yöntem tasarlandı ve uygulandı daha sonra nesnelerin interneti için hibrit derin öğrenme modellerine dayalı yeni bir yöntem sunuldu. Bu durumda her bölüm ayrı ayrı tartışıldı.

1.1.1. Sağlam temel bileşen analizi (robust principal component analysis)

Biyometrik kimlik doğrulama sistemleri hayatımızda oldukça yaygındır, oysa farklı saldırılara karşı savunmasızdır. Bu bağlamda, bu tür sahtekarlıkları önlemek için geleneksel biyometrik uygulamalarla sağlam ve güvenilir yöntemler geliştirmek kaçınılmazdır. Biyometrik bilgilerin alınması sırasında kaçınılmaz eserler ele geçirilir. Bu artefaktlar, canlı videonun (geçerli erişim) veya tekrar videonun imzalarını ayırt etmek için kullanılabilir. Önerilen yaklaşım, derin öğrenme algoritmasına dayalı yüz saldırılarının tespiti için etkili bir yaklaşımdır. Bu makalede, veriye dayalı yöntemler olarak yeni derin inanç ağı (DBN) [3] ve Sağlam Temel Bileşen Analizi (RPCA) [4] boru hattı önerilmiştir. RPCA algoritması, dinamik değişikliklerin katkısını, her video karesindeki karmaşık arka plan, gölgeler ve ayrıntılar dahil olmak üzere tüm video olarak ayırır. DBN'lere dayalı RPCA ile çıkarılan özellikleri öğrenmek için, öncelikle DBN'ler, etiketlenmemiş görüntüler üzerinde denetimsiz bir ön eğitim sağlar ve daha sonra denetimli ince ayar, SoftMax katmanıyla sınıflandırma için etiketli özelliklerden yararlanır. Önerilen RPCA-DBN modelimiz hem hareket hem de doku analizi özellik kümelerini sınıflandırır. Önerilen yöntemle elde edilen sonuçlar, SIW ve Replay saldırısı olmak üzere iki genel erişim veritabanına dayanan son teknoloji algoritmalar tarafından elde edilen sonuçlardan daha etkilidir.

1.1.2. Derin çok renkli özellik öğrenme modeli ile yüz sahtekarlığı

Günümüzde Nesnelerin İnterneti (IOT), akıllı evden akıllı şehre kadar geniş bir teknoloji yelpazesinde insan yaşamını etkiliyor. Sağlık hizmetleri, güvenlik ve yönetim vb. Gibi farklı nedenlerle bilgi toplamak ve analiz etmek için çok sayıda IOT cihazı kullanılmaktadır. Araştırmacılar'in tahminine göre, veri depolamanın yaklaşık % 90'ı faydasız olacaktır [2]. Bu nedenle, araştırmacılar bulut bilişim için uygulama veya hizmet mimarisindeki uç aygıtları kullanmayı önerdiler. Veriler uç cihazlarda analiz edilebilir ve filtrelenebilir ve bulutta işlenmek üzere daha fazla iyileştirilmiş veri gönderilebilir. Örneğin, trafik izleme için konuşlandırılmış sensörler, düşük maliyetli ve düşük performanslı cihazlarla yangın tespiti için de kullanılabilir. Ancak IoT tabanlı sistemler, internetten gelen güvenlik tehdidi gibi farklı sorunlarla karşı karşıyadır. Örneğin, kan şekeri seviyesi ve kan basıncı gibi kritik bilgileri içeren IoT tabanlı bir sağlık hizmeti uygulamasını düşünelim. Kablosuz kanallar aracılığıyla veri iletişimi için kimlik doğrulama sistemi, kullanıcılerin kritik bilgilerinin korunması için güvence altına alınmalıdır. Kablosuz iletişimde bir kişinin kimliğini belirlemek için biyometrik kimlik doğrulama kullanılabilir. Bu kimlik doğrulama, konuşma, yüz, parmak izleri, avuç içi izi, yürüyüş ve iris gibi kişisel özniteliklerin kullanılmasını gerektirir [5]. Bu tür bir kimlik doğrulama, farklı sensörlerin yardımıyla toplanan istemcinin fiziksel yönü ile depolanan bir kopya arasındaki bir karşılaştırmaya dayanır. Danışanların fizyolojik bilgileri, bilgiye dayalı yöntemlere kıyaslamasi daha güvenilirdir çünkü bu bilgiler benzersizdir ve paylaşılamaz. Bu nedenle, istemcilerin kimlik doğrulaması için IoT tabanlı bulut bilişim sistemleri biyometri bilgilerini uygulamıştır.

Örneğin Kumari ve ark. [6], bulut çerçevesini kullanarak biyometrik kimlik doğrulamada bir özellik seçme tekniği önerdi. Başka bir benzer çalışmada, Shakil ve ark. [7] , buluttaki sağlık hizmeti verilerinin güvenliği için bir biyometrik kimlik doğrulama sistemi ve veri yönetimi uygulaması önerdi. Ayrıca Vidya ve ark. [8], bulut bilişim için entropi tabanlı yerel ikili model özelliği tanımlama tekniğine dayalı çok modlu bir biyometrik kimlik doğrulama sistemi önerdi. Ek olarak, Masud ve ark. [9] IoT ortamlarında yüz tanıma için Derin öğrenmeye dayalı bir yaklaşım önerdi. Yüz

tanıma sistemleri, cep telefonlarının ve dizüstü bilgisayarların kimlik doğrulama veya kayıt sistemleri gibi birçok uygulamaya çevrimiçi sınav merkezleri ve havalimanları gibi yerlerde önemli bir ilgi görmüştür [2]. Büyük Veri analitiği platformundaki bu tür güvenlik sistemleri, gerçek zamanlı uygulamalar için bir endişe konusudur. Bir kişinin kayıt için bir havaalanında tanınması veya bir öğrencinin çevrimiçi sınava katılması senaryosunu düşünün. Bu senaryolarda ve diğer benzer koşullarda kamera sürekli olarak yüzün görüntülerini yakalar ve bu verileri bulut ortamında işlenmek üzere gönderir. Yüz görüntüsünün anlamlı bilgilerine dayanarak, belirli bir kişi kolayca tanımlanabilir. Bununla birlikte, bu tür kimlik doğrulama ve kayıt sistemleri, farklı saldırı türlerine karşı savunmasızdır. Biyometrik kimlik doğrulama sistemlerinin güvenliğini artırmak için çeşitli yöntemler ve modeller önerilmiştir.

Örneğin Ali ve ark. [2], IoT tabanlı bulut ortamında biyometrik bilgilerin gizliliğini korumak için şifreleme yöntemini kullanan çok modlu biyometrik kimlik doğrulama sistemi önerdi. Başka bir çalışmada, Barrero ve ark. [5], şifreleme yöntemi ile çoklu biyometrik şablonun gizliliğini korumak için bir çerçeve önerdi. Ancak, yukarıda belirtilen yöntemler, kablosuz iletişimde aktiv saldırılarına dayalı koruma sağlamak için tasarlanmıştır. Literatürlere göre, IoT bulut ortamında yüz sahtekarlığı saldırısı henüz tartışılmamış ve çalışılmamıştır. Bu çalışmanın temel amacı, kullanıcının bilgilerini yüz sahteciliği saldırılarından korumak için bir IoT bulut tabanı çerçevesi sunmaktır. Yüz sahteciliği saldırısında davetsiz misafir, kurbanın sahte bir yüzünü göstererek kimlik doğrulama sistemini atlar. Bu tehdit nedeniyle, sağlam ve kararlı yüz Sunum Saldırı Algılama (PAD) yöntemleri geliştirilmeli ve tasarlanmalıdır. Yüz sahtekarlığı saldırıları dört ana grupta sınıflandırılabilir: yazdırma, görüntüleme, yeniden oynatma ve maskeleme saldırıları [10].

Bu tür saldırıların tespiti için sensör türlerine göre farklı algoritmalar önerilmektedir [11]. Genel olarak, Işık Alanı Kamera sensörleri, kızılötesi ve termal sensörler [11] veya çoklu biyometrik füzyon sistemleri [12] gibi diğer sensörlere kıyasla daha popülerdir çünkü bu ek ekipmanlar, kimlik doğrulama sistemlerinin maliyetini artırır. Bu durumda, birçok araştırmacı özellik tabanlı yöntemleri araştırır. Bu tür sahtekarlık algılama yöntemleri, gerçek kullanıcıyı sahte bir yüzden tanımak için ayırt edici

özellikler çıkarmaya çalışır. Örneğin, baskı, sergileme ve maske saldırılarında dudak hareketi, baş hareketi ve göz kırpma gibi yüz canlılığı özellikleri sahtekarlık saldırılarının tanınmasına yardımcı olabilir. Dahası, bu tür canlılık özellikleri içerdikleri için tekrar saldırılarının tespiti daha zordur [10]. Bazı durumlarda, davetsiz misafir, bir maskeden dudak ve göz bölgesini kırparak bir maske saldırısında canlılık özelliklerini uygular, bu da canlılık özelliklerinin tek başına sahtekarlık saldırılarını doğru şekilde tespit edemediğini gösterir. Yeniden oynatma ekranı ve basılı saldırı görüntüleri, bilgilerin bir kamera tarafından yeniden yakalanması nedeniyle bazı parazit ve kusurlar içerir. Bilginin yeniden yakalanması sırasında, sahte yüz, görüntülerin doku ve renk bilgilerinden etkilenerek yüksek frekanslı bilgileri kaybeder ve bu özellikler, gerçek bir kişiyi ve yeniden yakalanmış bir yüz görüntüsünü ayırt etmeye yardımcı olabilir. Özellikle saldırıların basılması ve gösterilmesinde, bilgilerin yeniden yakalanması sırasında, sahtekarlık yapan yüz görüntüsünde bazı kusurlar ve sesler ortaya çıkmaktadır. Bu eserler, gerçek biyometrik örneklere kıyasla yetersiz renk üretimine yol açar [13]. RGB, birçok cihazda renkli görüntüleri algılamak ve görüntülemek için yaygın olarak kullanılan renk alanıdır. Yine de, kırmızı, yeşil ve mavi renk bileşenleri arasındaki yüksek korelasyon ve parlaklık ve renklilik bilgilerinin eksik ayrılması nedeniyle görüntü analizindeki bu renk alanı yetersizdir [14]. Canlı ve sahte görüntülerin tespiti için cilt tonlarının canlılık ipuçlarıdır. Bu nedenle, farklı renk alanlarına dayalı görüntü doku analizi, yüz sahtekarlığı saldırıları [15] alanındaki araştırma alanlarının dikkatini çekmiştir. Derin öğrenme algoritmalarının bilgisayarla görme ve multimedya analizi alanındaki başarısı ile yüz sahtekarlığı problemlerinde derin doku analizine dayalı algoritmalar kullanılmıştır. Bununla birlikte, derin öğrenmeye dayalı yüz sahtekarlığı algılama algoritmaları, az sayıdaki sahtekarlık verisi ve derin bir ağı eğitmeyi zorlaştıran senaryo çeşitliliğinin olmaması gibi bazı sorunlarla karşı karşıyadır [16] [17]. Ek olarak, IoT tabanlı kimlik doğrulama sistemleri, gerçek zamanlı olarak depolama veya işleme gibi çeşitli zorluklarla karşılaştı .Bu sorunları çözmek için, IoT tabanlı bulut bilişim için farklı renk uzaylarında hibrit Evrişimli Sinir Ağı (CNN) modellerine dayalı yeni bir yaklaşım sunduk. Önerilen derin öğrenme yaklaşımı, yanıltıcı yüz görüntülerinin tanınmasında yararlı olan parlaklık ve renklilik bilgilerini çıkarmak için farklı renk uzayında önceden eğitilmiş üç model kullandı. Tek bir görüntüden elde edilen sağlam ve ayırt

edici özellikler sayesinde, önerilen bu model daha az eğitim veri setiyle tatmin edici sonuçlar elde edebilir. Önerilen yaklaşımın bu avantajı, bulut bilişim sistemlerinin temel sorunlarından birini ele alan bulut bilişimde eğitim verilerinin depolanmasını azaltmaya yardımcı olur. Önerilen yaklaşımımızın son teknoloji yöntemlerle karşılaştırılması için önceden tanımlanmış değerlendirme protokollerine sahip iki zorlu kamu erişim sahtekarlığı veritabanına dayalı olarak kapsamlı deneysel analiz gerçekleştirildi. Bu deneysel sonuçlar, önerilen yaklaşımımızın, kıyaslama veritabanlarına dayalı son teknoloji yöntemler arasında mevcut tüm derin tabanlı yöntemlerden daha iyi performans gösterdiğini göstermektedir. ana katkıları aşağıdaki gibidir:

Yüz sahtekarlığı tespiti için bir IoT güvenlik çerçevesi önerme.
Yeni bir derin öğrenme yaklaşımı sunmak ve modeli iki kamu veri tabanında değerlendirmek.

1.2. İzinsiz Giriş Tespiti

İzinsiz Giriş Tespit Sistemi (IDS), başlangıçta bir hedef uygulama veya bilgisayara yönelik güvenlik açığı istismarlarını tespit etmek için oluşturulmuş bir ağ güvenlik teknolojisidir. Saldırı Önleme Sistemleri (IPS), tehditleri tespit etmenin yanı sıra engelleme yeteneği de ekleyerek IDS çözümlerini genişletti ve IDS / IPS teknolojileri için baskın dağıtım seçeneği haline geldi. Bu makale, IDS dağıtımını tanımlayan yapılandırma ve işlevler hakkında ayrıntılı bilgi verecektir. Bir IDS'nin yalnızca tehditleri algılaması gerekir ve bu nedenle ağ altyapısına bant dışı yerleştirilir; bu, bilginin gönderen ve alıcısı arasındaki gerçek zamanlı iletişim yolunda olmadığı anlamına gelir. Daha ziyade, IDS çözümleri satır içi trafik akışının bir kopyasını analiz etmek için genellikle bir TAP veya SPAN bağlantı noktasından yararlanır (ve böylece IDS'nin satır içi ağ performansını etkilememesini sağlar). IDS başlangıçta bu şekilde geliştirildi, çünkü o zamanlar saldırı tespiti için gereken analiz derinliği, ağ altyapısının doğrudan iletişim yolundaki bileşenlere ayak uydurabilecek bir hızda gerçekleştirilemiyordu. Açıklandığı gibi, IDS aynı zamanda yalnızca dinlenen bir cihazdır. IDS, trafiği izler ve sonuçlarını bir yöneticiye bildirir, ancak tespit edilen bir

istismarın sistemi ele geçirmesini önlemek için otomatik olarak eylemde bulunamaz. Saldırganlar, ağa girdikten sonra güvenlik açıklarından çok hızlı bir şekilde yararlanma yeteneğine sahiptir, bu da IDS'yi önleme cihazı için yetersiz bir dağıtım haline getirir. Saldırı tespiti tartıştığımız ana sorunlardan biridir ve bu çalışma alanı için iki farklı yaklaşım önerdik.

1.2.1. Çok amaçlı parçacık sürüsü algoritmasına dayalı özellik seçimi ve hızlı öğrenme ağının kombinasyonuna dayalı ağ izinsiz giriş tespit sistemi

Kablosuz ağların büyümesi ve iletişim ağlarının, özellikle mobil ad hoc ağların (MANET'ler) avantajlarının ve uygulamalarının artması göz önüne alındığında, bu tür ağlar, kullanıcıların ve araştırmacıların ilgisini eskisinden daha fazla çekmiştir. Geleneksel iletişim altyapılarına dayalı ihtiyaçları ortadan kaldıran bu tür ağların çeşitli ağ türlerinde ve ortamlarda üretkenliği, bu ağların çeşitli alanlarda kullanılmasının ana nedenlerinden biridir. Öte yandan, bu ağların artan popülaritesi, en önemlilerinden biri ağ güvenliği olan birçok zorluğa yol açmıştır. Bu bağlamda, MANET'lerde düzenleyici ve güvenlik altyapısının eksikliği, ağdaki izinsiz girişlerin en önemli sorunlardan biri olarak kabul edildiği veri gönderme ve alma konusunda bazı sorunlara neden olmuştur. MANET'lerde kablosuz notlar, kaynak ve hedef düğümler arasında bir bağlantı görevi görür ve ağdaki rölelerin ve yönlendiricilerin rolünü oynar. Bu nedenle, kötü niyetli düğüm penetrasyonu ve bilgi paketlerinin imhası mümkün hale gelir. Günümüzde saldırı tespit sistemleri (IDS'ler), kablosuz sensör ağlarında bulunan düğümlerin performans ve davranışlarının uzaktan izlenmesi yoluyla sorunun üstesinden gelmek için bir çözüm olarak kullanılmaktadır. Ağdaki kötü niyetli düğümleri tespit etmenin yanı sıra, IDS'ler çoğu durumda gelecekte kötü niyetli düğümlerin davranışını tahmin edebilir. Bu nedenle, bu çalışma, çok amaçlı parçacık sürüsü optimizasyon algoritması (MOPSO) [18] tabanlı özellik alt küme seçimi (FSS) ve hızlı öğrenme ağı (FLN) kombinasyonunu kullanarak MOPSO-FLN adlı bir ağ IDS (NIDS) tanıttı. Bu teknikte, özellikleri seçmek, ağı eğitmek ve modeli test etmek için KDD Cup veri setini kullandık. Simülasyon sonuçlarına göre, bu yöntem, temsili özelliklerin sayısının hedefleri ile evrimsel güce dayalı eğitim hataları

arasında bir denge oluşturarak, IDS'nin diğer önceki yöntemlere göre değerlendirme kriterleri açısından performansını iyileştirebilmiştir. MOPSO.

Mobil ad hoc ağlar (MANET'ler), herhangi bir kablosuz bağlantılar üzerinden iletişim kuran bir grup mobil düğümdür. MANET'lerin merkezi kontrol mekanizması yoktur ve her mobil düğüm, ağda bir terminal olmanın yanı sıra ağın diğer belirli düğümlerine veri paketlerini aktarmak için yönlendiriciler olarak işlev görür . Dinamik bir topolojiye ve ağa herhangi bir zamanda kolayca girip çıkabilen ve ağdaki veri akışına erişebilen düğümlere sahip olması nedeniyle güvenlik MANETS'de en önemli sorundur. Ek olarak, birkaç mobil düğüm, hesaplama gücü ve enerji kaynağı [19] [20] açısından kaynaklarla sınırlıdır. Bu nedenle, sınırlı kaynaklar nedeniyle ağda kalıcı güvenlik izleme düğümlerinin varlığı neredeyse imkansızdır ve MANET'te [21] ağdaki düğümlerin davranışının uzaktan kontrolüne ve güvenlik gereksinimlerinin belirlenmesine ihtiyaç vardır.

Ağ saldırı tespit sistemleri (NIDS), düğüm etkinliğini veya ağ trafiği etkinliğini izlemek için kullanılır. NIDS'lerin ana amacı, kötü niyetli düğümleri tespit etmek ve ağda gelecekteki olası saldırıları tahmin etmektir [22]. Ağda kötü niyetli bir düğüm tespit edilirken daha fazla eylem için bir uyarı oluşturulur. NIDS tarafından saldırıları tespit etmek için çeşitli teknikler önerilmiştir ve bir IDS'nin başarısının bu konuda kullanılan tekniğin türüne bağlı olması dikkate değerdir [23]. NIDS performansındaki anahtar faktörlerden biri, ana veri setinden [24] temsili özelliklerin seçilmesidir. Veri setinde bulunan özelliklerin sayısını (örneğin, düğümlerin davranışı ve ağ trafiği), sınıflandırma hassasiyetini etkilemeden azaltmak, IDS performans optimizasyonunda önemli bir rol oynayabilir [25].

Önerilen yöntemde, MOPSO'ya (çok amaçlı partikül sürüsü optimizasyonu) dayalı özellik seçimi yaklaşımı, ana veri setinin temsili özelliklerinin seçilmesinden sorumludur. Seçilen özellikler, çözüm olarak bir hızlı öğrenme ağına (FLN) girilir. FLN, hızlı eğitimi kullanarak çözümleri değerlendirir ve seçilen özelliklere göre modelin hatasını belirler. Bu çalışmanın temel amacı, modelin veri boyutunu ve karmaşıklığını azaltmak için ilgisiz özellikleri, nitelikleri ve eklentileri ortadan

kaldırırken, kötü niyetli düğümlerin ve ağ saldırılarının modelini daha yüksek bir hızda belirlemede sınıflandırma doğruluğunu arttırmaktı. Bu nedenle, önerilen yöntem, önemli özellikleri belirlemek için MOPSO'ya dayalı özellik seçimi yaklaşımını içeriyordu.

Bu teknikte, özellikler, çok amaçlı bir parçacık sürüsü optimizasyon algoritmasının (PSO) birincil parçacıkları olarak kabul edilir. Ayrıca, önerilen yöntemde kullanılan özellik sayısını ve sınıf hatasını en aza indirmek için hedef işlev uygulanır. Ayrıca, birincil parçacıklar, veritabanındaki tüm özelliklerin bir alt kümesi olarak seçilir. Parçacıklar, fit fonksiyonunun değerini tahmin etmek için bir çözüm olarak MOPSO'da FLN'ye gönderilir. MOPSO algoritmasının her tekrarında en küçük fonksiyon değerine sahip partiküller, uzman partiküller ve bu turdaki optimal çözümler olarak seçilir ve solüsyonlar havuzunda saklanır. Sonraki turda, diğer parçacıkların konumu ve hızı uzman parçacıklara olan eğilim doğrultusunda güncellenir. Algoritmanın sonunda, çözüm havuzunda depolanan uzman parçacıklar, fit fonksiyonunun değerine göre sıralanır ve optimum çözüm olarak en küçük değere sahip bir çözüm seçilir. Dahası, optimal çözümün belirlediği özellikler, kötü niyetli düğümlerin davranış kalıbı olarak belirlenir ve ağdaki gelecekteki kötü niyetli düğümleri tahmin etmek için kullanılır.

1.2.2. Hibrit çıkarım sistemleri kullanan ağ güvenliği için anormallik ve imza tabanlı IDS

Günümüz dünyasında iletişimin yaygınlaşması ve mesafe boyutu ne olursa olsun iletişim ağları aracılığıyla insanlar arasında etkileşim yaratma imkanı ile birlikte, alışverişi yapılan veri ve bilgi için güvenlik oluşturma konusu araştırmacılar tarafından büyük ilgi gördü. Bu amaçla çeşitli yöntemler önerilmiştir, en önemli yöntemlerden biri, ağa izinsiz girişleri hızlı bir şekilde tespit etmek ve yöneticiyi veya sorumlu kişileri bu davetsiz misafirlerin neden olduğu hasar miktarını azaltmak için bir operasyon seti gerçekleştirmeleri için bilgilendirmek için saldırı tespit sistemleridir. .Önerilen saldırı tespit sistemlerinin temel zorluğu, üretilen hatalı uyarı mesajlarının sayısı ve bunlardaki izinsiz girişlerin doğru tespitinin düşük yüzdesidir. Bu araştırmada

Suricata IDS / IPS, meta-sezgisellerin hedeflenen ağdaki kötü amaçlı trafiği manuel olarak algılaması için NN modeliyle birlikte konuşlandırılmıştır. Metaheuristics dayalı özellik seçimi için sinir ağı ve anormallik tabanlı tespit için, bu araştırma makalesinde bulanık mantık kullanılmıştır. Kali Linux 2020.3'ün en son kararlı sürümü, web uygulamaları ve farklı işletim sistemleri için bir saldırı sistemi olarak kullanılır. %96.111'e ulaşılmıştır.

Saldırı tespit sistemleri, izinsiz girişleri iki şekilde algılayabilir:

- İmza tanıma: Ağlarda yetkili kullanıcılar ve bilgisayar korsanları tarafından gerçekleştirilen işlem ve işlemlerin geçmişine ilişkin veriler kullanılarak normal davranış ve anormal davranış kalıpları oluşturulur. Bu kalıpları veya imzaları mevcut kullanıcıların davranış kalıplarıyla eşleştirerek, yetkili kullanıcılardan yetkisiz kullanıcıları veya bilgisayar korsanlarını belirlemek mümkündür. Bu yöntemin en önemli dezavantajı, eğer kullanıcının imzası veya kalıbı yeniyse ve daha önce veritabanında benzer kalıp veya imza yoksa yetkili veya yetkisiz kullanıcı olup olmadığını belirleyemiyoruz.
- Anormallikleri tanımlayın: Makine öğrenme yöntemlerinden (sinir ağları, SVM, vb.) Ağdaki davranışlarına göre (oluşturulan trafik miktarı, paylaşılan veya indirilen dosyaların içeriği gibi) bir kullanıcı sınıflandırması oluşturmak için, Ağ kullanım süresi vb.). Sistemin eğitildiği sisteme göre kullanıcıları tanımlamak ve sınıflandırmak için normal ve anormal olmak üzere iki sınıf oluşturulur. Bu yöntemin avantajlarından biri, sisteme sızan hackerları yeni yöntemlerle tespit etmenin mümkün olmasıdır.

Saldırı tespit sistemlerinde gerçekleştirilen tüm süreç iki ana bölüme ayrılabilir. Bu parçalar:

- Kaydedilen ve toplanan veri kümesinde yer alan tüm özelliklerden belirli özellikleri seçin: Çünkü, kullanıcıların davranışları ve farklı ağlarla etkileşimleri hakkında toplanan veri kümesi farklı türde özellikler içerebilir ve bu nedenle, kalıpları tanımlamak veya performans için bu Özelliklerin tümünü

kullanmak Analizler zaman alıcıdır ve saldırganların ve sıradan kullanıcıların kalıplarını tespit etmek için farklı tekniklerin uygulanmasını karmaşık hale getirebilir veya kafa karıştırabilir, böylece hackerların farklı ağlardaki anormal davranışlarının tespitini hızlandırmak için seçim tekniklerini kullanarak, tümün bir alt kümesi toplanan özellikler seti oluşturulacaktır. Bu konuda kullanışlı ve etkili özellikler seçiyoruz. Başka bir deyişle, özellik seçiminde, mevcut veri kümelerindeki toplam özelliklerden bir alt küme seçeriz ve bu alt küme, bu verileri analiz etmek ve normal ve anormal davranışları belirlemek için gereken süreyi azaltmaya yardımcı olabilir, ancak aynı zamanda bu verilerin karmaşıklığını da büyük ölçüde azaltabilir. .

- Normal kullanıcıları saldırganlardan ayırmak için iki teknik (sınıflandırma ve anormallik algılama dahil) kullanma: Tüm ağ kullanıcıları genel olarak iki gruba ayrılabilir (normal kullanıcılar ve saldırganlar). Bu nedenle, sınıfların türü ve sayısı bilindiğinden, ağ ortamındaki her bir kullanıcının sınıf türünü farklı sınıflandırma teknikleri (SVM, Karar Ağacı vb.) Kullanarak belirlemek ve son olarak tanımlamak için kalıplar oluşturmak mümkündür.

BÖLÜM 2. KAYNAK ARAŞTIRMASI

2.1. Yüz Sahteciliği Algılama ile İlgili Çalışmalar

Farklı canlılık ipuçlarına dayanarak, çeşitli tespit yöntemleri önerilmiştir. Bu yöntemlerin sınıflandırılması temel olarak dört farklı grupta durmaktadır: doku analizi, hareket analizi, görüntü kalitesi analizi ve donanıma dayalı yöntemler.

Yazdırılan bir görüntü veya aygıttan bilgi alınırken bazı hatalar meydana gelir. Bu hatalar, kimlik doğrulama için çekilen görüntünün veya videonun dokusunu etkiler. Bu tür algoritmalar, parodi deseninin dokusunun ve geçerli erişimin bir analizini yapmaya çalışır. J. Määttä ve diğ. [26], bir yüz görüntüsünün dokusunu analiz etmek için çok ölçekli lokal ikili (MLBP) örüntülere dayanan bir yöntem önermiştir. Ayrıca, Z. Boulkenafet ve ark. [27] parlaklık ve renklilik kanallarından renk bazlı bir yerel ikili model (LBP) önerdi. Ek olarak, I. Chingovska ve ark. [28] LBP ve potansiyel özellikleri bulmak için varyasyonlarına dayanan bir doku özellik tanımlayıcısı sunarken, başka bir çalışmada canlılık ipuçlarının tespiti için farklı renk kanallarında yedi farklı özellik tanımlayıcısı önerilmiştir [13]. S. Phan ve ark. [29] dokuyu analiz etmek için Üç Dik Düzlemden (LDP-TOP) yüksek dereceli bir Yerel Türev Kalıbı önerdi. Tüm geleneksel özellik tanımlayıcı yöntemlerin yanı sıra, günümüzde çalışmalar derin özelliklerin analizine odaklanmaktadır. L. Li ve diğ. [30] evrişimsel bir sinir ağı (CNN) yardımıyla canlı ipuçlarının çıkarılması için derin kısmi özellikleri tanımladı. G.B. Souza ve diğ. [31], LBP ve modifiye edilmiş bir evrişimli sinir ağı yardımıyla derin bir doku özellikli çıkarıcı önerdi. Z. Xu ve ark. [32] CNN'li Uzun Kısa Süreli Bellek (LSTM) birimlerinden oluşan derin bir mimari bildirmiştir.

Kalite analiz yöntemleri; Basılı görüntülerden veya görüntüleme cihazlarından biyometrik bilgilerin yeniden alınması nedeniyle kaydedilen verilerin kalitesi düşer ve

bazı durumlarda video veya görüntü parazit veya bulanıklaştırma içerir. Bazı yöntemler kaliteden yararlandı ve kimlik sahtekarlığı tespiti için kullandı. Örneğin, Z. Zhang ve ark. [33] düşük, ortalama ve yüksek kalite olmak üzere üç farklı kalite kategorisi önermiş ve canlı ipuçlarını keşfetmek için yüz bölgesindeki yüksek frekanslı bilgileri araştırmıştır. X. Tan ve ark. [34] seyrek düşük sıralı bilinear ayrımcı modeliyle tekil görüntülere dayalı bir çevrimiçi yöntem önerdi. H. Li ve ark. [35] önceden bilgi içeren kümeler ve çoklu kalite güdümlü sınıflandırıcılar temelinde önerilen eğitim. Bu yöntemde, her küme çıkarılan görüntü kalitesi değerlendirme özelliğini içerir.

Hareket analizi yöntemleri; Doku analizi ve kalite analizinin yanı sıra, özellikle basılı ve görüntülü görüntü saldırıları için kimlik sahtekarlığı saldırılarının özelliklerinin saptanmasında mükemmel bir performans gösterir. T. Edmunds ve diğ. [36], video ve maske saldırılarını ayırt etmek için katı ve katı olmayan istismarlar için yüz hareketlerini analiz eden Koşullu Yerel Nöral Alanlar (CLNF) tabanlı bir yöntem önermiştir. Anjos ve ark. [37] yüz hareketleri ve arkaplan arasındaki korelasyonları araştırdı. S.T. Phan [38], yüz hareketinin çıkarılması için LDP-TOP özellik tanımlayıcı algoritmaları önermiştir. G. Zhao [39], Birim Yerel İkili Kalıplara (VLBP) dayalı dinamik bir doku tanıma yöntemi önermiştir. W. Bao ve ark. [40] iki ve üç boyutlu görüntülerde iki alan arasındaki derecelerin farkına dayanan optik akış alanlarının yardımıyla bir yöntem önerdi.

Donanım tabanlı analiz yöntemleri ; Donanım tabanlı analiz aynı zamanda bilgi alırken farklı cihazlarla biyometrik görüntüleri değerlendiren sağlam kimlik sahtekarlığı tanıma yöntemlerinden biridir. Örneğin, N. Erdogmus ve ark. [41] Kinect tarafından yakalanan renk ve derinlik bilgisini kullanarak LBP tabanlı yöntemler önerdi. I. Pavlidis ve diğ. [42], yakın kızılötesi kamera yardımıyla çift bantlı füzyon donanım sistemlerini sundular ve standart bir kameraya kıyasla daha iyi sonuçlar elde etmek için teorik ve deneysel analizden faydalandılar. Z. Zhang ve ark. [43] Lambertian modelini kullanarak çokbantlı bir kimlik sahtekarlığı saptama yöntemi önerdi. Ayrıca, bu sistemde, sahte bir yüzü gerçek olandan ayırt etmek için cildin multispektral özelliklerini analiz ettiler.

Bu kategorilerin yanı sıra, bazı yöntemler daha güçlü ve doğru algoritmalar tasarlamak için farklı grupların avantajlarını sağlamıştır. Karşılık gelen çoklu işaret tabanlı yöntemlerin farklı perspektiflerden kombinasyonu çok sayıda alt problemi çözebilir. Örneğin, Feng ve ark. [44] görüntü kalitesi ve hareket işareti analizinin bir kombinasyonunu içeren bir çerçeve önerdi. Bu çerçevede, hareket temelli özellikleri elde etmek için Yoğun Optik Akış kullanılmıştır ve kalite analizi için Shearlet tabanlı görüntü kalitesi özellikleri kullanılmıştır. T.F. Pereira [45], özellik çıkarıcı ve yerel dinamik mikro doku yüz hareketleri için LBP-TOP içeren 3D-LBP tabanlı yöntemleri önerdi. J. Komulainen ve diğ. [46] hareket ve doku tabanlı yöntemler içeren füzyon modellerini önermişlerdir. Hibrit sistemlerinde, her bir müşteri karesinin korelasyon matrisini ve arka plan sahnelerini ölçmek için basit hareket analizi kullandılar. S. Tirunagari ve ark. [47] hareket analizi için bir dinamik mod ayrıştırma (DMD) algoritması tarif etmiş ve bu bilgiler bir LBP özellik çıkarıcısı ile açıklanmıştır. Bu çalışmada, çoklu işaret temelli makaleler gözden geçirilmiş ve önerilen yaklaşım Tablo 2.1.'de gösterilmiştir. Önerilen yaklaşımımız RPCA algoritması ile hareketi analiz etmiş ve bu özellikleri ayrıntılı olarak sunulan bir DBN mimarisinin yardımıyla çıkarmış ve ayarlamıştır.

Tablo 2.1. Çoklu işaret tabanlı yöntemlerin sınıflandırılması

Önerilen algoritma	Doku analizi	Hareket analizi	Kalite analizi
Feng et al. [44]	-	Dense Optical Flow	Shearlet-based features
T.F. Pereira [45]	LBP	Dynamic micro-texture	-
J. Komulainen [46]	LBP	Motion correlation matrix	-
S. Tirunagari [47]	LBP	DMD	-
Önerilen yaklaşımımız	DBN	RPCA	-

2.2. İzinsiz Giriş Tespit Literatür Araştırması

Yazarlar tarafından, IDS sistemleri tarafından saldırı tespitinin doğruluğunu artırmak için önerilen teknikler veya yöntemler hakkında çeşitli araştırmalar yapılmıştır. Ayrıca, birçok yazar, IDS sistemlerinde kesinliği artırmak için özellik seçim yöntemlerini kullanmıştır. Bu çalışmada, bu araştırmaların bazı hedeflerini ve sonuçlarını gözden geçireceğiz.

Farha Haneef, Shailendra Singh, [48] Özellik seçimi üzerine çalıştılar. Meta-sezgisel optimizasyon kavramını kullanarak akıllı bir hibrit teknik önerdiler. Önerilen teknik, verilerden sık kullanılan özellikleri seçmek için IWD ve ACO'yu birleştirir. Bu makalenin temel amacı, eğitim süresini kısaltmaya ve optimum özellik alt kümesi oluşturmaya odaklanmaktır. Başka bir deyişle, bu yazarlar mevcut verilerden özellik seçimi sürecini optimize etmeye çalıştılar. Son olarak, bu yazarlar, KDD CUP'99 verilerinden özellik seçimi için önerdikleri tekniği uyguladılar ve sonuçlar, önerdikleri tekniğin amacına ulaştığını gösterdi.

Azam Davahli & Abaei, [49] SVM tabanlı LIDS geliştirmek için GA kavramlarını ve GWO'nun matematiksel denklemlerini kullanan yeni bir model önerdiler. Bu yeni modelin adı GABGWO. İki yeni çaprazlama ve mutasyon operatörü uygulayarak LIDS performansını artırmaya yönelik yeni model, en alakalı trafik özelliklerini bulmaya ve ilgisiz olanları ortadan kaldırmaya çalışıyor. GABGWO'nun performansı değerlendirildi ve sonuçlar, bu modeli kullanarak optimum trafiği seçebileceğimizi, hesaplama maliyetini azaltabileceğimizi ve LIDS için yüksek doğruluk elde edebileceğimizi gösteriyor. Ayrıca sonuçlar, GA ve GWO bileşiminin diğer yeni yöntemlere ve mevcut FS algoritmalarına kıyasla daha iyi performansa sahip olduğunu göstermektedir.

Al-Yaseen [50], Yeni bir sarmalayıcı özelliği seçim yöntemi önermek için Destek Vektör Makinesi (SVM) ve ateş böceği algoritması (FA) kullanıldı. Bu araştırmanın amacı, verilerin boyutunu küçültmek ve sınıflandırma süresini azaltmak için ilgisiz ve tekrar eden özellikleri kaldırmak ve son olarak IDS'nin performansını iyileştirmekti. FA, çeşitli kombinasyon problemlerinde uygulanamaz ve bu araştırma, özellik alt kümelerini üretmek için kullanılmıştır. Bu özellik alt kümelerini değerlendirmek için SVM modeli kullanıldı. Önerilen yöntemin temel avantajı, FA'nın bir optimal özellik alt kümesi üretme yeteneğini geliştirmektir. Bu yazarlar, önerilen yöntemlerinin değerlendirilmesi için NSL-KDD veri setini kullandılar. Deneysel sonuçlar, önerilen yöntemin IDS'nin% 78.89 genel doğruluğuna sahip olduğunu gösterdi. Ayrıca, bu sonuçlar, önerilen yöntemin (FA-SVM) özelliklerin sayısını azaltabileceğini ve aynı

zamanda davetsiz misafirleri tanımlamanın doğruluğunu artırabileceğini ve yanlış alarm oranlarının sayısını azaltabileceğini gösterdi.

Hadeel Alazzam, [51] Yeni bir sarmalayıcı seçim algoritması ve IDS için sürekli bir güvercin optimize ediciyi ikileştirmek için yeni bir yöntem önerdi. Yeni algoritma, güvercinden ilham alan optimize ediciyi kullanarak seçim sürecini kullanmayı amaçlamaktadır. Bu yazar, yeni yöntemi, sürekli sürü akıllı algoritmalarını ikileştirmeye yönelik geleneksel yöntemlerle karşılaştırdı. Bu araştırmada, kosinüs benzerliğinin kullanımına dayanan yeni bir ayrıklaştırma yöntemi, sürekli bir algoritma önerilmiştir. Önerilen bu algoritmayı değerlendirmek için, bu yazarlar UNSW-NB15, NLS-KDD ve KDDCUP 99 dahil olmak üzere üç popüler veri setini kullandılar. Sonuçlar, önerilen algoritmanın IDS oluşturmak için gereken özelliklerin sayısını başarıyla azaltabildiğini ve yüksek TRP'ye sahip olduğunu gösterdi. , FPR ve doğruluk ve F-Puanı. Dahası, önerilen algoritma karar oluşturma için gereken süreyi kısalttı.

Yukang LIU [52] ,MH_SFS adı verilen yeni bir özellik seçme algoritması önerdi. Bu algoritmanın temel amacı, anormallik tespit yöntemlerinin boyutunu azaltmaktır. Önerilen algoritma, SFS özellik seçme algoritmasının performansını artırabilir. Meta-sezgisel arama sürecine ek olarak hesaplama maliyetini düşürmek için bu yazar bir filtre seçme işlevi ekler. Önerilen algoritmalarını test etmek için KDD Cup 99 veri kümesini kullandılar. Onlarınki, önerilen bu algoritmanın performansını geleneksel SFS ve IFFS algoritması ile üç anormallik algılama modeli üzerinden karşılaştırdı. Sonuçlar, bu yazarlar tarafından önerilen algoritmanın yüksek performansa sahip olduğunu ve diğer algoritmalarla karşılaştırıldığında daha az sayıda özelliğin seçildiğini gösterdi.

Laura Calvet [53], Diğer araştırmacılar tarafından makine öğrenimi yöntemlerinin metasezgisellikle birleştirilmesi ile ilgili yapılan araştırmaları inceledi. Sezgisel öğrenme kavramının yardımıyla yeni bir tür hibrit algoritma önerdiler. Sezgisel tarama, kombinatoryal optimizasyon problemlerini çözmek için dinamik girdileri (COPDI'ler) kullanma girişimlerini öğrenin. Genellikle, bu COPDI'larda, sorun

girdileri sabit değildir, ayrıca tahmin edilebilir şekilde değişir. Bu nedenle çözüm, bazı sezgisel tabanlı yinelemeli işlemlere göre yapılır. Bu yazarlar, meta sezgisel algoritma ile öğrenme mekanizması arasındaki koordinasyonun, girdideki farklılıklar nedeniyle ortaya çıkan problemleri çözmek için gerekli olabileceğini söylediler. Önerilen yeni hibrit algoritma türlerini test etmenin sonuçları, öğrenme yöntemleri yinelemesinin, meta-sezgisel tarafından kullanılan girdi modellerini güncellediğini gösterdi.

Kuan-Cheng Lin, [54] Çeşitli IoT uygulamalarından oluşturulan büyük verileri inceledi. Sınıflandırma yöntemlerini uygulamak için bu büyük verilerden en uygun özellikleri alt kümesini bulmak için meta-sezgisel bir arama algoritmasına ihtiyacımız olduğunu söylediler. CSO'nun değiştirilmiş bir versiyonunu önerdiler ve MCSO adını verdiler. Önerilen algoritmanın temel amacı, problem alanı içinde arama verimliliğini artırmaktır. Deneysel sonuçlar, UCI veri kümelerindeki alt özelliklerde azalan sayıda özelliğe sahip MCSO'nun, orijinal CSO'ya kıyasla sınıflandırma doğruluğunu iyileştirdiğini göstermektedir. Ayrıca, MCSO eğitim süresini uzatır ve orijinal STK'ya kıyasla daha yüksek doğruluğa sahiptir. Bu nedenle, MCSO gerçek zamanlı IoT uygulamalarına uygulanabilir.

Yuyang Zhou [55], özellik seçimi ve topluluk öğrenme tekniklerine dayanan yeni bir IDS çerçevesi önerdi. Optimal bir özellik alt kümesini seçmek için, CFS-BA adı verilen sezgisel bir algoritma önerdiler. Bu algoritma, özelliklerin optimum alt kümesini seçmek için özellikler arasındaki korelasyonu kullanır. Ayrıca Forest, RF ve C4.5'i Forest PA algoritmaları ile birleştirdiler. Temel öğrenicilerin saldırı tespiti için olasılık dağılımını birleştirmek için, bu yazarlar oylama teknikleri kullanıldı. Algoritmalarını 3 farklı IDS veri kümesinin (CIC-IDS 2017, AWID ve NSL-KDD veri kümeleri dahil) yardımıyla test ederler. Sonuçlar, önerilen algoritmanın diğer yaklaşımlarla karşılaştırıldığında daha iyi performansa (% 99,81'e eşit doğruluk) sahip olduğunu gösterdi.

Opeyemi Osanaiye, [56] Yeni bir özellik seçme yöntemi önermek için üç farklı filtre yöntemini (ReliefF, Ki-kare ve Kazanç oranı dahil) birleştirdi. Temel amaçları, sistem karmaşıklığını azaltmak ve sınıflandırma (karar ağacı algoritması ve J48 kullanarak)

doğruluğunu artırmaktı. Önerilen yöntem, NSL-KDD veri kümesindeki 41 orijinal özellikten 14 önemli özelliğe sahip bir alt küme oluşturdu. Doğruluk, tespit oranı ve yanlış alarm oranını göz önünde bulundurarak önerilen yöntemin performansını değerlendirirler. Deneysel sonuçlar, önerilen yöntemin etkili özellikleri azaltabileceğini ve diğer filtreleme yöntemlerine kıyasla yüksek sınıflandırma doğruluğuna ve algılama oranına ve daha az güç tüketimine sahip olduğunu göstermektedir.

Melike GÜNAY [57], FA tabanlı özellik seçiminin önerilen modifikasyonu. Bir KNN sınıflandırıcı kullanarak ve fazladan bir özellik seçme adımı ekleyerek geleneksel FA'nın performansını iyileştirdiler. IDS'nin 4 farklı veri kümesini kullandılar, her veri kümesi için çeşitli alt özellikler yaptılar ve bu alt kümelere uygulanan sınıflandırma yöntemlerinin performansını karşılaştırdılar. Deneysel sonuçları, önerilen FA'nın özelliklerin boyutunu azaltabildiğini ve bellek kullanımını azaltabildiğini (yaklaşık% 50) ve hesaplama süresinden tasarruf ettiğini göstermiştir. Ayrıca, önerilen FA, sınıflandırmanın doğruluğunu geliştirdi.

Saldırı tespit sistemlerinin performansını optimize etmek için Alebachew Chiche [58],ölçeklenebilir ve doğası gereği uyarlanabilir yeni bir entegre öğrenme yaklaşımı. Bu yaklaşımda, sınıflandırılmış modeli oluşturmak için rastgele bir orman makine öğrenimi algoritması kullanılmıştır. Önerilen yöntem NSL-KDD 40558 veri seti ile uygulanmış ve değerlendirme sonuçları, bu yöntemi uygulayarak saldırı tespitinin doğruluğunun% 99,91 olduğunu göstermiştir.

Xin Li P. Y., [59] Saldırı tespit sistemlerinde düşük performans ve yüksek sayıda yanlış pozitif ile ilgili sorunları çözmek için doğrusal en yakın komşu kement adımına (LNNLS-KH) dayalı geliştirilmiş bir kril sürüsü algoritması önerildi. Bu yöntemde, doğrusal en yakın komşu kement aşaması optimizasyonu gerçekleştirilir, bu da saldırı tespitinin doğruluğunu artırır. Bu araştırmacılar tarafından gerçekleştirilen uygulamaların sonuçları, LNNLS-KH algoritmasının NSL-KDD veri setinde ortalama 7, CICIDS2017 veri setinde ise 10.2 özellik seçtiğini ve uygulanamayan özelliklerin kolayca kaldırıldığını göstermiştir. Bu algoritma aynı zamanda optimum uygunluk

yineleme eğrisinde, yakınsama hızında iyi performans gösterir ve yanlış bir pozitif oran gösterir. bu araştırmacılar NNGE algoritmasının önerildiler. NNGE algoritmasının sınıflandırma doğruluğunu ve hızını iyileştirmek ve hesaplamalı kaynak tüketimini azaltmak için, VHDRA (Dikey ve Yatay Akıllı Veri Kümesi Azaltma yaklaşımı) olarak adlandırılan bir dikey ve yatay veri azaltma yöntemi sundu. VHDRA aşağıdaki özellikleri sağlar:

- En önemli özellikleri seçerek ve NNGE dikdörtgenlerini aşırı küçülterek veri kümesindeki özellikleri dikey olarak azaltın.
- Durumları ve veri çıkarmayı izlemek için bir yöntem olan STEM adı verilen bir yöntemi kullanarak veri çıkarma modunu ve yöntemini yatay olarak izleme.
- Önerilen yöntemin uygulanmasının sonuçları, bu yöntemin diğer yöntemlere kıyasla veri setindeki özelliklerin sayısını azaltabileceğini ve saldırı tespitinin doğruluğunu artırabileceğini göstermiştir.

Muhammad Hilmi Kamarudin, [60], Birleşik Saldırı Anormalliği Algılama (UIAD) yöntemini kullanarak, web sunucularında bilinmeyen saldırıları tespit etmek için saldırı tespit sistemlerinin işlevini geliştirmek için yeni bir yol sundu. Önerilen yöntemde üç bileşen kullanılmıştır (ön işleme, istatistiksel analiz ve sınıflandırma). Önerilen yöntemin DARPA 1999 ve ISCX 2012 veri setlerini kullanarak uygulanması, bilinmeyen saldırıları tespit etmede% 95 doğruluğa sahip olduğunu ve yanlış alarmların tespit oranının yaklaşık% 1 olduğunu göstermiştir.

Herrmann, [61], Nesnelerin İnterneti'nde kullanılan iletişim ağlarında (WSN, MANET, CPS gibi) saldırı tespit sistemlerinin kullanımı üzerine kapsamlı araştırmalar yaptı. Araştırmacılar, Nesnelerin İnternetinde kullanılan kaynakların sınırlamaları nedeniyle çoğu saldırı tespit sisteminin pek uygun olmadığını söyledi. Bu nedenle, Nesnelerin İnterneti için uygun saldırı tespit sistemleri geliştirmemiz gerekiyor.

Guoquan Li, [62], İzinsiz giriş tespit sistemlerinin kullanımındaki en önemli sorunlardan bazıları, çok sayıda yanlış alarm oluşturarak ve doğru saldırı tespitinin doğruluğu yapılmıştır. Bu araştırmada, bu sorunu çözme yöntemleri araştırılmıştır. Bu

amaçla, ağ saldırılarını tespit etmek için veri füzyon (DF) tekniklerine odaklandılar ve DF tekniklerinin performansını karşılaştırmak için bir dizi kıyaslamayı incelediler. Bu çalışmada, birçok sınıflandırma tekniğinin (RF, C4.5, NN ve SVM gibi) daha verimli tespit sistemleri oluşturmadaki etkinliği gösterilmiştir.

Ansam Khraisat, [63], hibrit bir HIDS IDS önerdi (C5 karar ağacı sınıflandırmasını ve bir destek vektör makinesini (SVM) birleştiren). Bu saldırı tespit sisteminin amacı, bilinen ve bilinmeyen tehditleri tespit etmede geleneksel saldırı tespit sistemlerinin sorunlarının üstesinden gelmektir. Ayrıca, bilinen izinsiz girişleri tanımlamayı ve saldırı tespitinin doğruluğunu artırmayı ve yanlış alarm oranlarını azaltmayı amaçlayan bir çerçeve önerdiler. Bu çerçevede, anormallikleri tanımlamak (bilinmeyenleri belirlemek için) ve imzaları tanımlamak (bilinen tehditler için) için iki yöntem kullanılmıştır. Önerilen HIDS, farklı veri kümeleri kullanılarak değerlendirildi ve değerlendirme sonuçları, tanı doğruluğu ve düşük yanlış alarm oranı açısından SIDS ve AIDS'e kıyasla daha iyi performansa sahip olduğunu gösterdi.

Jyoti Snehi, [64], imza temelli farklı etki sistemleri ve bunların faydaları hakkında tartıştı. Çalışmalarının sonuçları, bir dizi imzanın ve temel modelin, saldırı tespit sisteminin her bir özelliğinin göreceli önemini gösterdiğini ve sistem yöneticilerinin siber saldırıları ve ağ ve bilgisayar sistemi tehditlerini belirlemesine yardımcı olduğunu gösterdi. Bu nedenle, izinsiz girişlerin% 80'i imza tabanlı tespit yöntemleri kullanılarak kolayca ve hızlı bir şekilde tanımlanabilir.

David Mudzingwa, [65], saldırı tespit sistemleri ve saldırı önleme sistemleri oluşturmak için kullanılan yöntemleri incelemeye çalışmıştır. Araştırmacılar daha çok anormallik tabanlı, imza tabanlı, son teknoloji ve kompozisyon tabanlı protokol analizine odaklandılar. Anormalliğe dayalı yöntem, kullanıcılar için herhangi bir güncelleme veya girdi olmaksızın yeni tehditlerin tespit edilmesine dahil olur, ancak piyasadaki çoğu IDPS, birkaç temel yöntemin bir kombinasyonunu kullanır. Bu çalışma aynı zamanda pazardaki IDPS ürünleri tarafından kullanılan IDPS yöntemlerinin kolay karşılaştırılması ve değerlendirilmesi için yöntemler sağlar.

Liu Hua Yeo, [66], farklı saldırı tespit sistemleri türlerine, nasıl sınıflandırıldıklarına ve izinsiz giriş tespit sistemlerinde çalışmak için olağandışı etkinlikleri tanımlamak için kullanılan farklı algoritmalara genel bir bakış sağladı. Bu araştırmanın ana odağı, anormallik tabanlı ve imza tabanlı saldırı tespit sistemleri üzerineydi. Daha sonra, bu araştırmacılar farklı penetrasyon teknikleri yöntemlerini karşılaştırmaya çalıştılar. Bilgi güvenliğinde IDS'lerin farklı yöntemlerini ve önemini de açıkladılar.

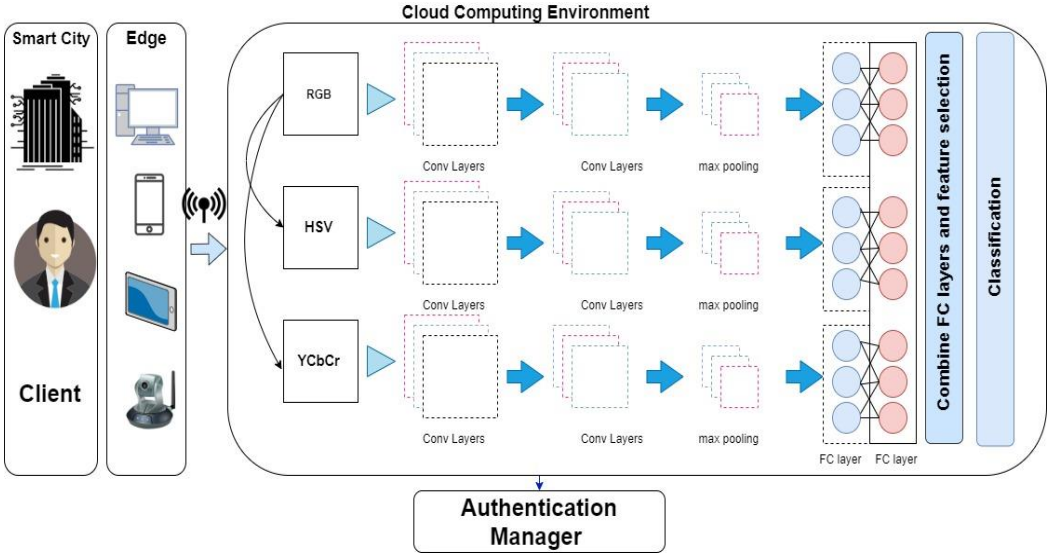
Singh, [67], iki yaklaşımı tek bir sistemde birleştirerek hibrit bir IDS önerdiler. Açık kaynaklı bir proje olan kötüye kullanım tabanlı IDS Snort kullanılarak oluşturulan paket üstbilgisi anormallik algılamasını (PHAD) ve ağ trafiği anormallik algılamasını (NETAD) birleştiren hibrit IDS, anormallik algılamaya dayalı bir sistemdir. MIT Lincoln Laboratories ağ trafiği verilerini (IDEVAL) simüle edilen veri kümelerini kullanarak önerilen karma saldırı tespit sistemi ve farklı saldırı türlerini tanımlamadaki etkinliği değerlendirildi. Bu değerlendirmenin sonuçları, önerilen sistemin anormallikler ve suistimaller yaratarak yaratılan izinsiz girişleri belirlemede yüksek bir etkinliğe sahip olduğunu göstermiştir.

BÖLÜM 3. ÖNERİLEN YÖNTEMLER

Ağ Güvenliği, tüm ağ türlerinde hayati bir rol oynamaktadır. Günümüzde ağ ofisler, okullar, bankalar vb. Her yerde uygulanmaktadır ve hemen hemen tüm bireyler sosyal ağ medyası. Birçok ağ güvenlik sistemi türü kullanımda olsa da, savunmasız faaliyetler ara sıra gerçekleşiyor. Bu proje, web saldırıları gibi çeşitli ağ saldırıları türleri ve kullanımda olan farklı Saldırı Tespit Sistemleri (IDS) hakkında bir özet sunar. Bu proje, ağ sistemini çeşitli ağ saldırılarından koruyabilecek yeni bir IDS türü tasarlamak için bir yol açabilir. esas olarak, sahtekarlık saldırıları, Ip sahtekarlığı, yüz sahtekarlığı veya parmak izi sahtekarlığı gibi izinsiz giriş saldırıları ana gruplarından biridir.

3.1. Önerilen Iot Tabanlı Çerçeve Yüz Sahtekarlığı Algılama

Akıllı şehir çerçevesi, Şekil 3.1.'de gösterildiği gibi akıllı cihazlar, yüksek hızlı kablosuz ağ ve bulut sunucusu gibi birden çok bileşeni içerir. Nesnelerin İnterneti cihazları tarafından yakalanan yüz görüntüleri, analiz ve kenarlarla ön işleme. Kenarları ve akıllı cihazları olan ön işleme bölümü, yüz görüntüsünü çıkarmak ve bulut kaynağını optimize etmek için daha fazla gelişmiş veri göndermek için Viola ve jones [68] yüz algılama algoritmasını içerir. Ardından, yakalanan yüzlü görüntüler kablosuz teknoloji kullanılarak sürekli olarak bulut ortamına gönderilir. Bulut bölümünde, birkaç Sanal Makine (VM) paralel modda çalışır. Bu sanal makineler, sahtekârlık saldırısının tespitinde derin öğrenme yaklaşımını kullanırlar.

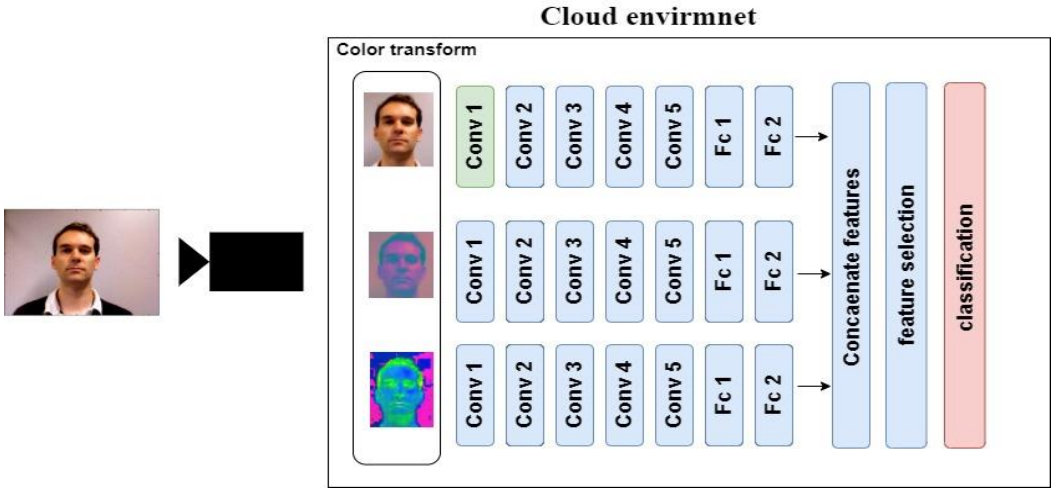


Şekil 3.1. Yüz sahtekarlığı tespiti için önerilen IoT tabanlı çerçeve

Bulut bilişim ortamlarında sınıflandırma için yüz görüntüsünü derin modele beslemeden önce, RGB renk alanı HSV ve YCbCr renk uzaylarına dönüştürülür. Önerilen derin öğrenme yaklaşımında önceden eğitilmiş üç paralel model kullanılmıştır. Literatüre dayanarak, az sayıdaki veri ve kontrollü ortamlarda senaryo eksikliği nedeniyle, CNN modellerini sıfırdan eğitmek ve istikrarlı ve yüksek performanslı bir model elde etmek oldukça zordur. Bu durumda, yüz sahtekarlığı tespiti için RGB renk alanında VGG -Face [69] modelini kullandık [17] [70]. Ek olarak, HSV ve YCbCr renk uzaylarının dönüştürülmüş görüntüleri bulut tarafında ayrı ayrı VGG16 [71] modeli tarafından eğitilir. Modellerin farklı bir renk uzayıyla ince ayarından sonra, her derin model için 4096 özellikten oluşan son tam bağlantılı katmanın özellikleri çıkarılır. Bu özellikler birleştirilir ve ardından minimum Artıklık Maksimum Alaka Düzeyi (mRMR) [72] özellik seçim algoritması kullanılarak seçilir. Bu seçilen özellikler, Şekil 3.2.'de sunulduğu gibi, sahtekarlık görüntüsünün tespiti için Doğrusal Regresyon (LR), Destek Vektör Makinesi (SVM), Doğrusal Ayrımcı Analiz (LDA) ve K En Yakın Komşuluk (KNN) gibi farklı sınıflandırma algoritmaları yardımıyla sınıflandırılır.

Bir öğrencinin çevrimiçi bir sınava erişmek istediği bir senaryo varsayalım. Akıllı telefon veya bilgisayar gibi akıllı bir cihaz, öğrencinin yüz görüntüsünü yakalar ve bu görüntüyü 5G kablosuz teknolojisini kullanarak buluta gönderir. Bulut sunucusunda,

yüz sahtekarlığı görüntü veritabanı ve derin öğrenme yöntemi kullanılarak, üç farklı renk uzayında yüz görüntüsünün derin özellik seti çıkarıldı. Bu birleşik özellik kümeleri, çevrimiçi sınav senaryosunda yüz sahtekarlığını tespit etmeye yardımcı olan yüz ten tonlarından çeşitli canlılık anahtarları içerir



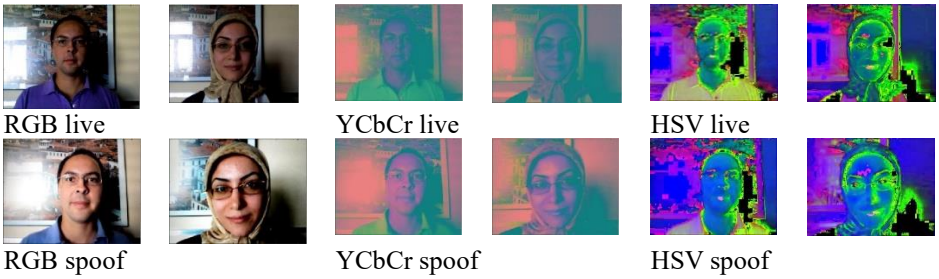
Şekil 3.2. Derin öğrenme yaklaşımının mimarisi.

Önerilen yöntem, Replay attack ve ROSE-Youtu olmak üzere iki genel erişim veritabanına dayalı olarak test edilir ve değerlendirilir. Yeniden oynatma saldırıları, MacBook dizüstü bilgisayar web kamerası ve Huawei, iPhone 5s, ZTE ve Hasee akıllı telefon tarafından yakalanan ROSE-Youtu veritabanı tarafından yakalanır.

3.2. Renk Alanı Dönüşümü

RGB, renkli görüntüleri görüntülemek ve algılamak için birçok cihaz ve sensör için ortak bir renk alanıdır. Yine de, kırmızı, yeşil ve mavi renklerin yüksek korelasyonu ve parlaklık ve renklilik bilgilerinin eksik ayrımı nedeniyle bu renk alanı görüntüleri analiz etmek için oldukça sınırlıdır. Bu durumda, sahtekarlık veritabanlarında tekrarlanan artefaktların tespiti için farklı renk uzayları kullanılır [15]. RGB'ye ek olarak HSV ve YCbCr, yüz ten tonlarından farklı canlılık ipuçlarını algılamak için sağlam özellikler sağlar. Hem HSV hem de YCbCr renk uzayları, parlaklık ve renklilik bileşenleri gibi renk dokusu bilgileri sağlar. HSV renk uzayında, H ve S, renklilik bilgisini sunmak için renk tonu ve doygunluk boyutlarını tanımlar ve V, görüntülerin

parlaklık bilgisini sunmak için değer boyutunu tanımlar. YCbCr alanı, RGB'yi parlaklık (Y), Krominans Mavisi (Cb) ve Renk Kırmızısı (Cr) olarak ayırır. HSV ve YCbCr alanları, farklı sahtekarlık saldırılarında yüz cilt tonlarından ayırt edici renk tabanlı doku sağlar [14]. Şekil 3.3., hem canlı hem de sahte yüz görüntüleri için Replay saldırı veritabanında farklı renk boşlukları sunar.



Şekil 3.3. Replay saldırı veritabanlarına dayalı farklı renk uzayları.

3.2.1. Evrişimli sinir ağları

Evrişimli sinir ağları (CNN'ler), geri yayılma algoritmalarının yardımıyla özelliklerin uzamsal hiyerarşilerini otomatik olarak öğrenmek için tasarlanmış ve geliştirilmiştir [73]. CNN'ler, esas olarak evrişim, havuzlama ve tamamen bağlı (FC) katmanlar gibi çoklu temel yapısal blokları içeren çoklu nöron katmanlarına dayalı olarak tasarlanmıştır. Her evrişimli katman, boyutları 3 × 3, 5 × 5 veya 7 × 7 piksel olabilen bir dizi filtre içerir. Bu nedenle, her evrişimli katman, bir filtre uygulayarak, bir sonraki katmanın girdisini oluşturur [73]. Bu evrişim sürecinin sonuçları, yerel ayırt edici özellikler içeren aktivasyon haritalarıdır. Denklem 3.1'e göre, L katmanının $Y_i^{(l-1)}$çıktısı $m_2^{(l)} \times m_3^{(l)}$ boyutlarında $m_1^{(l)}$özellik haritalarını içerir.). Bu denklemde, $B_i^{(l)}$ve $k_{I,j}^{(l)}$,sırasıyla i. Özellik haritası [74] için temel matrisi ve filtre boyutunu temsil eder.

$$Y_i^{(l)} = f\left(B_i^{(l)} + \sum_{j=1}^{m_i^{(l-1)}} k_{i,j}^{(l)} \times Y_j^{(l-1)}\right) \tag{3.1}$$

Havuzlama katmanı, modeldeki parametrelerin ve hesaplamaların sayısını azaltmak için görüntünün uzamsal boyutunu azaltır. Bu katman, görüntü özelliklerini ve

bilgilerini olduğu gibi tutmak için her özellik haritasında bağımsız olarak çalışır. Her havuz katmanı L, filtre $F^{(l)}$ ve $S^{(l)}$ adımının uzamsal boyutu olarak iki ana parametre içerir. Havuzlama katmanının girdisi, $m_1^{(l)} \times m_2^{(l)} \times m_3^{(l)}$ boyutundaki verilerdir ve bu katmanın çıktı hacmi şu şekildedir: $m_1^{(l)} \times m_2^{(l)} \times m_3^{(l)}$ (Denklem 3.2) kısaca havuzlama katmanının çalışmasını göstermektedir.

$$\begin{cases} m_1^{(l)} = m_1^{(l-1)} \\ m_2^{(l)} = \frac{m_2^{(l-1)} - F^{(l)}}{S^{(l)}} + 1 \\ m_3^{(l)} = \frac{m_3^{(l-1)} - F^{(l)}}{S^{(l)}} + 1 \end{cases} \tag{3.2}$$

Son evrişimli veya havuzlama katmanının özellik haritalarının çıktısı, tam bağlantılı katman olarak adlandırılan katmanda düzleştirilir. FC katmanı, önceki katmanların çıktısını tek boyutlu bir özellik vektörüne dönüştürür, ağırlıkları günceller ve her etiket için mümkün olan en son değerleri sağlar . Bu katmanlar, Yoğun katman olarak da bilinen daha tam bağlantılı bir katmana bağlanabilir. Bir öğrenme hızı kullanarak, her giriş her çıkışa bağlanır. Özellikler, Evrişim katmanları tarafından çıkarılır, havuzlama katmanları tarafından aşağı örneklenir ve FC katmanı tarafından modelin son çıktısına eşlenir. Son FC katmanı, sınıflandırma görüntülerinin sınıflarının sayısına eşit sayıda düğüm içerir. Her FC katmanı, ReLU işlevi gibi doğrusal olmayan bir işlevle desteklenir. Denklem Şekil, FC katmanının işleme adımlarını ağırlıklarla (W) ve doğrusal olmayan $f\left(Z_i^{(l)}\right)$ fonksiyonuyla gösterir [75].

$$Y_i^{(l)} = f\left(Z_i^{(l)}\right) \text{ with } Z_i^{(l)} = \sum_{j=1}^{m_i^{(l-1)}} w_{i,j}^{(l)} \times y_j^{(l-1)} \tag{3.3}$$

3.2.1.1. Önceden eğitilmiş modeller

Yüz sahtekarlığı tanıma için önceden eğitilmiş deney modellerini değiştirmek için, modeller sahte veri tabanları kullanılarak ince ayar yapılmıştır. Tespit problemlerini sahtekarlık yapmak ve sınıflandırma katmanının çıktısını iki sınıf sahtekarlık ve gerçek yüz olarak değiştirmek için ikili sınıflandırma kullanılmıştır.Önceden eğitilmiş

modellerin son FC katmanının maliyet işlevi (Denklem. 3.4). Bu denklemde, i ve n sırasıyla eğitim örneklerinin indeksi ve $[Y_0; Y_1]$; Tüm tahmin değerleri için Örneğin tahmin değeridir. Matristeki maksimum değeri bulmak için $\max(Y_i)$ fonksiyonu kullanılır.

$$\text{Cost} = \sum_{i=1}^{n}\{\max(Y_i)\} + \log\left(\sum_{j=0}^{1}\exp\left(y_{ij} - \max(Y_i)\right)\right) - y_{ir}\} \quad (3.4)$$

Tablo 3.1. VGG mimarisi

Layer	Patch size / stride	Input size
Conv × 2	3× 3/1	64 × 224 × 224
Pool	2 × 2	64 × 224 × 224
Conv × 2	3× 3/1	128 × 112 × 112
Pool	2 × 2	128 × 112 × 112
Conv × 3	3× 3/1	256 × 56 × 56
Pool	2 × 2	256 × 56 × 56
Conv × 3	3× 3/1	512 × 28 × 28
Pool	2 × 2	512 × 28 × 28
Conv × 3	3× 3/1	512 × 14 × 14
Pool	2 × 2	512 × 14 × 14
FC	25088 × 4096	25088
FC	4096 × 4096	4096

Eğitim aşamasında sahtekarlık veritabanına dayalı SoftMax sınıflandırma katmanını değiştirdikten sonra, VGG16 ve VGG-Face modelleri, sahtekarlık veritabanına dayalı olarak ince ayarlandı. VGG yüz modeli, yüz tanıma sistemleri için önceden eğitilmiş popüler modellerden biridir. Bu model Oxford Visual Geometry Group [69] tarafından geliştirilmiştir. Model, RGB renk alanında 2,6 M yüz görüntüleri ile eğitilmiştir ve bir girdi görüntüsünün varsayılan boyutu 224 × 224'tür [70]. Bu model, beş maksimum havuzlama, düzeltilmiş doğrusal birim (ReLU) işlevine sahip on üç evrişimli katman ve FC6, FC7 ve FC8 olmak üzere üç tam bağlı katman içerir. Tamamen bağlı son katman (FC8), 2622'den (yüz görüntüsü sınıfları) 2 sahte ve gerçek sınıfına değiştirilir. VGG-Face modelinin mimarisi, Tablo 3.1.'de gösterildiği gibi, yüz görüntüleri ile eğitilen VGG16'nın bir çeşididir. Bu yaklaşımda, yüz yanıltma veri tabanına dayalı ince ayarlanmış VGG-Face ve VGG-16 modelleri kullanılmaktadır. derin bir özellik çıkarıcı olarak. Derin özellikler, çıktı katmanından önceki son katman olan FC7'den (yedinci tam bağlı katman) alınmıştır. Tüm modeller için bu FC katmanının aktivasyon değerleri, girdi görüntüleri için 4096'ya (boyutsal özellik vektörleri) eşit varsayılan değer olarak ayarlanmıştır.

3.2.2. Özellik seçimi

MRMR yönteminin temel amacı, sınıfla en fazla korelasyona sahip olan özelliklerin alt kümesini seçmek ve karşılıklı bilgiye dayalı olarak ilgisiz ve fazlalık özelliklerini azaltmaktır [76] [77]. I'nin iki X ve Y özelliği arasındaki karşılıklı bilgisinin ölçülmesi, Denklem 3.7'ye göre tanımlanır.

$$\mathrm{I}(\mathrm{x},\mathrm{y}) = \sum_{\mathrm{i,j}} \mathrm{p}\left(\mathrm{x_i},\mathrm{y_j}\right)\log\frac{\mathrm{p}\left(\mathrm{x_i},\mathrm{y_j}\right)}{\mathrm{p}(\mathrm{x_i})\mathrm{p}(\mathrm{y_j})} \tag{3.5}$$

Burada $p(x_i)$ ve $p\left(y_j\right)$ marjinal olasılıkları temsil eder ve $p\left(x_i, y_j\right)$ ortak olasılık dağılımını temsil eder. Denklemin her bir özelliğini K-boyutlu vektörde F_i olarak tanımlayalım ($F_i = [F_{1i}, F_{2i}, F_{3i}, \dots, F_{Ki}]$). Bu durumda, değişkenlerin (i, j) karşılıklı bilgileri $I\left(F_i, F_j\right)$ olarak tanımlanır. Seçilen alt kümenin en iyi özelliklerini bulmak için aşağıdaki Denklem. 3.8 ve 3.9 karşılanmalıdır. Minimum fazlalık özelliği Denklem. 3.8 ve maksimum alaka koşulu (Denklem 3.9).

$$\mathrm{minW}, \mathrm{W} = \frac{1}{|\mathrm{s}|^2}\sum_{\mathrm{F_iF_j}} \mathrm{I}\left(\mathrm{F_i},\mathrm{F_j}\right) \tag{3.6}$$

$$\max \mathrm{V}\ , \mathrm{V} = \frac{1}{|\mathrm{s}|}\sum_{\mathrm{F_iF_j}} \mathrm{I}(\mathrm{H},\mathrm{F_i}) \tag{3.7}$$

H, sınıf etiketini ve s, seçilen özelliklerin sayısını gösterir. MRMR özellik seti, Denklem 10'da sunulan özellik seçim kriterleri olan Karşılıklı Bilgi Farkı (MID) ve Karşılıklı Bilgi Katsayısı (MIQ) kombinasyonunun optimize edilmesiyle elde edilir.

$$\begin{cases} \mathrm{MID} = \max(\mathrm{v} - \mathrm{w}) \\ \mathrm{MIQ} = \max\left(\frac{\mathrm{v}}{\mathrm{w}}\right) \end{cases} \tag{3.8}$$

MID ve MIQ koşullarını optimize etmek için, aşağıdaki denklemde gösterildiği gibi bunların tek bir kriter fonksiyonunda [72] birleştirilmesi gerekir:

$$f_{mRMR}(X_i) = I(H, F_i) - \frac{1}{|s|}\sum_{F_i F_j} I(F_i, F_j) \quad (3.9)$$

$I(H, F_i)$ sınıf için eklenecek uygunluk özelliğini ölçer ve $\frac{1}{|s|}\sum_{F_i F_j} I(F_i, F_j)$, önceden seçilmiş s özelliklerine göre özelliklerin fazlalığını tahmin eder. Bu seçilen özellikler, yüz sunum saldırısını algılamak için doğrusal regresyon sınıflandırma algoritması ile sınıflandırılır.

3.3. Yüz Sahtekarlığı Tespiti İçin Sağlam Derin İnanç Ağı

Biyometrik kimlik doğrulama yöntemleri günümüzde çok sayıda kullanıcı tarafından önerilmekte ve güvenilmektedir. Bu sistemlerin tanıtımının temel nedenleri, paylaşılmayan nitelikleri ve yüksek güvenlikleri olmakla birlikte, aslında, bu kimlik doğrulama sistemleri çeşitli saldırılara karşı da savunmasızdır [78]. Bu tür kimlik doğrulama sistemleri için Temel Geçirgenlik hataları yüz sahtekarlığı saldırılarıdır. Bu saldırılar, saldırganın kurbanın biyometrik bilgilerini toplayacak ve kimlik doğrulaması için kullanacağı şekilde yapılandırılmıştır. Bu bilgilerin çoğuna sosyal ağlar üzerinden erişilebilir . Saldırı türleri göz önüne alındığında, yüz sahtekarlığı saldırıları dört ana tekrar saldırısı, 3D saldırılar, ekran görüntüsü ve baskı saldırısı gruplarına ayrılmıştır [79]. Basılı ve görüntülü görüntü saldırılarında, siber suçlu, mağdurun yüz görüntüsünü alıp dijital bir aygıtta bastırarak veya görüntüleyerek kimlik doğrulama sistemini çatlatır. Aynı şekilde, 3D maske saldırıları için, saldırganlar kurbanın yüzüyle bir maske yaparlar. Tekrar oynatma veya video saldırıları, genellikle kurbanın yüzünün videosuna ihtiyaç duyan sistemi kirletmek için karmaşık bir yöntemdir. Bu yöntemde, kayıtların yüz hareketlerinin daha doğal görünmesi gerekir ve diğer üç tür kimlik sahtekarlığı saldırısına kıyasla tespit edilmesi daha zordur. Çoğu parodi saldırısında bilgileri yeniden yakalama sırasında, bazı eserler kalır. Bu eserler sahte videodan canlı videoyu tanımlamaya yardımcı olur. Bununla birlikte, videolardan hayati işaretlerin keşfedilmesi, örneğin yetersiz kimlik sahtekarlığı verileri gibi çeşitli sorunlara maruz kalmaktadır [70]. Bu alanda, senaryo eksikliği veya saldırı türleri ile karşı karşıya olan bazı kamu erişim veritabanları elde edebiliriz. Başka bir sorun, farklı senaryolara karşı belirsiz performanstır. Örneğin,

yerel ikili kalıplar veya Yerel Yönlü Kalıplar [39] gibi özellik tanımlayıcılarına dayanan bazı mevcut yöntemler, ışık, gölgeler ve arka plan varyasyonlarını değiştirme gibi senaryolarda zayıf performans gösterir.

Bu tür sorunları çözmek için sağlam ve doğru bir tanıma yaklaşımı öneriyoruz. Bu yaklaşımın temel yeniliği Sağlam Temel Bileşen Analizi (RPCA) yardımıyla yüz dinamiği bilgilerinin çıkarılmasıdır [80]. Şekil 3.4.'de gösterildiği gibi, veri odaklı bir model olarak dudak hareketi, kafa hareketi ve göz kırpma gibi karmaşık canlı ipuçlarını yakalar. Gri renklerle vurgulanan bölümler dinamik değişiklikleri gösterir. Ayrıca, RPCA algoritması daha önce tanıma görevleri için kullanılmamıştır. RPCA özelliklerinin sınıflandırılması için Derin İnanç Ağı (DBN) [3] yaklaşımı kullanılmıştır. DBN algoritmaları, görüntü yeniden oluşturma ve sınıflandırma için güçlü yöntemler olarak kabul edilmektedir. DBN'lerin başarısı, birçok araştırmacıyı bu derin öğrenme yöntemlerini bir özellik çıkarma ve sınıflandırma çerçevesi olarak kullanmaya teşvik etmelidir.

Makalemizin ana katkıları aşağıdaki gibidir: ilk olarak, RPCA algoritması yüz sahteciliği tespitinin hareket analizi kısmına uygulanır. Bu algoritma, tüm videodaki önemli ipuçlarını kare kare ayıklar. Hayati ipuçları arasında tekrar hareket saldırılarını, görüntü görüntülerini ve basılı saldırıları ayırt etmeye yardımcı olan dudak hareketi, kafa hareketi ve göz kırpma bulunur. ikincisi, derin inanç ağı, ayırt edici özellik kümelerini öğrenmek ve bu özelliklerin SoftMax katmanıyla ince ayarını yapmak ve sınıflandırmak için etiketlenmemiş RPCA görüntü setleri üzerinde ön eğitimdir. Finalde, iki farklı kamu veritabanında deneysel sonuçlar elde edilir ve sonuçlar, önerilen yöntemin sağlamlığının, en son teknoloji algoritmalarına kıyasla önemli ölçüde iyileştiğini göstermektedir.


Client 24 real data set


Client 21 real data set

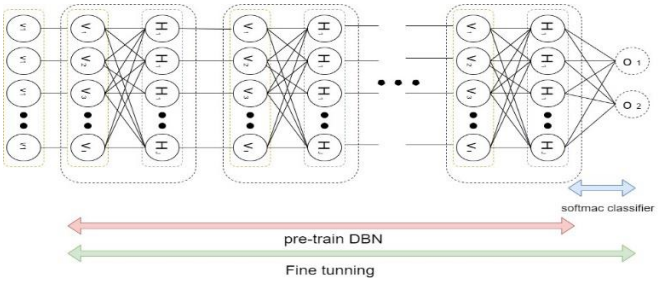

Client 24 RPCA for real data set


Client 24 RPCA for real data set

Şekil 3.4. Olumsuz bir senaryo için web kamerası kimlik doğrulamasında

Bu makale şu şekilde düzenlenmiştir: İlk bölümde, ilgili çalışmaları kısaca tanıtıyoruz. İkinci bölümde modellerimizin metodolojisini ve yapısını sunuyoruz. Üçüncü bölümde, deneysel sonuçlar sunuyoruz. Dördüncü bölümde önerilen yaklaşımımızı özetliyoruz.

Her sınıflandırma algoritmasının performansı büyük ölçüde orijinal verilerden çıkarılan ve öğrenilen özelliklere bağlıdır. Bu nedenle, girdi verilerinden ayrımcı özellikler elde etmek ve öğrenmek için bir model tasarlamak için birçok girişimde bulunulmuştur. Bu nedenle, derin öğrenme yöntemleri bu amaç için tasarlanmış ve geliştirilmiştir . Son araştırmalara dayanarak, derin öğrenme yöntemleri örüntü tanıma, nesne algılama ve sınıflandırma gibi birçok uygulama için doğruluk durumunda önemli sonuçlar elde etmektedir. Derin sinir ağı, yığılmış oto kodlayıcı (SAE), DBN ve evrişimli sinir ağı (CNN) gibi üç farklı mimari içerir. [33] ‘te DBN modeli sunulduktan sonra, DBN’ler önemli derin öğrenme algoritmaları modellerine dönüşür. Bu yöntemde, üretim modeli ve geri yayılım, Şekil 3.5.’te sunulduğu üzere, eğitim öncesi prosedür ve ince ayar adımları için sırasıyla uygulanır. DBN algoritmasının iki ana özelliği, eğitim verilerinin sınır sayısında önemli ölçüde performans gösterir [81]. yüz sahteciliği tespitinde olduğu gibi ve en uygun parametreleri hızlı bir şekilde bulma (hızlı öğrenme). Bu yaklaşımda, yüz kimlik sahtekarlığı tespiti için RPCA video çıkış verisi için DBN’nin etkinliği ve avantajlarını inceliyoruz.



Şekil 3.5. Görüntü sınıflandırması için DNN mimarisi

3.3.1. Sınırlı boltzmann makinesi

DBN'lerin Eğitimi için, Kısıtlı Boltzmann makinesi (RBM) [82] katman bazında eğitilebilir. Bir RBM, bu ağın sırasıyla görünür ve gizli birimler adıyla iki katmanlı içerdiği iki taraflı yönlendirilmemiş bir grafik model olarak tanımlanır $\upsilon = \{0, 1\}_D$ ve $h = \{0, 1\}_F$,, sunulduğu gibi Şekil 3.5.'te.

Boltzmann makine mimarisi, P (υ, h) derz dağılımlarına dayanan tasarımdır. Görünür v ve gizli h birimlerinin her olası kombinasyonunun enerji fonksiyonu E (υ, h; θ) olan ortak olasılık P (υ, h), Denklem 3.12'e göre sunulmuştur.

$$E(\upsilon, h; \theta) = -\sum_{i=1}^{D} b_i \upsilon_i - \sum_{j=1}^{F} a_i h_i - \sum_{i=1}^{D} \sum_{j=1}^{F} w_i v_i h_j \ (\theta = \{b_i, a_j, w_{ij}\})$$

Burada wij, görünür ve gizli birimler arasındaki ağırlıktır ve bi ve ai, görünür ve gizli birimin i ve jth değerlerinin sırasıyla ardışık olmasıdır. Normalleştirme sabiti olarak Z (θ) ile P (υ, h; θ) eklem dağılımı üniteler üzerinden hesaplanır. bu ağ, her bir giriş vektörü için E (υ, h; θ) enerji fonksiyonu ile bir olasılık hesaplar. Egzersiz vektörü sırasında, denklem 3.13'da gösterildiği gibi, enerjiyi azaltmak için θ değiştirilerek olasılık düzeltilebilir.

$$P(\upsilon, h; \theta) = \frac{1}{Z(\theta)} \exp(-E(\upsilon, h; \theta)) \ Z(\theta) = \sum_v \sum_h E(\upsilon, h; \theta) \quad (3.13)$$

gizli ünite v verilen her giriş vektörünün h koşullu dağılımları için uygulanan lojistik fonksiyon, gizli ünite v verilen v giriş vektörü h, Denklem 3.14. Burada, g (x) lojistik fonksiyonudur.

$$p(h_j = 1|v) = g(\sum_{j=1}^{D} w_{ij} v_i + a_j)$$
$$p(v_j = 1|h) = g(\sum_{j=1}^{F} w_{ij} h_i + b_j) \quad (3.14)$$
$$g(x) = \frac{1}{1+\exp(-x)}$$

Kontrastlı ıraksama (CD) [83] algoritması ağ ağırlıklarının W güncellenmesi için yararlı bir yaklaşım sağlar. rekonstrüksiyon sırasında sadece giriş katmanının özellikleri olarak öğrenilen gizli birimlerde bilgi kullanılır. Model orijinal girişi düzgün bir şekilde kurtardığında, gizli birimlerin girişten yeterli bilgi öğrendiğini gösterir.

3.3.2. Ön hazırlık DBN

Eğitim öncesi adımların ana fikri, DBN ağını önemli özellikleri yeniden üretmeyi öğrenir. Bu üretken model (sınıflandırma katmanı olmadan), eğitim öncesi etiketlenmemiş eğitim verilerini yeniden yapılandırır; Bu durumda, denetimsiz bir şekilde gerçekleştirildi. DBN'nin hiyerarşik mimarisine dayanarak, ön hazırlık adımları yinelemeli açgözlü bir öğrenme moduna uygulanabilir. DBN'leri eğitmek, RBM'leri CD algoritması kullanarak yığın modunda yığın katman eğitmek anlamına gelir. eğitim RBM, girdi eğitim setlerinin ($X=\{v_n^l\}$). günlük olabilirlik log $p(x|w^l)$ maksimize etmeye dayanır. dolayısıyla RBM'nin maliyet fonksiyonu C (x), Denklem 3.15'de sunulmaktadır.

maliyet işlevini en üst düzeye çıkarmak için degrade tabanlı yöntemler uygulanabilir. ağırlıklar n-aşamalı CD yöntemiyle yaklaşık eğime göre güncellenir [84]. CD algoritması, aşağıdaki denklemde olduğu gibi model dağılımına göre ağ ağırlıklarının W güncellenmesi için faydalı bir yaklaşım sağlar.

$$\Delta_{w_{ij}^l} C(x) \propto \langle v_i^l h_j^l \rangle \text{ data} - \langle v_i^l h_j^l \rangle \text{ recons} \quad (3.15)$$

burada $\langle\langle v_i^l h_j^l\rangle$ recons rekonstrüksiyonları, giriş verilerinden Gibbs örneklemesinin n-aşamasından sonra dağılımına göre yeniden yapılanma özelliğini göstermektedir [82].

$$P\left(\hat{Y}k\middle|\hat{X}k,\theta\right)=O_{\hat{y}k}\left(\hat{X}k,w^{l+1},B^l\right)=\frac{\exp\{-\sum_{m=1}^{M}\delta(\hat{y}k=m)\left(w_m^{L+1}\right)^T h^l\left(\hat{X}k,w^l,B^l\right)\}}{\sum_{m=1}^{M}\exp\{-\left(w_m^{L+1}\right)^T h^l\left(\hat{X}k,w^l,B^l\right)\}} \tag{3.16}$$

Burada $h^l\left(\hat{X}k,w^l,B^l\right)$, j-th gizli birimlerinin çıktısını birleştirmek için L-th katmanının vektörüdür. Bu durumda, $\hat{X}k$ girişi için

$$h_j^l\left(\hat{X}k,w^l,B^l\right)=\frac{1}{1+\exp\left(-b_j^l-\sum_{i=1}^{j_{l-1}}w_{ij}^l h_i^{l-1}\left(\hat{X}k,w^{l-1},B^{l-1}\right)\right)} \tag{3.17}$$

Burada w^l ve B^l , ağırlık ve bias parametreleri kümesini tanımlar ve j , DBN için l-katman birimlerinin sayısıdır. İnce düzeltme için log-posteriorun maksimize edilmesi, Denklem (3.18) 'i takip ederek Q (θ) minimize edilmesine eşdeğerdir.

$$Q(\theta)=-\log P\left(\hat{Y}\middle|\hat{X},\theta\right)=-\sum_{k=1}^{K}\log\left(O_{\hat{Y}k}\left(\hat{X}k,w^{l+1},B^l\right)\right) \tag{3.18}$$

$\theta=\left\{W^{l+1},B^l\right\}$ olduğunda, tüm model parametreleri kümesini belirtir. Bu parametreler, denklemle (3.19) t + 1 yinelemede gradyan alçalması ile güncellenir.

$$W^{(t+1)}=W^{(t)}-\overline{W^{(t)}},\ W^{(t+1)}=\mu\overline{W^{(t)}}+\alpha\frac{\partial Q(\theta)}{\partial W^{(t)}} \tag{3.19}$$

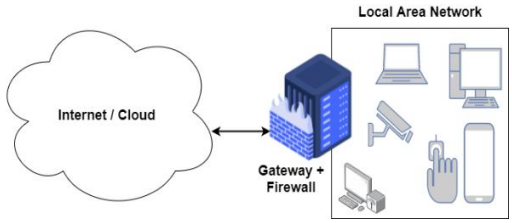
$$B^{(t+1)}=B^{(t)}-\overline{B^{(t)}},\ B^{(t+1)}=\mu\overline{B^{(t)}}+\alpha\frac{\partial Q(\theta)}{\partial B^{(t)}} \tag{3.20}$$

Burada, μ momentum ve α öğrenme hızıdır.

3.4. Hibrit İmza Sistemi ve Anormallik Tabanlı Saldırı Tespit Sistemi

Bu araştırmada, çeşitli saldırı türlerine karşı herhangi bir kuruluşun ağ güvenliği için önerilen çözüm. Bu saldırılarda web uygulaması, işletim sistemi güvenlik açıkları veya her türlü yazılım açıkları dikkate alınır. Yapılandırılmış Sorgu Dili (SQL) Enjeksiyon saldırısı, Siteler Arası Komut Dosyası (XSS) saldırısı, bozuk kimlik doğrulama ve fidye yazılımı saldırıları için herhangi bir yük gibi, çoğunlukla odaklanmıştır. Bunun için FreeBSD 12 Unix işletim sistemi, IDS / IPS olarak Suricata ile birlikte bir ağ geçidi veya güvenlik duvarı olarak kullanılır. Hedeflenen ağdaki kötü amaçlı trafiği engellemek için Suricata imzalarının oluşturulmasında iki tür makine öğrenimi yöntemi kullanılır. Meta-turizme dayalı özellik seçimi için sinir ağı ve anormallik tabanlı tespit için, bu araştırma makalesinde bulanık mantık kullanılmıştır. Kali Linux 2020.3'ün en son kararlı sürümü, web uygulamaları ve farklı işletim sistemleri için bir saldırı sistemi olarak kullanılır. Bu istemci sistemlerinde Windows 10/7 ve Ubuntu 20.04 kullanılmaktadır.

Web uygulamalarına erişmek için Chrome, Firefox ve Edge tarayıcıları kullanılır. Bu laboratuvar ortamı, kavram kanıtı için sanal kutuya yerleştirilmiştir. Herhangi bir kuruluşun ağ güvenliği için temel genel görünümü Şekil 3.6.'de verilmiştir.

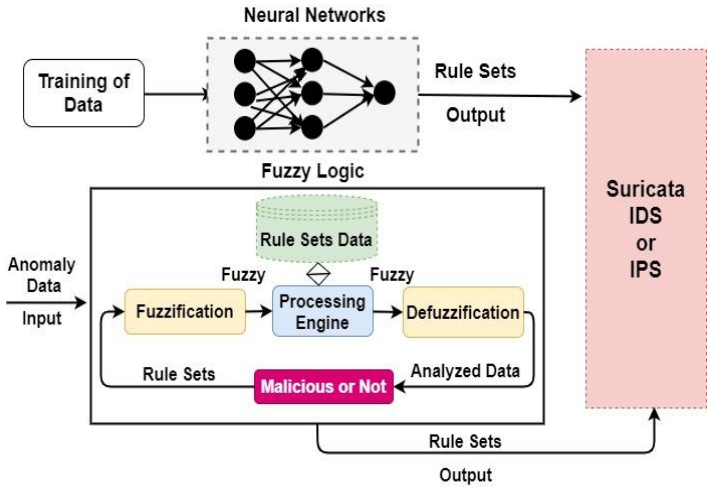


Şekil.3.6. Ağ Güvenliğine temel genel bakış

3.4.1. Sinir bulanık mantık çıkarım sistemi

Burada önerilen çözümde Suricata IDS / IPS, meta-sezgisellerin hedeflenen ağdaki kötü amaçlı trafiği manuel olarak algılaması için NN modeliyle birlikte dağıtılır. Kötü niyetli trafiğin tespiti için bu yöntemi kullanarak, daha yüksek tanımlama oranı ve daha düşük yanlış alarm ile farklı saldırılar. NN modeli, yaygın olarak kullanılan

yöntemlerden biridir ve kısmen doğrudan bir başlangıca dayandıkları ve fark edilmesi zor olmadıkları için çeşitli bileşik makul rahatsızlıkların ve farklı meta-sezgisel düzene sokma algoritmalarının üstesinden gelmede verimli olmuştur. İkincisi, kesin bilgi gerektirmez, üçüncü olarak mahalle optimasından kaçınma yeteneğine sahiptir. Dördüncüsü, zıt disiplinleri kapsayan geniş kapsamlı konularda kullanılabilir. Doğanın zorladığı meta-sezgisel figür, doğal veya fiziksel mucizeleri kopyalayarak yükseltme sorunlarını çözer. Üç ana işlevde toplanabilirler: ilerleme temelli, malzeme bilimine dayalı ve sürü temelli prosedürler. İlerlemeye dayalı prosedürler, ticari marka geliştirme yasaları tarafından uygulanmaktadır. Faiz metodolojisi, ortaya çıkan yaşların üzerinde yaratılan gelişigüzel yaratılmış insanlarla başlar. Bu sistemlerin kalite nedeni, en iyi bireylerin, bireylerin bu şekilde zamanının ana hatlarını çizmek için sürekli olarak ve büyük ölçüde birleşmeleridir. Bu, genel nüfusu stratejinin zenginliğinde çok uzun bir süre yeniden tasarlanmasını sağlar.YSA tabanlı IDS iki bakış açısından mevcuttur: I) özellikle düşük ziyaretli saldırılar için daha düşük vahiy kesinliği, örneğin mahalleye uzak, istemciden köke ve II) daha kırılgan tanımlama kararlılığı. (Beghdad, R., 2008). Bulanık mantık, anormallik tabanlı saldırıların tespiti için kullanılır. Ek dosyalarına veya bilinmeyen protokollere sahip trafik, anormallik trafiği olarak tespit edilene dayalı olarak bulanık mantık tarafından işlenecektir. Önerilen modelin ayrıntılı dahili çalışması Şekil 3.7.'de açıklanmıştır.



Şekil 3.7. IDS / IPS için Önerilen Çözümün dahili çalışması

Web uygulamaları, işletim sistemleri (OS) ve herhangi bir mobil uygulama ile ilgili çeşitli saldırı türlerinin kalıpları veya imzaları NN modelinde eğitilecektir. NN yönteminden eğitilen verilerin işlenmesinden sonra, SQL Enjeksiyon saldırıları, XSS saldırıları, bozuk kimlik doğrulama, güvensiz trafik, herhangi bir uygulamanın veya çerçevenin eski sürümleri, savunmasız işletim sistemi gibi çeşitli kötü amaçlı trafik türleri için yeni kural setleri oluşturulacaktır. ve mobil uygulamaların herhangi bir bilinen güvenlik açığı. NN modelinin çıktısı, hedeflenen ağa yapılan saldırıları önlemek için Suricata IDS / IPS'ye girilecektir. Önerilen çözümün daha verimli performansı için, açık kaynak kara liste İnternet Protokolü (IP) adres kaynakları kullanılır. Kaynak kara liste IP adresi kaynakları, bu IP adreslerini her 4 saatte bir güncelleme sıklığında veritabanında saklanır. Kara liste IP adreslerini depolamak için program, özel PHP ve MySQL topluluk sürümü kullanılmıştır.

3.5. IDS'de Çok Amaçlı Parçacık Sürü Algoritması Tabanlı ve Hızlı Öğrenme Ağının Kombinasyonu

Bu makalede, MOPSO ve FLN tabanlı FSS kombinasyonuna dayalı olarak NIDS için bir yöntem önerilmektedir. Önerilen yöntem, ağdaki saldırı tespit modellerini belirlemek ve modeli değerlendirmek için KDD Kupası veri setini kullandı. Özellikler, öncelikle ilgili özellikleri seçerek sınıflandırma zorluğunu azaltmak ve sınıflandırma doğruluğunu artırmak için seçilir. Tek amaçlı özellik seçimi görevlerinde, özellik seçiminin optimizasyon için bir amacı vardır. Özellik seçimi, en uygun sınıflandırma performansı için en iyi özellik kombinasyonunu bulmak için yapılır. Çok amaçlı özellik seçimi (MOFS), hedefin birden çok hedefi optimize etmek için bir denge oluşturmak olduğu çok amaçlı bir optimizasyon problemine dönüştürerek özellik seçiminden sorumludur. FSS için bu optimizasyon yönteminin temel amacı, sınıf etiketine dayalı özelliklerin sayısını azaltmak ve ağdaki saldırı algılama hatalarını azaltmaktır, bu da test örneklerini tahmin etmenin doğruluğunu artıracaktır. Sonuç olarak, çok amaçlı özellik seçimi optimizasyon problemi için bir çözüm, her bir çözümün iki bileşenin bir vektörü, özellik sayısı ve sınıflandırma hata oranı olduğu bir dizi baskın çözümdür. Amaç, özellik seçme problemini bir en aza indirme sorunu olarak kullanarak ilgisiz özelliklerin sayısını en aza indirgemek ve böylece

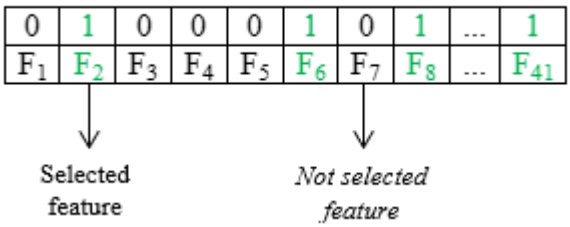
sınıflandırma hata oranını en aza indirmektir. Önerilen yöntem aşağıda formüle edilmiştir.

3.5.1. Önerilen yöntemin formülasyonu

Kennedy ve Eberhart ilk kez 1995 yılında sürü davranışından esinlenerek PSO'yu rapor ettiler. PSO'nun temel amacı, en iyi besin kaynağı arayışında bir sürünün arama modeline benzer bir hedef fonksiyonun arama alanında en uygun çözümü bulmaktır. Oluşturulan bir dizi parçacık, PSO'daki en iyi çözümleri rastgele arar. Bu bağlamda, bir arama parçacıkların kendi uçuş hızlarını ve yönlerini sırasıyla 1 ve 2 denklemlerine göre ayarlamasıyla gerçekleştirilir [18].

$$x_{id}(t+1) = x_{id}(t) + v_{id}(t+1) \tag{3.21}$$

veri kümesinde bulunan özelliklerin sayısı. Şekil 3.8., veri setinde bulunan özelliklerin sayısının 41 olarak tahmin edildiği bir parçacığın temsilinin bir örneğini göstermektedir.



Şekil 3.8. Veri kümesi örneğinin ilk popülasyon vektörünün bir temsili

Gözlemlendiği gibi, PSO'daki her parçacık, veri kümesinde bulunan bir dizi özellik olarak kabul edilir. Bu bağlamda, vektörün bir dizi elemanı rastgele sıfır ve bir olabilir. Sıfır değerine sahip öğeler, seçilmemiş unsurları belirtirken, bir değeri olan öğeler, öğeyle ilgili özellik seçimini gösterir. Sonuç olarak, seçili özellik alt kümesinin [F2, F6, F8, F41] özellik kümesini içerdiği açıktır.

Önerilen yöntemde, Sigmoid (S) ‘nin transfer fonksiyonu, birincil parçacık vektörleri için öznitelik seçiminin veya seçim eksikliğinin olasılığını tanımlamak için kullanıldı. Bu fonksiyonun işlevi, rasgele olasılığın, genellikle 0.5 olarak kabul edilen transfer fonksiyonunun eşik değerinden küçük olması durumunda, ilgili elemandaki bu özelliğe sıfır değeri tahsis edilecek şekildedir. Aksi takdirde, özellik için bir değer kaydedilecek ve istenen özellik hedef fonksiyona göre değerlendirilecektir. Her parçacığın birincil konumu ve hızı, PSO’nun doğasına göre ilk popülasyonun seçilmesinin ardından değerlendirme fonksiyonları tarafından belirlenir. Bu teknikte, her bir parçacığın konumu, veri setinde bulunan özelliklerden seçilen özellikler olarak kabul edilir ve her bir parçacığın hızı, yüksek sınıflandırma oranına yakınsama oranı ve sınıflandırma hatasının azaltılması olarak kabul edilir. En yüksek değerlendirme işlevi değerine ve daha yüksek çevreleyen parçacık sürüsüne sahip özellikler, birincil özellik seçim aşamasının çıktısı olarak seçilir. En iyi parçacık konumu ve hızı sonuçları bu aşamada saklanır ve parçacık konumu güncellenir. Süreç, hedefler arasında bir denge oluşturan nihai bir yanıta ulaşana kadar devam eder.

3.5.2. Hedef fonksiyon

Daha önce bahsedildiği gibi, önerilen yöntem MOPSO’yu sınıf etiketi için seçilen özelliklerin bir alt kümesini seçmek için uyguladı. Bu teknikte, birden çok hedef birleştirilir ve sonunda en aza indirme şeklinde iki genel özellik kategorisi elde edilir. Ayrıca, özelliklerin seçilen alt kümeleri, özelliklerin sayısını ve sınıflandırma hata oranlarını azaltmaya yönelik iki ana hedefe dayalı olarak değerlendirilir. Uyum fonksiyonu, ilk popülasyonun değerlendirilmesi, uzman popülasyonunun seçimi ve en büyük ağırlığa sahip partiküllerin bulunmasına göre denklem 3.22 şeklinde sunulur.

$$Minimize\ F(x) = \begin{cases} f_1(x) = \frac{L}{A} & , L \in A, A \in \mathbb{R}^+ \\ f_2(x) = 1 - \frac{FP+FN}{P+N} & , (P+N) \in \mathbb{R}^+ \end{cases} \tag{3.22}$$

Burada L, veri kümelerinden seçilen özelliklerin sayısıdır ve A, toplam özellik sayısıdır. Karışıklık matrisi ile ilgili kriterler, her bir adımda seçilen özelliklere dayalı olarak her parçacığın hata oranını değerlendirmek için kullanıldı; burada gerçek pozitif

(TP), normal olarak normal olduğu tespit edilen normal düğümlerin kategorisini göstermek için kullanılır. sınıflandırma modeli ve seçilen özelliklere göre. Ek olarak, yanlış pozitif (FP), sınıflandırma modeli tarafından yanlış bir şekilde izinsiz giriş olarak algılanan ve seçilen özelliklere dayanan normal düğümlerin kategorisini göstermek için uygulanır. Ayrıca, gerçek negatif (TN), sınıflandırma modeli tarafından doğru bir şekilde tespit edilen ve seçilen özelliklere dayanan izinsiz giriş düğümlerinin kategorisini göstermek için kullanılır. Son olarak, yanlış negatif (FN), sınıflandırma modeli tarafından yanlışlıkla normal olarak algılanan ve seçilen özelliklere dayalı olarak izinsiz giriş düğümlerinin kategorisini belirtmek için uygulanır. 3.22 denkleminde P, TP + FN'ye eşittir ve N, FP + TN'ye eşittir. Birinci hedef fonksiyonu f1 (x), seçilen özelliklerin veri setinde mevcut olan toplam özelliklere oranı ile ilgilidir, ikinci fonksiyon f2 (x) ise sınıflandırma hata oranını değerlendirmek için kullanılır.

3.5.3. FLN tabanlı sınıflandırma

FLN, önde gelen tek katmanlı bir ağdan ve üç giriş, gizli ve çıkış katmanı içeren üç katmanlı bir sinir ağından gelen paralel bir bağlantıdır. Genel olarak FLN, çift paralel ileri sinir ağı (DPFNN) olan yapay bir sinir ağıdır ve burada sınıflandırma hata oranı, en küçük kare tekniği adı verilen bir analiz yaklaşımı kullanılarak tahmin edilir [12]. Bu, çok katmanlı bir paralel bağlantıyı ve tek katmanlı bir sinir ağını açıklar. Daha önce tartışıldığı gibi, MOPSO'daki optimal parçacıklar, FLN'ye girdi olarak girilen veri kümesinden seçilen özelliklerin alt kümesini gösterir. Önerilen yöntemde FLN, MOPSO'nun merkezinde yer alır ve çözümlerin sınıflandırma hatalarını tahmin etmekten sorumludur. FLN'de kodlanan çözümler, ağırlıklandırıldıkları ve eğitildikleri giriş katmanı aracılığıyla orta katmana aktarılır. FLN ve sinir ağları arasındaki temel fark, FLN'deki tüm gizli oyuncuların antrenman ağırlıklarını beklememesi ve hata miktarının belirtilen eşikten daha az olduğu her gizli katman katmanındaki önyargı miktarlarının ve ağırlıklarının çıktı katmanına aktarılmasının olmamasıdır. Bu, ağda aşırı uyumu önlemenin yanı sıra çözümlerin öğrenme ve sınıflandırma hızında bir artışa izin verir.

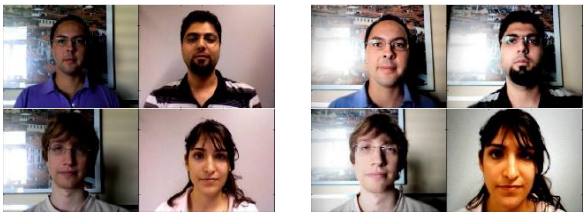
Önerilen yöntemde, MOPSO'da rastgele seçilen ilk çözümler, özelliklerin sayısı ve uygunluk işlevinde seçilen özelliklerin önemi değerlendirilmesinin yanı sıra FLN tarafından sınıflandırılır ve bunların hata değeri, çoklu nesnel uygunluk işlevi. En düşük sayıda önemli özelliğe ve en düşük sınıflandırma hata oranına sahip parçacıklar, her aşamada uzman parçacıklar ve baskın olmayan çözümler olarak seçilir ve uzman çözüm havuzunda saklanır. Önerilen algoritmanın bir sonraki aşamasında, önceki aşamadaki optimal parçacıkların hata oranına dayalı olarak hata eşiği miktarı dikkate alınır. Eşik koşulu için geçerli olan her gizli katmanda FLN'ye girilen çözümler çıkışa doğru yönlendirilir.

BÖLÜM 4. DENEYSEL VERİTABANLARI

Bu tezde, aşağıdaki gibi tanımlanan dört farklı veri setini kullandık:

4.1. The Replay-Attack Database

Yüz sahtekarlığı için Replay-Attack Veritabanı, farklı aydınlatma koşulları altında 50 kullanıcıye yönelik 1300 video klibi fotoğraf ve video saldırı girişiminden oluşur. Bu Veritabanı, İsviçre'deki Idiap Araştırma Enstitüsü'nde üretildi. Tüm videolar, bir (gerçek) kullanıcının yerleşik bir web kamerası aracılığıyla bir dizüstü bilgisayara erişmeye çalışmasıyla veya aynı istemcinin bir fotoğrafını veya video kaydını en az 9 saniye boyunca görüntüleyerek oluşturulur. Web kamerası 320 piksel (genişlik) x 240 piksel (yükseklik) çözünürlüğe sahip renkli videolar üretir. Filmler QuickTime çerçevesi (codec: Motion JPEG) kullanılarak bir Macbook dizüstü bilgisayarda kaydedildi ve ".mov" dosyalarına kaydedildi. Kare hızı yaklaşık 25 Hz'dir. Apple bilgisayarlardaki yerel desteğin yanı sıra, bu dosyalar mplayer, ffmpeg veya Linux veya MS Windows sistemleri altında bulunan diğer video araçları kullanılarak * kolayca * okunabilir. Saldırı protokolleri, saldırıları yanıltmaya yönelik karşı önlemlerin (ikili sınıflandırma) performansını değerlendirmek için kullanılır. Veritabanı, saldırıyı oluşturmak için kullanılan cihaz türüne göre 6 farklı protokole bölünebilir: baskı, mobil (telefon), yüksek çözünürlüklü (tablet), fotoğraf, video veya genel test (tüm türler). Ayrıca, saldırıları saldırganın çıplak elle gerçekleştirdiği şekilde veya sabit bir destek kullanarak sınıflandırarak önceki 6 grubun tepesinde alt kümeleme gerçekleştirilebilir. Bu sınıflandırma şeması, 2D yüz sahtekarlığı saldırılarına karşı önlemlerin performansını incelemek için kullanılabilecek toplam 18 protokol oluşturur. Aşağıdaki Şekil, her protokoldeki video kliplerin miktarını detaylandırmaktadır. Bu veri tabanındaki bazı görüntüler Şekil 4.1. olarak sunulmuştur [85].



Live face Spoof face

Şekil 4.1. Canlı ve sahte görüntüler için saldırı veritabanı örneklerini yeniden oynatın.

4.2. ROSE-Youtu Face Liveness Detection Dataset

ROSE-Youtu Yüz Canlılık Algılama Veritabanı, çok çeşitli aydınlatma koşullarını, kamera modellerini ve saldırı türlerini kapsar. ROSE-Youtu Yüz Canlılık Algılama Veritabanı (ROSE-Youtu), toplamda 25 konulu 4225 videodan oluşur (5.45GB boyutunda 20 konuyla herkese açık 3350 video) [86].

Her konu için, ortalama süresi yaklaşık 10 saniye olan 150-200 video klip bulunmaktadır. Veritabanını toplamak için beş cep telefonu kullanıldı: (a) Hasee akıllı telefon (640 * 480 çözünürlüklü), (b) Huawei Akıllı telefon (640 * 480 çözünürlüklü), (c) iPad 4 (çözünürlüklü) 640 * 480), (d) iPhone 5s (1280 * 720 çözünürlüklü) ve (e) ZTE akıllı telefon (1280 * 720 çözünürlüklü). Tüm yüz videoları öne bakan bir kamera tarafından çekilir. Yüz ile kamera arasındaki mesafe yaklaşık 30-50 cm'dir. Gerçek yüz videosu için normalde 25 video vardır (5 sahneli 5 cihaz). Sahne, ofis ortamında 5 farklı aydınlatma koşulunu kapsar. Kullanıcı gözlük takarsa, 25 video daha olacaktır. Bu veritabanı, basılı kağıt saldırısı, video yeniden oynatma saldırısı ve maskeleme saldırısı dahil olmak üzere üç sahtekarlık saldırısı türünü içerir. Basılı kağıt saldırısı için, hala basılı kağıtla yüz görüntüsü ve titreyen basılı kağıt (A4 boyutu) kullanılır. Video yeniden oynatma saldırısı için, Lenovo LCD ekranında ve Mac ekranında bir yüz videosu görüntülüyoruz. Maskeleme saldırısı için, kırpılmış ve kırpılmamış maskeler dikkate alınır. Dahası, yüz videoları, yüz videolarının farklı aydınlatma koşullarıyla birleştirilmesini garanti eden farklı arka planlarla çekilir. Orijinal yüz videosuyla tutarlı olmak için, sahtekarlık aracı ile kamera arasındaki ayrılma mesafesi de yaklaşık 30-50 cm'dir.

Live face Spoof face

Şekil 4.2. Canlı ve sahte yüz görüntüleri için ROSE-Youtu Yüz Canlılık Algılama örnekleri

4.3. Oulu-Npu

OULU-NPU veritabanının amacı, daha önce görülmeyen giriş sensörleri, saldırı türleri ve edinim koşulları dahil olmak üzere bazı gerçek dünya varyasyonları altında mobil senaryolarda yüz PAD tekniklerinin genelleme performanslarını değerlendirmektir. Bu veritabanı Finlandiya'daki Oulu Üniversitesi'nde ve Çin'deki Northwestern Politeknik Üniversitesi'nde oluşturuldu. Oulu-NPU yüz sunumu saldırı tespit veritabanı, 4950 gerçek erişim ve saldırı videosundan oluşur. Bu videolar, farklı aydınlatma koşulları ve arka plan sahneleriyle (Oturum 1, 2. Oturum ve 3. Oturum). OULU-NPU veritabanında dikkate alınan sunum saldırısı türleri, yazdırma ve videoyu yeniden oynatmadır. Saldırılar, iki yazıcı (Yazıcı 1 ve Yazıcı 2) ve iki görüntüleme aygıtı (Ekran 1 ve Ekran 2) kullanılarak oluşturuldu. Samsung Galaxy S6 telefonu ile yakalanan gerçek erişimlerin ve saldırıların bazı örnek görüntülerini göstermektedir. 55 deneğin videoları eğitim, geliştirme ve test için üç konuya ayrılmış alt gruba ayrıldı [87].

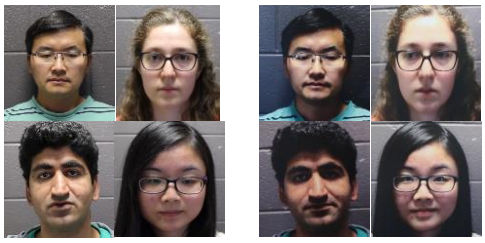
Live face Spoof face

Şekil 4.3. Canlı ve sahte yüz görüntüleri için OULU-NPU örnekleri

4.4. Spoofing in the Wild Database (SIW)

SiW, 165 özneden canlı ve sahte videolar sağlar. Her konu için toplam 4.478 videoda 8 canlı ve 20 adede kadar sahte videomuz var. Tüm videolar 30 fps, yaklaşık 15 saniye

uzunluk ve 1080P HD çözünürlüktedir. Canlı videolar, mesafe, poz, aydınlatma ve ifade çeşitliliği ile dört seansta toplanır. Sahte videolar, basılı kağıt ve tekrar oynatma gibi çeşitli saldırılarla toplanır [88].



Live face Spoof face

Şekil 4.4. Canlı ve sahte yüz görüntüleri için SIW örnekleri.

4.5. KDD Cup 1999 Data

Bu, KDD-99 Beşinci Uluslararası Bilgi Keşfi ve Veri Madenciliği Konferansı ile birlikte düzenlenen Üçüncü Uluslararası Bilgi Keşfi ve Veri Madenciliği Araçları Yarışması için kullanılan veri setidir. Rekabet görevi, izinsiz girişler veya saldırılar olarak adlandırılan `` kötü '' bağlantılar ile `` iyi '' normal bağlantılar arasında ayrım yapabilen bir öngörü modeli olan bir ağ saldırı detektörü oluşturmaktı. Bu veritabanı, askeri bir ağ ortamında simüle edilen çok çeşitli izinsiz girişleri içeren, denetlenecek standart bir veri seti içerir. KDD veri kümesinin bazı öznitelikleri aşağıdaki tabloda sunulmuştur.

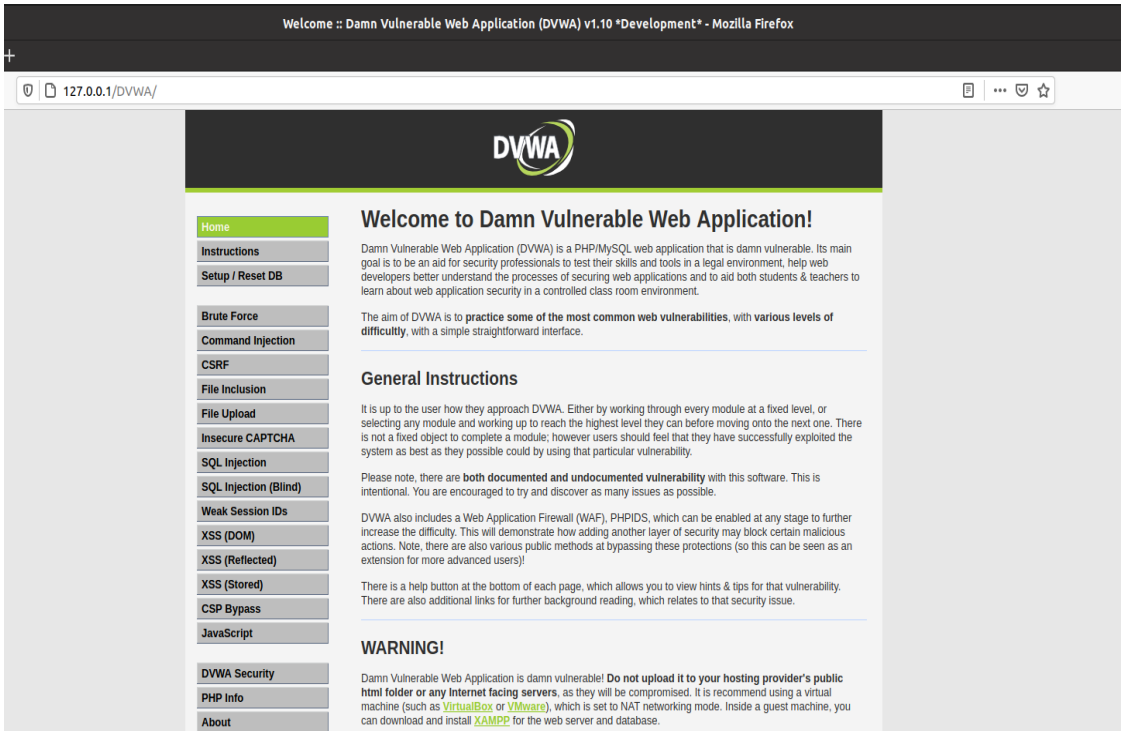
Tablo 4.1. KDD veri kümesinin bazı öznitelikleri

	Duration	Protocol_Type	Service	Flag	Src_Bytes	Dst_Bytes	Land	Outcome
0	0	tcp	http	SF	181	5450	0	normal.
1	0	tcp	http	SF	239	486	0	normal.

4.6. Karma İmza ve Anormallik Veri Kümesi

Laboratuvar, makine öğrenimi yöntemlerini kullanarak IDS / IPS için önerilen çözüme ilişkin konseptin kanıtı için sanal bir ortamda konuşlandırılmıştır. Bunların tümü, herhangi bir gerçek sunucuya veya kullanıcıya zarar vermekten kaçınmak için VirtualBox açık kaynaklı yazılımında konuşlandırılmıştır. Bu nedenle, herhangi bir web uygulaması kullanıcılarının veya işletim sistemi kullanıcılarının gizliliği

korunmaktadır. FreeBSD 12.1, sanal laboratuvar ortamı için bir ağ geçidi ve güvenlik duvarı olarak konuşlandırılmıştır. Bunun üzerine, manuel sinir ağları ve anormal bulanık mantık çıkarım sistemleri için önerilen makine öğrenme yöntemi yüklenmiştir. Bununla birlikte Suricata IDS / IPS, FreeBSD yerleşik Paket Filtreleme (PF) ve farklı açık kaynaklı kaynaklardan gelen IP adresi veritabanları kara liste için PHP'de geliştirilen özelleştirilmiş program kullanılır. Ubuntu 20.04, bu araştırma belgesinde önerilen çözümü test etmek için Lanet Savunmasız Web Uygulaması (DVWA) savunmasız web uygulamaları için dağıtılmıştır. Bu web uygulaması, gelişmiş SQL enjeksiyon saldırılarının yanı sıra ilk on güvenlik açığının tümüne sahiptir. Aşağıdaki Şekil 4.5.'te tasvir edilmiştir.



Şekil 4.5. Virtual Lab'de Dağıtılan Savunmasız Web Uygulaması.

Windows 10 istemci sistemi, makine öğrenimi yöntemlerini uygulayarak Suricata IDS / IPS aracılığıyla bilgisayar korsanlarının saldırılarına karşı güvenliğini sağlamak için de kurulur. Bilgisayar korsanlığı makinesi, Kali Linux 2020.3 sürümünün kurulmasıyla da konuşlandırıldı. Bu, işletim sistemi ve web uygulaması güvenlik açıklarından yararlanmak için kullanılacaktır.

DVWA web sitesinde bir saldırıyı için Windows 10 işletim sisteminde Kali Linux kullanılır. Kali Linux yardımıyla Suricata IDS / IPS'nin güvenlik imzası ML yöntemleri kullanılarak oluşturulur. Bu süreçte iki tür teknik kullanılmaktadır. Bunlardan biri, SQL enjeksiyonu, XSS, bozuk kimlik doğrulama, işletim sistemi güvenlik açıkları gibi iyi bilinen saldırılar için bir Sinir Ağıdır. Kali Linux'ta SQL enjeksiyon saldırısı SQLMAP açık kaynak aracı yardımıyla başlatılır. İlk komutta, veritabanı adı hedef web uygulamasından çıkarılır. Ancak bir güvenlik duvarı olarak Suricata IDS / IPS nedeniyle, veri tabanı adını alamaz veya hedeflenen web uygulamasını, Şekil 4.5.'te gösterildiği gibi veri tabanı bilgileriyle ilgili olarak sıralayamaz. İkinci olarak, kullanıcı adları ve şifreler web uygulamasının o veri tabanından çıkarılır. -Temper veya -random-aracı kullanarak gelişmiş SQL enjeksiyon sorguları için, aynı sonuç türünün tekrarlanması nedeniyle gerekli bilgileri alamamak için bu sonucun bir kağıt görüntüsü buraya dahil edilmemiştir. Bu modelin bazı özellikleri aşağıdaki tabloda sunulmuştur.

Tablo 4.2. Windows 10 İstemcisinde Başarıyla Kullanıcı Oturumu Açma

Action	Date and Time	Status	Source IP	Destination IP	Username	Risk Level
logged on	Oct 01, 2020, 1:24:43 AM	User Login Success	192.168.150.128	192.168.150.135	N/A	5
logged on	Oct 01, 2020, 1:20:03 AM	User Login Success	192.168.150.128	192.168.150.135	N/A	5
logged on	Oct 01, 2020, 1:13:13 AM	User Login Success	192.168.150.128	192.168.150.135	N/A	5
logged on	Oct 01, 2020, 1:07:13 AM	User Login Success	192.168.150.128	192.168.150.129	N/A	5
logged on	Oct 01, 2020, 1:00:53 AM	User Login Success	192.168.150.128	192.168.150.129	N/A	5

Aşağıdaki Tablo 4.2.'de veriler Suricata IDS / IPS günlüklerinden sunulmuştur. Bu günlükler, Windows istemci sistemi ve web uygulamasında uzaktan oturum açmanın bir güvenlik duvarında oluşturduğu birçok olay türü ile ilgilidir. Bu saldırılarda SMB

istismarları, SQL enjeksiyon saldırısı, XSS, web uygulaması oturum açmaya kaba kuvvet saldırısı.

Tablo 4.3. Güvenlik duvarında farklı saldırı türleri

Action	Suricata IDS/IPS	Date and Time	Status	Source IP	Destination IP	Username or Attack Type	Risk Level
Failed to log on	192.168.150.131	Oct 01, 2020, 1:29:53 AM	Failure	89.46.223.240	192.168.150.135	POSTGRES	3
Failed to log on	192.168.150.131	Oct 01, 2020, 1:29:43 AM	Failure	118.107.76.23	192.168.150.135	TEST1	3
Failed to log on	192.168.150.131	Oct 01, 2020, 1:29:43 AM	Failure	192.168.150.128	192.168.150.135	ADMINISTRATOR	3
Failed to log on	192.168.150.131	Oct 01, 2020, 1:29:43 AM	Failure	212.42.214.3	192.168.150.135	LENOVO	3
Failed to log on	192.168.150.131	Oct 01, 2020, 1:29:43 AM	Failure	124.109.54.218	192.168.150.129	SQLi	3
Failed to log on	192.168.150.131	Oct 01, 2020, 1:29:43 0AM	Failure	192.168.150.128	192.168.150.129	SQLi	4
Failed to log on	192.168.150.131	Oct 01, 2020, 1:29:43 AM	Failure	212.42.214.3	192.168.150.129	XSS	3
Failed to log on	192.168.150.131	Oct 01, 2020, 1:29:34 AM	Failure	192.168.150.128	192.168.150.129	XSS	3
Failed to log on	192.168.150.131	Oct 01, 2020, 1:29:34 AM	Failure	212.42.214.3	192.168.150.129	SQLi	3
Failed to log on	192.168.150.131	Oct 01, 2020, 1:29:34 AM	Failure	112.161.27.203	192.168.150.129	SERVER	3
Failed to log on	192.168.150.131	Oct 01, 2020, 1:29:34 AM	Failure	192.168.150.128	192.168.150.129	ADMINISTRATOR	4
Failed to log on	192.168.150.131	Oct 01, 2020, 1:29:34 AM	Failure	212.42.214.3	192.168.150.129	MASTER	3
Failed to log on	192.168.150.131	Oct 01, 2020, 1:29:34 AM	Failure	192.168.150.128	192.168.150.129	ACER	3
Failed to log on	192.168.150.131	Oct 01, 2020, 1:29:34 AM	Failure	89.46.223.240	192.168.150.129	Web Application	3

BÖLÜM 5. DENEYSEL SONUÇLAR

Önerilen yöntemler bir NVIDIA GeForce 4GB grafik kartı (GPU) ile derlendi. Diğer donanım detayları, Intel Core i5 3.6 GHz işlemci ve 16 GB RAM idi. Aşağıdaki tabloda sunulduğu gibi, bu parametreler varsayılan değerleri ile kullanılmıştır. Ayrıca mini parti boyutu 32 olarak belirlendi.

Tablo 5.1. Bu çalışmada kullanılan önerilen yaklaşımın parametre değerleri.

Software	Optimization	Activation function	Momentum	Decay	Mini-batch	Learning rate
Keras	Adam	ReLU	0.9	1e-6	32	0.01

Modellerin performansını ölçmek için Doğruluk (Acc), Duyarlılık (Se) ve Özgünlük (Sp), Kesinlik (Pr) ve kafa karışıklığı matrisinden türetilen F-skor metrikleri kullanılmış ve metriklerin formülasyonları aşağıdaki gibidir:

$$\begin{cases} \mathrm{Acc} = \frac{(\mathrm{TP}+\mathrm{TN})}{(\mathrm{TF}+\mathrm{FN})+(\mathrm{FP}+\mathrm{TN})} \\ Se = \frac{(TP)}{(TP+FN)} \\ Pr = \frac{(TP)}{(TP+FP)} \\ F-score = \frac{(2\times TP)}{(2\times TP+FP+FN)} \end{cases} \tag{5.1}$$

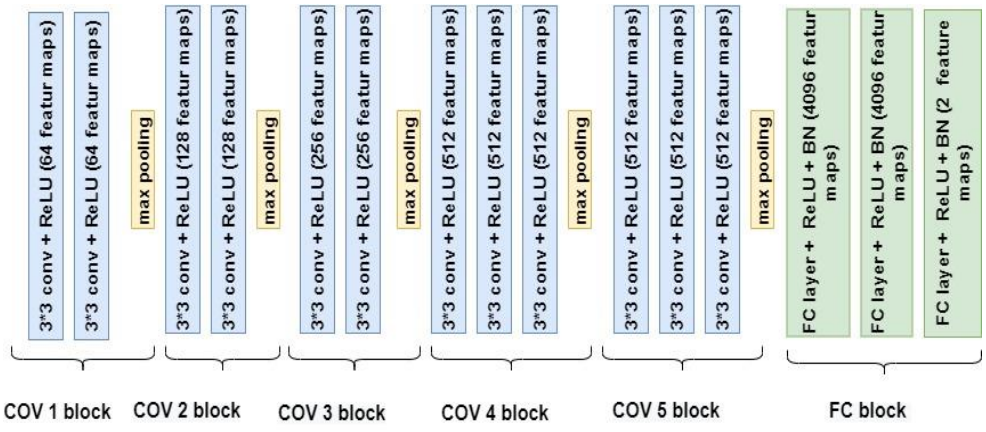
Yeni yaklaşımımızı son teknoloji yöntemlere göre değerlendirmek için aşağıdaki Denklemde Yarı Toplam Hata Oranı (HTER) formülünü uyguladık.

$$\mathrm{HTER} = \frac{FRR(\mathcal{K},\mathcal{D})+FAR(\mathcal{K},\mathcal{D})}{2} \tag{5.2}$$

FRR (K, D) yanlış bir reddetme oranı olduğunda, D kullanılan veri tabanını belirtir ve K, Eşit Hata Oranına (EER) göre tahmin edilir. Bu bağlamda FAR (K, D) Yanlış Kabul Oranı anlamına gelir.

5.1. Yüz Sahtekarlığı Tespiti İçin Derin Öğrenme Yaklaşımının Deneysel Sonuçları

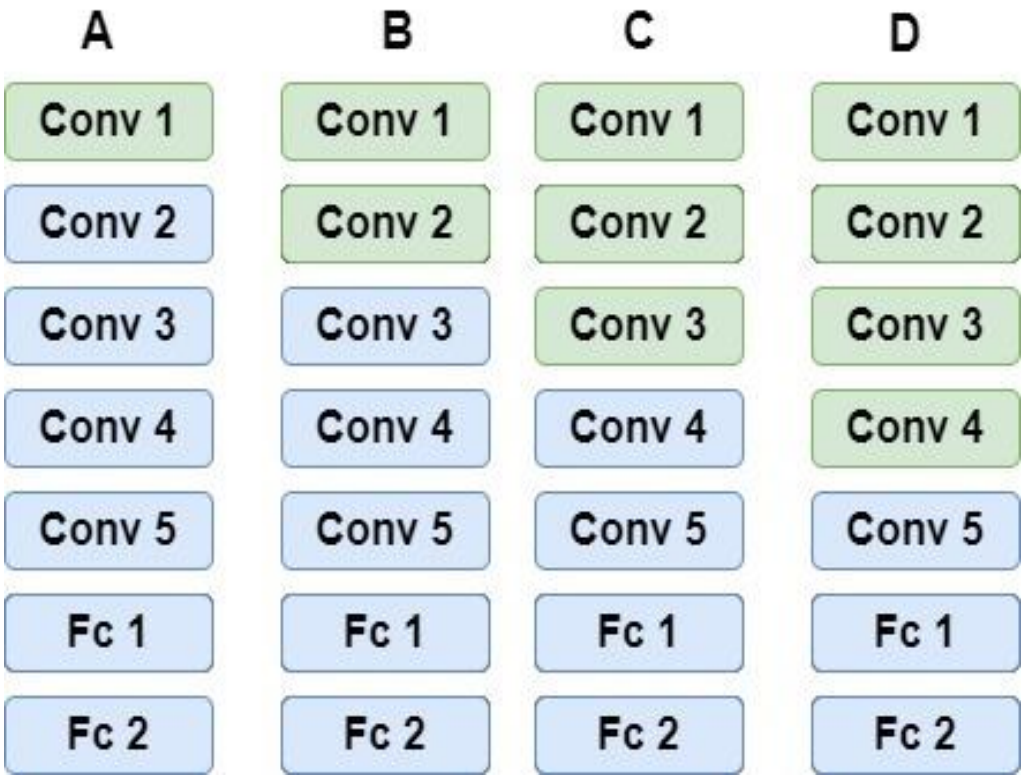
İlk adımlarda yüz sahtekarlığını tanıma yaklaşımımız VGG-Face modeline dayanıyordu. VGG-Face modeli, büyük bir yüz görüntüleri veritabanıyla eğitilir. Şekil 5.1.'da gösterildiği gibi, her bir evrişim bloğu, düzeltilmiş doğrusal birim (ReLU) fonksiyonunu ve 3x3 çekirdek boyutunu içerir. Ayrıca, her evrişim bloğu 2x2 çekirdek boyutuna sahip bir maksimum havuzlama katmanı içerir. ReLU fonksiyonu ve parti normalizasyonu ile 4096 kanallı iki FC katmanı ayarlanır. Son FC katmanı, ReLU işlevi, toplu normalleştirme ve bu katmanın çıktısının yüz sahtekarlığı tanıma etiketleri üzerinde kategorik dağılım sunduğu SoftMax etkinleştirme işlevini içerir.



Şekil 5.1. VGG-Face modelinin yapısı

Yüz sahtekarlığı algılama veritabanları için VGG-Face modelinin performansı, evrişimli blokların ince ayar seviyesine bağlıdır. Bu nedenle, bu testte, her bir önceden eğitilmiş evrişimli bloğun modelin doğruluğu üzerindeki etkilerini değerlendirdik [14]. A, B, C ve D modellerinin isimleri ile ağın parametrelerinin yeniden eğitilmiş ve dondurulmuş seviyelerine göre düzenlenen farklı modeller Şekil 5.2.'de sunulmuştur. Dönüş1, Dönüşüm2, Dönüşüm3 adlarıyla beş evrişim bloğu, Conv4 ve Conv5 ve iki

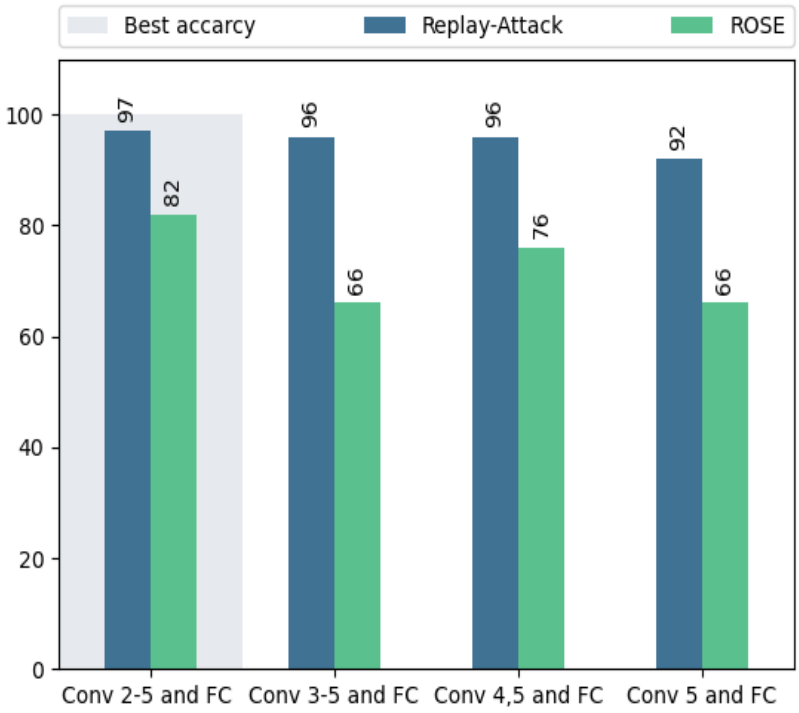
FC katmanı, ince ayar düzeyine göre eğitildi. Örneğin, ilk model (A) Conv2-5 ve FC katmanlarından oluşuyordu, bu da 2'den 5'e kadar olan evrişimli blokların yeni veri kümelerine göre eğitildiği ve modelin geri kalan parametrelerinin dondurulduğu anlamına geliyor. Aynı şekilde, B, C ve D modelleri sırasıyla üçüncü, dördüncü ve beşinci evrişimli bloklardan tamamen bağlı katmanla eğitilmiştir.



Şekil 5.2. Yeşil gölgeli bloklar dondurulur ve önceden eğitilir ve mavi gölgeli bloklar eğitim sürecinde yeniden eğitilir

Şekil 5.3.'de sunulan deneysel sonuçlara göre, en iyi doğruluk model A (Dönş 2-5 ve Fc katmanları) içindi. Gri gölgeleme ile vurgulanan Replay-Attack ve ROSE-Youtu veritabanları için sırasıyla% 97,99 ve% 82 ile . Tüm modeller (A, B, C ve D) Tablo 5.2.'de ve 1000 çağda sunulan parametrelere göre eğitilmiştir. Ek olarak, görüntülerin sınıflandırılması için, iki kanallı canlı ve sahte etiket ile SoftMax sınıflandırıcı kullanılmıştır. Sonuç olarak, tekrar-saldırı ve ROSE-YOUTU veritabanları için A modeli, sırasıyla (% 97,% 82) ile B (% 96,% 66), C (% 96,% 76) ile en iyi doğruluğu korudu.) ve D (% 92,% 66). Bu deneysel sonuçlara dayanarak, RGB renk uzayına dayalı sahtekarlık tespiti için, VGG-yüz modelinin optimum ince ayar seviyesinin,

tamamen bağlı iki katmana sahip 2'den 5'e kadar numaralandırılmış eğitimli evrişimli bloklar olduğu kanıtlanabilir. ve birinci evrişimli blok parametrelerini dondurarak.



Şekil 5.3. Ağların ince ayar seviyesine bağlı olarak VGG-Face modelinin doğruluğu

Bu durumda, RGB renk alanı için deneysel sonuçların geri kalanında, yüz sahtekarlığı tespiti için VGG-Face modeli için en iyi doğruluk oranında kalan aynı düzeyde ince ayar (model A) kullandık. Derin modelleri ROSE-Youtu veritabanıyla eğitmek için, eğitim için ilk 10 endekslenmiş veri örneğinden verilerin% 70'ini seçtik ve bunların geri kalanı doğrulama için kullanıldı. Bu durumda, eğitim ve doğrulama verileri tamamen ayrılmıştır. ROSE-Youtu veri tabanı saat yönünde ve saat yönünün tersine 90 derece gibi farklı dönüşlere sahip veriler içerdiğinden, Keras kütüphanesindeki görüntü verisi büyütme tekniği kullanılmıştır.

5.1.1. Renk tabanlı yaklaşım modeli

Bu bölümde, renk uzayını RGB'den HSV ve YCbCr'ye dönüştürme sürecini açıklıyoruz. Ayrıca, her bir renk uzayının sınıflandırmanın doğruluğu üzerindeki

etkilerini bulmak için üç karşılaştırmalı VGG modelini değerlendirdik. Bu testte, iki VGG16 modelini kullandık ve her ağın tamamını, varsayılan pencere boyutuna sahip sahtekarlık veri kümelerinden HSV ve YCbCr renk alanı görüntüleriyle eğittik. Tüm modeller, Tablo 5.2.'de ve 1000 çağda sunulan parametrelere göre eğitilmiştir.

Tablo 5.2. HSV ve YCbCr renk alanlarıyla önceden eğitilmiş VGG16 modellerinin ince ayarının deneysel sonuçları

Metrics %	HSV		YCbCr	
	Replay-Attack	ROSE-YOUTU	Replay Attack	ROSE-YOUTU
ACC	99.46	71.94	98.75	79.53
SE	99.25	77.42	99.25	88.61
SP	100	66.67	97.50	45.77
PR	99.47	71.87	98.75	83.75
F-score	99.47	71.87	98.75	71.03

HSV ve YCbCr renk uzayları üzerindeki deneysel sonuçları ve bu renk uzayları ile tüm ağların ince ayarının değerlendirilmesini göstermektedir. Elde edilen sonuçlara göre, Replay-attack veritabanındaki HSV renk alanı tabanlı görüntü, doğrulukta% 0,71 artırarak YCbCr renk uzayına kıyasla önemli sonuçlar elde etti. Bununla birlikte, ROSE-Youtu veritabanında, YCbCr alanı% 7,59 iyileştirerek HSV'ye kıyasla daha iyi sonuçlar sağlamıştır. Bu sonuçlara göre, aydınlatma değişiklikleri ve yüksek çözünürlüklü kamera görüntüleme gibi farklı koşullar altında yüz sahteciliği tanıma için her iki renk alanının da farklı senaryolarda canlı bir görüntüyü sahte yüzden ayırt etmeye yardımcı olabilecek ayırt edici özellikler içerdiği sonucuna varılabilir.

5.1.2. Derin özellik çıkarma

Deneysel prosedürümüzün ikinci adımlarında, 4096 kanalı içeren RGB renk uzayına dayalı önceden eğitilmiş VGG-yüz modelinin tamamen bağlı katmanının (FC7) özellikleri çıkarıldı. Bu katmandan çıkarılan özellikler, SVM, LDA ve KNN gibi farklı tipik sınıflandırıcılarla sınıflandırıldı. Ayrıca, bu sonuçlar, çıkarılan derin özelliklerin performansını diğer sınıflandırma algoritmalarıyla değerlendirmek için SoftMax sınıflandırıcısı ile karşılaştırılmıştır.

Tablo 5.3. Sınıflandırma sonuçları, farklı sınıflandırıcılara ve VGG-yüz modelinin derin özelliklerine dayanmaktadır.

Model	Database	Classification	ACC %	SE %	SP %	PR %	F-score %
VGG-Face (RGB Color space)	Replay Attack database	SoftMax	97.32	99.25	99.50	97.34	97.30
		SVM	98.93	98.50	100	98.97	98.93
		LDA	98.91	98.91	100	99.78	99.78
		KNN (K=1)	98.93	98.50	100	98.97	98.93
	ROSE-Youtu	SoftMax	82.84	97.42	72.41	89.52	88.00
		SVM	78.38	59.75	90.03	78.46	77.65
		LDA	70.30	50.13	82.91	69.61	69.39
		KNN (K=1)	78.38	59.75	90.03	78.46	77.65

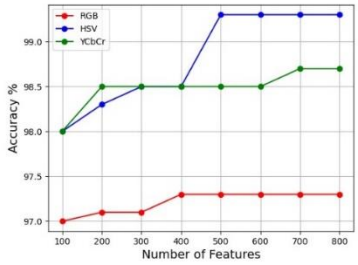
Tablo 5.3.'te gösterilen deneysel sonuçlara göre, en iyi sonuçlar 98.93 (ACC), 98.50 (SE), 100 (SP), 98.97 (PR) ve% 98.93 (F-Score) ile Replay-attack veritabanında SVM ve KNN için olmuştur.Replay-Attack veritabanında, SoftMax sınıflandırıcı, sonuçlara göre diğer sınıflandırıcılar arasında dördüncü aşamaya yerleştirildi. Bununla birlikte, ROSE-Youtu veritabanında, SoftMax sınıflandırıcı diğer sınıflandırıcılara göre 82.84 (ACC), 97.42 (SE), 72.41 (SP), 89.52 (PR) ve% 88.00 (F-scor) ile önemli sonuçlar elde etmiştir.

5.1.3. Özellik seçimi ve sınıflandırması

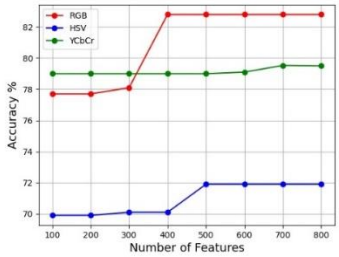
Bu adımda, üç farklı modelden çıkarılan özelliklerin boyutunu azaltmak ve sağlam ve ayırt edici özellik kümeleri seçmek için mRMR'yi kullandık. Her model için çıkarılan özelliklerin boyutu 4096 idi ve bu üç VGG modeli birleştirilerek boyut 12288 özelliğe çıkarıldı. Özellik setlerinin optimum boyutunu bulmak için, Şekil 5.4.'da (A&B) sunulan mRMR özellik seçimi yardımıyla farklı boyutlardaki özellikleri analiz ettik. Sonuçlara göre, tekrar-saldırı için en iyi özellik boyutları 400, 500 ve 700 idi ve ROSE-Youtu veritabanı için olanlar, LR sınıflandırıcısına dayalı RGB, HSV ve YCbCr için sırasıyla 300, 500 ve 700 idi. Bu durumda, hem veri tabanlarını hem de tüm renk alanlarını kapsayan optimum özellik boyutu 1600 özelliğe ayarlanabilir. Bu testin devamında, HSV renk uzaylarının derin özelliklerinin doğruluk oranlarının iyileştirilmesi üzerindeki etkilerini analiz ettik. Bu durumda, önceden eğitilmiş VGG yüz modelinin (RGB) FC7 katmanından çıkarılan özelliği VGG16 modeli (HSV) ile birleştirdik. Tablo 5.4.'te sunulan deneysel sonuçlar, yüz sahtekarlığı algılama

yaklaşımının doğruluğunun Replay-attack veritabanında büyük ölçüde iyileştirildiğini göstermektedir.

Tablo 5.4. Farklı boyutlardaki özelliklere göre LR sınıflandırmasının doğruluğu



Replay-attack



B. ROSE-Youtu

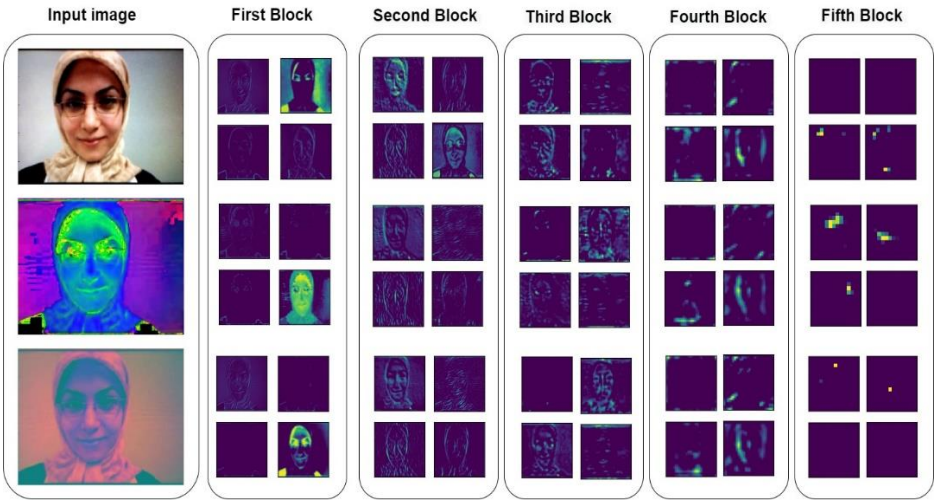
Bu veritabanında, LR, SVM ve KNN sınıflandırıcıları ile tüm değerlendirme metrikleri,% 99,82 (ACC), 99,75 (SE), 100 (SP), 99,82 (PR) ve% 99,82 (F-skor) ile önemli oranlarda kaldı. ROSE-Youtu veri tabanında ayrıca tüm değerlendirme ölçütleri dört farklı sınıflandırıcı ile geliştirilmiş ve doğrusal regresyon sınıflandırıcı için en iyi sonuçlar 95.98 (ACC), 99.00 (SE), 93.24 (SP), 95.98 (PR) ve 95.98 (F-skor)%. Tablo 5.5. ile karşılaştırıldığında bu tablodaki deneysel sonuçlar, HSV derin özelliklerinin sahtekarlık verilerinin tespitinin etkinliğini artırdığını göstermiştir. Tablo 5.6. ve 5.5.'in iki deneysel sonucunun karşılaştırılması, HSV derin özellikleri ile VGG-Face derin özellikleri birleştirilerek tüm değerlendirme ölçütlerinin iyileştirildiğini ve bu sonuçların 13.14 (ACC), 1.58 (SE), 20.83 (SP) ile iyileştirildiğini gösterdi. ROSE-Youtu veritabanındaki LR sınıflandırıcısına dayalı olarak 6.46 (PR) ve 7.98 (F-skor).

Tablo 5.5. RGB ve HSV'den çıkarılan özelliklerin sınıflandırma sonuçları.

Model	Databases	Classification	ACC %	SE %	SP %	PR %	F-score %
VGG-Face (RGB) + VGG16 (HSV)	Replay Attack database	LR	99.82	99.75	100	99.82	99.82
		SVM	99.82	99.75	100	99.82	99.82
		LDA	98.75	99.50	96.88	98.75	98.75
		KNN (K=1)	99.82	99.75	100	99.82	99.82
	ROSE-YOUTU	LR	95.98	99.00	93.24	95.98	95.98
		SVM	95.98	97.51	94.59	96.04	95.98
		LDA	83.34	77.11	92.79	85.97	85.22
		KNN (K=1)	94.79	97.51	92.34	94.96	94.80

Tablo 5.6.'da, özellik seçimi yöntemi uygulanarak önerilen derin modelin deneysel sonuçları sunulmuştur. VGG modellerinden farklı renk uzaylarından çıkarılan üç özelliğin birleştirilmesinden sonra, mRMR özellik seçimi uygulandı. Bölüm 3'te

tartışıldığı gibi, mRMR algoritmasını uygulamanın ana nedenleri, ilgisiz özellikleri azaltmak ve sağlam ve ayırt edici özellikleri seçmekti. Şekil 5.4., RGB, HSV ve YCbCr renk uzaylarıyla her beş evrişimli bloğun ilk dört özellik haritasının görselleştirmesini sunar. Her bir evrişimli blok ve özellikle beşinci evrişimli bloklardan çıkarılan özelliklere göre, her modelden gelen özelliklerin farklı renk uzayları ile birleştirilmesinin, önerilen yaklaşımımızın etkinliğini azaltan gereksiz ve ilgisiz özellikler içerdiği elde edilmiştir. Şekil 5.4.'daki bu sonuçlara dayanarak, çıkarılan YCbCr özellikleri, tekrar-saldırı veritabanındaki değerlendirme ölçütlerini iyileştiremez. Bununla birlikte, diğer yandan bu özellikler, ROSE-Youtu veri tabanında sahtekarlık verilerinin tanınmasının etkinliğini artırmış ve sonuçları 1.18 (ACC), 2.91 (SP), 2.25 (PR) ve 1.19 (F-skor) tabanlı olarak artırmıştır. LR sınıflandırıcı üzerinde. Ek olarak, doğrusal regresyon sınıflandırıcı, SVM, KNN ve LDA ile karşılaştırıldığında en iyi sonuçlarda kaldı.



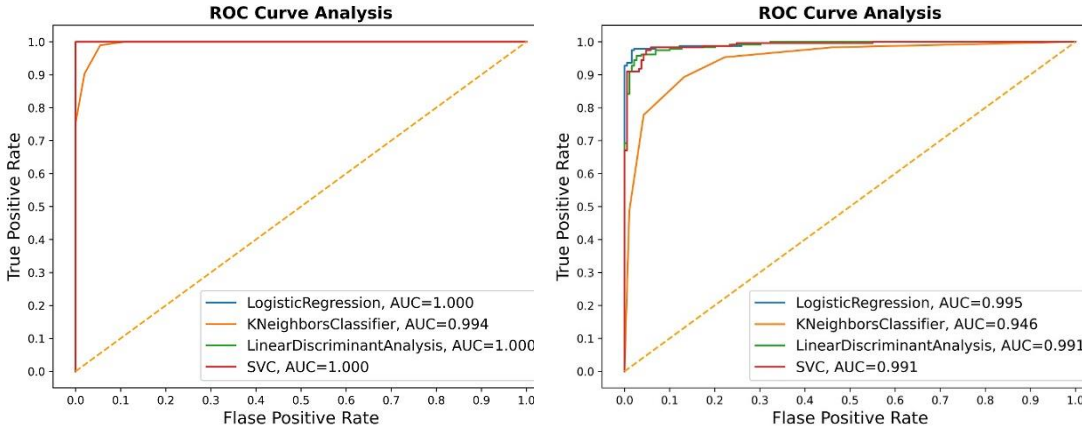
Şekil 5.4. Her evrişimli bloktan çıkarılan özellikler haritaları

Sonuçları daha iyi sunmak için, Şekil 'de gösterildiği gibi her iki deney veritabanı için de ROC eğri analizini kullandık. ROC eğri analizi, önerilen yaklaşımın RGB, HSV ve YCbCr renk uzaylarında iyi bilinen önceden eğitilmiş modellerin yardımıyla gösterdi. sahte yüz görüntülerinin tespiti için ayırt edici özellikler çıkarıldı. Bu sonuçlara dayanarak, LR sınıflandırıcılar, ROSE-Youtu (Şekil 5.5.b.) ve Replay-attack veritabanları (Şekil 5.5.a.) için sırasıyla 0,995 ve 1,00 oranında diğer belirtilen sınıflandırma algoritmalarına kıyasla en iyi AUC'de kaldı. Bu durumda, önerilen

yaklaşımımız için temel sınıflandırma algoritması olarak LR sınıflandırıcısını seçtik ve bu sınıflandırma algoritmasını makalenin geri kalanında kullandık.

Tablo 5.6. RGB ve HSV ve YCbCr'den çıkarılan özelliklerin sınıflandırma sonuçları

Model	Databases	Classification	ACC %	SE %	SP %	PR %	F-score %
VGG-Face (RGB) + VGG16 (HSV) + VGG16 (YCbCr)	Replay Attack database	LR	99.82	99.75	100	99.82	99.82
		SVM	99.82	99.75	100	99.82	99.82
		LDA	98.75	99.50	96.88	98.75	98.75
		KNN (K=1)	99.82	99.75	100	99.82	99.82
	ROSE-YOUTU	LR	97.16	98.41	96.15	97.21	97.17
		SVM	95.98	93.12	98.29	96.05	95.97
		LDA	96.45	97.73	95.73	96.49	96.46
		KNN (K=1)	88.17	86.77	89.32	88.18	88.18



Replay-attack ROSE-Youtu

Şekil 5.5. Farklı sınıflandırıcılara dayalı ROC eğrisi analizi.

5.1.4. Farklı saldırıları değerlendirme

Önerilen yaklaşımımızın farklı sahtekarlık saldırısı senaryolarında değerlendirilmesi ve önerilen yaklaşımımızın avantaj ve dezavantajlarını bulmak için derin öğrenme yaklaşımımızı farklı saldırılarda ayrı ayrı test ettik. Replay-attack ile ilgili deneysel sonuçlara göre (Tablo 5.6.), önerilen yaklaşımımızın Replay-attack veritabanında sunulan replay, display ve print saldırılarında tatmin edici sonuçlar verdiği sonucuna varılabilir. Yanlış sınıflandırma nedenlerini bulmak için bu testte sahtekarlık senaryolarının ayrı ayrı analiz edildiği ROSE-Youtu veritabanında. ROSE-Youtu veritabanını, Şekil 5.6.'de gösterildiği gibi kişilerden videolar içeren gerçek, göster ve yazdır, kırpmalı maske ve kırpmadan maske gibi beş farklı gruba ayırdık. Görüntüleme

ve yeniden oynatma saldırıları halihazırda farklı koşullarda test edilmiştir. Replay-attack adlı deneysel veri tabanlarında ışık değişimi ve tokalaşma gibi. Görüntü saldırısı ve yazdırma saldırısı kategorilerini birlikte belirledik ve Görüntü olarak etiketledik. Bununla birlikte, ROSE-Youtu veritabanının temel farkı, diğer deneysel veritabanlarında bulunmayan farklı koşullar ve senaryolarda maske saldırısıdır.

a. Display b. with cropping c. without cropping d. Replay

Şekil 5.6. ROSE-Youtu veritabanının sahtekarlık saldırılarının sınıflandırılması

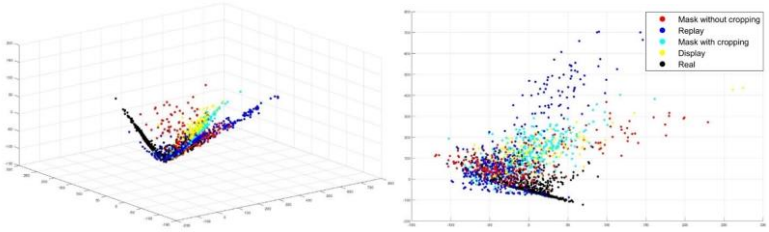
ROSE-Youtu veritabanındaki maske saldırısı, iki gözü ve ağzı kırpılmış maske, kırpılmamış maske, üst kısmı ortadan kesilmiş maske ve alt kısmı ortadan kesilmiş olarak maske gibi senaryolar içerir.

Bu testte bu maske saldırı senaryolarını kırpmadan maske ve kırparak maske olarak iki ana gruba ayırdık. Tablo 5.7.'de sunulan deneysel sonuçlara göre, önerilen yaklaşımın temel avantajının görüntüleme ve yazdırma saldırıları gibi sahtekarlık saldırılarının tespiti olduğu ortaya çıktı. Görüntüleme ve yazdırma saldırılarının tanınmasının doğruluğu% 98.00 idi ve bu, diğer sahtekarlık verileriyle karşılaştırıldığında en yüksek değerde kaldı. İkinci en yüksek doğruluk değeri,% 97,82 doğrulukla kırpma saldırıları ile maskelerdi. Tekrar saldırılarının sonuçları da% 94.64 doğrulukla uyumluydu. Öte yandan, en düşük sonuçlar 92.59 (ACC), 96.81 (SE), 98.93 (SP), 92.70 (PR) ve 92.33 (F-skor) ile kırpmasız maske için oldu. Bu sonuçlar, önerilen yaklaşımın görüntü ve basılı saldırının tanınmasında önemli bir doğruluğa ve kırpma senaryoları olmadan maskede uyumlu doğruluğa sahip olduğunu kanıtladı.

Tablo 5.7. ROSE-Youtube veritabanında farklı saldırı türlerini değerlendirme

Database	Types of attacks	ACC %	SE %	SP %	PR %	F-score %
ROSE-Youtu	Mask without cropping	92.59	96.81	98.93	92.70	92.33
	Replay Attack	94.64	90.99	96.81	94.64	94.63
	Mask with cropping	97.82	95.83	98.89	97.83	97.82
	Display and print attack	98.00	96.46	98.93	98.00	98.00

Bu testin devamında, saldırı gruplarına ve gerçek videolara dayalı olarak çıkarılan özelliklerin dağılım grafiğini kullandık. Bu bölümde, test setinden her videodan bir kare seçtik ve her bir görüntü ve sunum için X, Y ve Z değerlerini elde etmek için Temel Bileşen Analizi (PCA) yardımıyla özelliklerin boyutlarını 1600'den 3'e düşürdük. onları 3B dağılım grafiklerinde. Şekil 5.7.'te sunulduğu gibi, kırpma ve yeniden oynatma saldırı özellikleri içermeyen maskenin gerçek video kareleriyle örtüştüğü ortaya çıktı. Ayrıca, kırpma ile görüntüleme ve maske gibi diğer sahtekarlık saldırıları, gerçek videolardan açıkça ayrıldı.

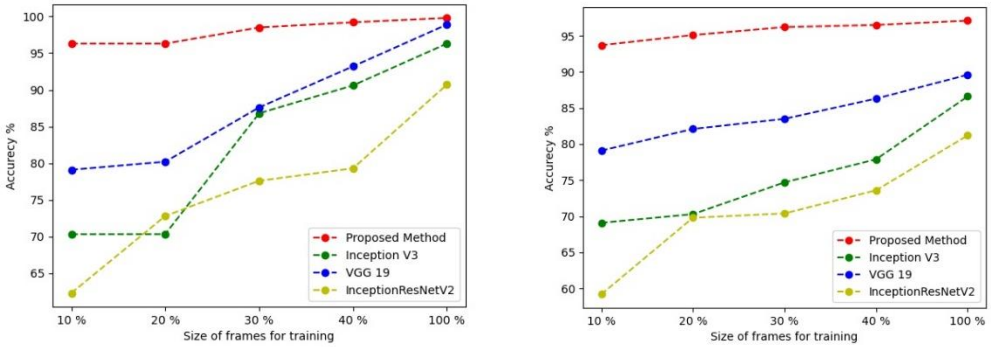


Şekil 5.7. Saldırılara dayalı özelliklerin 3B ve 2B dağılım grafiği.

5.1.5. Bulut sisteminde önerilen yöntemin değerlendirme verimliliği

Daha önce de belirtildiği gibi, bulut bilişim sistemlerinin temel sorunlarından biri, veri depolama ve kaynağı optimize etme yönetimleridir. Bu nedenle, daha az veriyle çalışan ve mevcut modellere kıyasla doğruluğa dayalı önemli sonuçlar elde eden bir derin öğrenme yaklaşımı önerdik. Yaklaşımımızı değerlendirmek için modeli dört farklı türde eğitiyoruz. İlk olarak, modeller her videonun karelerinin% 10'u üzerinde eğitilir ve tüm karelerde test edilir. İkinci, üçüncü ve dördüncü değerlendirme modu, test setlerinin tüm çerçevelerinde eğitim ve değerlendirme için çerçevelerin% 20, 30 ve% 40'ı gibi aynı koşuldadır. Bu senaryolar RGB renk uzayında Inception V3 [89], InceptionResNetV2 [90] ve VGG 19 [71] gibi iyi bilinen derin öğrenme modelleri üzerinde test edilmiştir. Image net veritabanındaki bu önceden eğitilmiş modeller, derin bir özellik çıkarıcı olarak kullanılır. Yüz sahtekarlığı veritabanıyla bu modellerde parametrelerin ince ayarını yapmak için, SoftMax sınıflandırma katmanını iki sınıf sahtekarlık ve gerçek yüz olarak değiştirdik. Ayrıca tüm modeller için 0.0001 ile az sayıda öğrenme hızı belirlendi, ayrıca Adam optimizasyonunu, parti boyutu 16 ve 10000 epoch'u kullandık. 30 fps'de 720p çözünürlükte bir dakikalık video

yakaladığımızı varsayalım, yaklaşık 60 MB olan 1800 kare içerir. Bu nedenle, her videonun karelerinin% 10'unu içeren eğitim modeli ile, yalnızca eğitim için veri boyutunu (yaklaşık 6 MB) değil, aynı zamanda eğitim aşamasında hesaplama maliyetini de düşürdü.



Replay attack ROSE-Youtu

Şekil 5.8. Sınıflandırmanın doğruluğu üzerine farklı boyutlardaki eğitim verilerinin değerlendirilmesi

Şekil 5.8.'te sunulan deneysel sonuçlara göre, önerilen yöntemin derin öğrenme yöntemlerini kıyaslama yöntemlerine kıyasla daha az eğitim verisi ile sahtekarlık saldırısının tespit edilmesinde önemli sonuçlara ulaştığı görülmektedir. Önerilen yöntem, videoların tamamında eğitim ve test için her videonun karelerinin yüzde onunda% 96,3 ile sınıflandırma doğruluğunu elde etti; bu puan, Inception V3, InceptionResNetV2 ve VGG 19 tarafından 70.32, 62.3 ile elde edilen sonuçlardan daha iyi ve Replay saldırı veritabanında sırasıyla 79.1. Önerilen yöntemin sonuçları% 96.3,96.3, 98.5, 99.2 ve 99.8'dir ve bu, Replay saldırı veritabanındaki her videonun karelerinin% 10'u, 20'si, 30'u, 40'ı ve% 100'ü için diğer deneysel derin öğrenme yöntemlerinden daha iyidir. Aynı durumda, ROSE-Youtu veritabanında da önerdiğimiz yöntem, eğitim için her videonun 10, 20, 30 ve 40 karelerinde yüzde 93.7,95.1, 96.2, 96.5 ile en iyi sonuçlarda kaldı.

5.1.6. Önerilen IOT yaklaşımının son teknoloji algoritmalarla karşılaştırılması

Tablo 5.8., önerilen yaklaşım ile son teknoloji yöntemler arasında bir karşılaştırma sağlar. Tablo 5.8.'de gösterilen deneysel sonuçlar, tekrar-saldırı veri tabanında çıkarılan derin özelliklerimizin etkinliğini göstermiştir.

Tablo 5.8. Önerilen yaklaşımın Replay-attack veritabanına dayalı son teknoloji algoritmalarla karşılaştırılması

Method	EER (%)	HTER (%)
Motion + LBP [46]	4.5	5.1
DMD [47]	3.8	5.3
SURF color texture [13]	1.2	4.2
color texture [14]	0.4	2.8
LBP net [70]	0.6	1.3
Color LBP [27]	0.9	4.9
Partial CNN [30]	2.9	4.3
CompactNet [15]	0.8	0.7
Dense optical flow + Shearlet [44]	0.83	0.0
Proposed method	0.2	0.4

Bu tabloda sunulan son teknoloji yöntemler arasında en iyi sonuçların 0.6 (EER) ve 1.3 (HTER) ile LBP ağı [70] gibi derin öğrenmeye dayalı yöntemler için olduğunu gözlemleyebiliriz. En iyi HTER 0,0 ile Yoğun optik akış + Shearlet [44] içindi. Ayrıca, önerdiğimiz yöntem 0.2 (EER) elde etti ve bu, daha önceki bir çalışmada [15] önerilen çoklu işaret derin yönteminden tek bir işaretle (renk dokusu analizi) daha iyi oldu.

Bu deneysel sonuçlara göre, önerdiğimiz yaklaşımın daha uygulanabilir olduğu ve replay-attack veritabanındaki son teknoloji yöntemlere kıyasla en iyi EER (%) değerlerinde kaldığı söylenebilir. Diğer karşılaştırmalı genel erişim veri tabanında (ROSE-Youtu), önerdiğimiz yaklaşım da en iyi ERR (%) değerlerinde kaldı. Bu veri tabanında, son teknoloji algoritmalardaki en iyi EER, önerdiğimiz yaklaşımımızın EER değerini% 0,76 oranında iyileştirdiği iki aşamalı derin model [42] yaklaşımı içindi. Bu deneysel sonuçlara ve son teknoloji algoritmalarla karşılaştırmaya dayanarak, önerilen yaklaşımımızın, tekrarlarda EER (%) için 0,2 ve 3,8 ile sahte yüzleri canlı yüzlerden ayırmada sağlam ve anlamlı sonuçlar elde ettiği sonucuna varılabilir -attack ve ROSE-Youtu veritabanları sırasıyla.

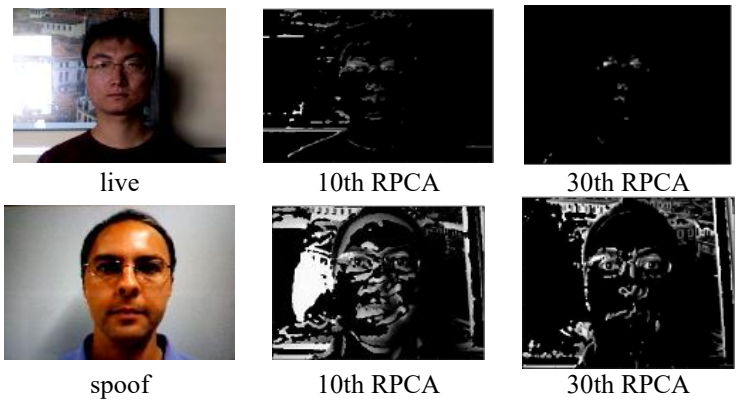
Tablo 5.9. Önerilen yaklaşımın ROSE-Youtu veritabanına dayalı son teknoloji algoritmalarla karşılaştırılması.

Method	EER (%)
Deep color-based feature [86]	8.0
SE-ResNet 18 [91]	7.2
3D CNN [92]	7.0
Two stage deep model [93]	4.56
Proposed method	3.8

5.2. RPCA Deneysel Sonuçlar ve Tartışmalar Yüz Sahteciliği Tespiti

Önerdiğimiz yaklaşımın değerlendirilmesi için iki yüzlü kimlik sahtekarlığı kamu veritabanı, Replay saldırısı, vahşi yaşamda kimlik sahtekarlığı ve OULU-NPU veritabanları kullanılmıştır. Bu veritabanlarının detayları aşağıdaki gibidir;

Video işlemedeki temel zorluklardan biri, sahnedeki arka plan varyasyonu (düşük rütbe) için iyi bir model tahmin etmektir. Bu senaryoların ana sorunları ön plandadır, nesnelerle taşan duyu veya aydınlatma gibi değişiklikleri barındıran arka plan gibi bir anomali için esnek olmalıdır. Bu çalışmada, seyrek matris ile düşük dereceli matrisin ayrılması problemleri, hatanın mekansal yapısı gibi herhangi bir ek bilgi kullanılmadan ana bileşen analizi yardımıyla çözülmüştür. Belirli saldırı türlerine sahip Replay saldırı veritabanlarından iki farklı video dikkate alınmıştır. Şekil 5.9., canlı senaryoda düşük dereceli matris ile seyrek matrisin ayrılmasını gösterir (Şekil 5.9. (ac)) ve bu durumda, düşük dereceli matris, vurgulanan dinamik değişiklikleri üretmek için kolayca hesaplanabilir Şekil 5.9.'teki (b'den c'ye) her çerçevede göz kırpma ve dudak hareketi olarak görünürler.



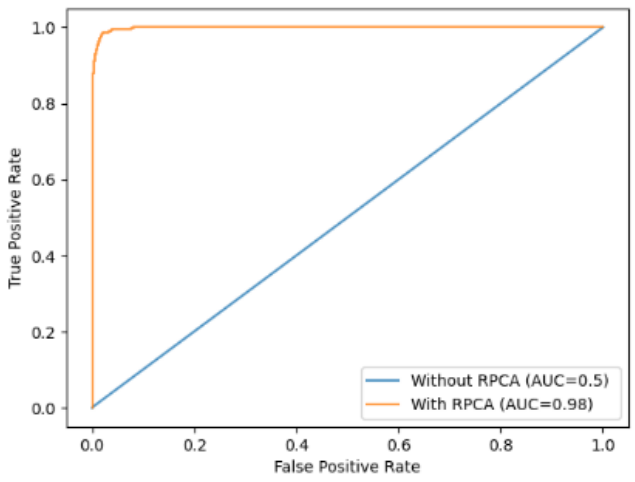
Şekil 5.9. Kontrollü senaryo içeren bir parodi videoyu gösterir.

Kimlik sahtekarlığı saldırılarında video bilgilerinin yeniden yakalanması sırasında, hem renk hem de doku bozuldu ve bunun nedeni baskı kalitesi kusurları, ışığı yansıtan baskılar, farklı aynasal yansımalar ve çeşitli nedenlerden kaynaklanıyordu. Bu nedenle, RPCA, Şekil 5.9. (ef) 'de gösterildiği gibi, düşük kalan ve seyrek adres sahteciliği video matrisini ayıramadığı için büyük miktarlarda işe yaramaz özellikler

içerecektir; videolar. Kimlik sahtekarlığı saldırılarında video bilgilerinin yeniden yakalanması içindir, hem renk hem de doku bozuldu ve bunun nedeni baskı kalitesi kusurları, ışıktan baskılar, farklı aynasal yansımalar ve gölgeler gibi çeşitli nedenlerden kaynaklanıyordu. Bu sayfada, RPCA, Şekil 6.9.(ef) 'de kullanılır gibi, düşük kalan ve seyrek adres sahteciliği video matrisini ayıramadığı için büyük miktarlarda işe yaramaz özellikler içerecektir; videolar. Şekil 5.10.'da, tekrar oynatma saldırısı veritabanlarındaki bu deneysel sonuca dayanarak, RPCA algoritması ile sırasıyla 0.985 ve ROCA'nın ROCA olmadan Alan için RPCA olmadan 0,50 puan aldı. Önerdiğimiz yaklaşımda RPCA'nın sevgisi hakkında daha fazla ayrıntı elde etmek için kesinlik, hatırlama, f1 skoru metrikleri uygulanır. Tablo 5.10.'e dayanarak, DBN modeli, hem sahte hem de gerçek (Sunum) videolar için RPCA senaryosu olmadan karşılaştırılan RPCA algoritmasının düzgün şekilde ayıklanan özelliklerini algılayabilir ve hassasiyet ve f1 için hassasiyet, geri çağırma ve f1-puan ölçümlerini (0.41, 0.25) Gerçek videolar için -score ve aynı şekilde, f1 puanı için (0.99, 0.99) geliştirin ve Spoofing sınıfında hatırlayın.

Tablo 5.10. Yeniden saldırı veritabanında RPCA olan ve olmayan karşılaştırma metrikleri.

	Class	Precision	recall
With RPCA	Spoof	1.00	0.00
	Real	0.56	1.00
Without RPCA	Spoof	0.99	0.99
	Real	0.97	0.98



Şekil 5.10. Replay saldırı veritabanında RPCA olan ve olmayan ROC eğrisi.

5.2.1. Tekrar saldırı veritabanında önerilen yaklaşımın sonuçları

Tablo 5.11., en yeni yöntemlerle ve önceden eğitilmiş mevcut derin öğrenmeye karşı bir karşılaştırma sunmaktadır. Önerilen yaklaşımımızla yöntemler. Önerilen yaklaşımımızın Replay-Attack veritabanındaki en gelişmiş yöntemlerden daha iyi performans gösterdiği görülmektedir. Bu tablodaki sonuçlarda gösterildiği gibi, en iyi Hata eşit oranı (EER)% 2,4 ile LBP [40] ve% 2,1 ile Derin CNN [30] idi; bu değerler önerilen yaklaşım sonuçlarına eşit veya çok yakındı , ancak HTER'miz karşılık gelen değerlerini% 3.1'den% 2.8'den% 1.2'ye düşürdü.Bu durumda, önerilen yöntemimiz tekrar saldırı veri kümesinde en iyi HTER'i verdi.

Tablo 5.11. Replay saldırı veritabanında önerilen yöntemin en gelişmiş yöntemlerle karşılaştırılması

Methods	EER (%)	HTER (%)
Motion + LBP [46]	5.6	4.2
Motion [94]	12.9	12.7
LBP [85]	15.2	13.5
LBP-TOP [39]	6.1	6.3
LDP-TOP [29]	2.9	2.6
DMD [47]	4.3	2.2
Scale LBP [95]	2.4	3.1
Color LBP [13]	2.6	2.8
Deep CNN [17]	2.1	2.8
Partial CNN [30]	3.1	2.3
Our proposed method	1.8	1.2

5.2.2. SIW veritabanında önerilen yaklaşımın sonuçları

farklı senaryolarda önerilen yaklaşımımızın doğruluğunu kanıtlamak için SIW veritabanı üç farklı protokol ile test edilmiştir. Yardımcı [88], STASN [96], SAPLC [43] yöntemleri ve önerilen RPCA-DBN Tablo 5.12.'daki SiW protokolleri ile denenmiştir. STASN [97] ilk protokolde% 1.00 (ACER) ile önemli sonuçlar elde etmiştir. Ayrıca, geçici yaklaşım modelini öğrenmenin, ilk yaklaşımda önerilen oranımız bu orana% 0,44 kadar yakındır. Yaklaşımımız sırasıyla% 0.24 ve% 3.57 ile ikinci ve üçüncü protokollerde en iyi ACER (%) üzerinde kalmaktadır. Yaklaşım sıralarımız I, II ve III protokollerinde sırasıyla ikinci, birinci ve ilk sıradadır ve en son teknoloji algoritmalarla karşılaştırılır.

Tablo 5.12. Önerilen yöntemin SIW veritabanındaki en son yöntemlerle karşılaştırılması

#	Model	ACER (%)	APCER (%)	BPCER (%)
Protocol 1	Auxiliary [88]	3.58	3.58	3.58
	STASN [96]	1.00	-	-
	SAPLC [97]	2.94	2.87	3.01
	Proposed approach	1.44	1.68	1.2
Protocol 2	Auxiliary [88]	0.57 ± 0.69	0.57 ± 0.69	0.57 ± 0.69
	STASN [96]	0.28 ± 0.05	-	-
	SAPLC [97]	0.38 ± 0.10	0.43 ± 0.16	0.33 ± 0.14
	Proposed approach	0.24 ± 0.12	0.27 ± 0.15	0.21 ± 0.11
Protocol 3	Auxiliary [88]	8.31 ± 3.81	8.31 ± 3.81	8.31 ± 3.81
	STASN [96]	12.10 ± 1.50	-	-
	SAPLC [97]	7.73 ± 1.05	7.78 ± 1.15	7.68 ± 0.94
	Proposed approach	3.57 ± 1.54	4.32 ±1.23	2.83 ± 1.86

5.3. Önerilen Hibrit IDS Çıkarım Sisteminin Karışıklık Matrisi

Karışıklık matrisi, statik verilerin analizi için hata matrisi olarak bilinir. Bu makalede olduğu gibi, hibrit çıkarım sistemi, Suricata saldırı tespit sistemi veya saldırı önleme sistemleri için imza oluşturma ve anormallik tabanlı trafik analizi için kullanılır. Yerel olarak geliştirilen laboratuvarda SQLi, XSS, Windows işletim sistemindeki güvenlik açıklarından yararlanma, Hedeflenen ağa Dağıtılmış Hizmet Reddi (DDoS) saldırısı gibi çeşitli saldırı türleri başlatıldı. Bahsedilen bu saldırılar, hedeflenen ağ için önerilen sistem tarafından önlenir. Sonuçların değerlendirilmesi için, aşağıdaki Tablo 5.13.'te tanımlandığı gibi karışıklık matrisi kullanılmıştır.

Tablo 5.13. IDS için Hibrit Çıkarım Sisteminin Karışıklık Matrisi

	Norm	*SQLi*	*XSS*	*Windows OS Attacks*	*DDoS*	*Classification Overall*	*Precision*
Normal	*500*	*0*	*0*	*0*	*0*	*500*	*100%*
SQLi	*0*	*900*	*50*	*0*	*50*	*1000*	*90%*
XSS	*0*	*0*	*925*	*25*	*50*	*1000*	*92.5%*
Windows OS Attacks	*0*	*0*	*0*	*1000*	*0*	*1000*	*100%*
DDoS	*0*	*0*	*0*	*0*	*1000*	*1000*	*100%*
Truth Overall	*500*	*900*	*975*	*1025*	*1100*	*4500*	
User Accuracy	*100 %*	*100%*	*94.872%*	*97.561%*	*90.909%*		

Genel Doğruluk =% 96.111 elde edilir.

Suricata IDS / IPS tarafından ağ trafiği algılamasının yanlış pozitif oranı nedeniyle% 96.11 sistem doğruluğuna ulaşılamadı. Bu belgede önerilen çözümün sonuçları,

hedeflenen ağa yönelik saldırıların tespit veya önlenmesinde genel olarak iyi bir doğruluk gösterdiğinden. Önerilen bu sistemin sınırlamaları, sınırlı veri setlerine göre olmasıdır. Ayrıca, önerilen bu sistem, zayıf işletim sistemleri ve bu testlerin çok uygulandığı uygulamalar için oluşturulmuş bir sanal sistem laboratuarında konuşlandırılmıştır. Algoritmanın çalışma süresi, önerilen sistemden beklenen yanıt dahilindedir. Büyük veri kümeleri için bu sistem gecikme ile karşılaşabilir, ancak gelecekte yanıt süresini gerekli zaman sınırları içinde iyileştirmek için optimize edebilir. Bu makalenin geçmiş alanlarında önerilen stratejiye göre, başlangıçta ekstrema üzerinde bulanık model üretin.

her düzeltme. Çerçeve yürütme ve kural karmaşıklığı arasında iyi bir uyum sağlamak için, farklı düzeltme boyutları ve benzerlik sınırları denenir. Çeşitli düzeltme boyutlarını kullanan sonraki kabarık çerçeveler, kural karmaşıklığı ve yakındaki tahmin hatasıyla değerlendirilir. Bu araştırmada olduğu gibi, önerilen sistem üzerinde test edilen farklı veri kümeleri ve saldırı türleri vardır. En iyi bilgiye göre bu tür işler daha önce yapılmadı.

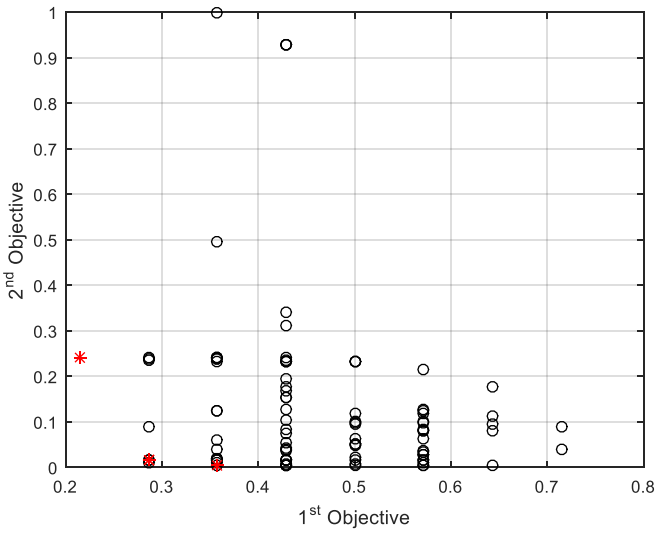
5.4. Çok Amaçlı Parçacık Sürüsü Algoritmasına dayalı Özellik Seçimi ve IDS için Hızlı Öğrenme Ağı

Önerilen yöntemde, birincil parçacıklar ilk olarak KDD-CUP veri setinden rastgele seçilir. İlk popülasyonun boyutu, veri kümesinde bulunan özelliklerin sayısı ve n boyutlu bir vektör olarak tanımlanır. İlk popülasyonu belirlemek için (0,1) aralığında 100 × 42 boyutlu rastgele sayılar matrisi oluşturulur. Matrisin A(i, j) öğesi, ith çözümünde (parçacık) jth özelliğinin var olma olasılığını gösterir. Önerilen yöntemde uygulanan Sigmoid fonksiyonuna göre, başlangıç popülasyon matris elemanlarının değerleri, 0.5 eşiğine göre ikiliye dönüştürülür. Diğer bir deyişle, A(i, j) elemanı eşiğin altında bir değere sahipse, jth özelliği ith çözümünde (parçacık) mevcut olmayacaktır. Öte yandan, seçilen özelliklerin alt kümelerinden birinin jthözelliği, bahsedilen elemanın değeri eşiğin üzerindeyse i'inci çözüme (parçacık) sahip olacaktır. Tablo 5.14., başlangıçtaki partikül popülasyonunu göstermektedir.

Tablo 5.14. İlk parçacık popülasyon matrisinin bir parçası

Particul #	F_1	F_2	F_3	F_4	F_5	F_6	F_7	F_8	F_9	F_{10}	F_{11}	F_{12}	F_{13}	F_{14}
1	1	0	1	0	0	1	1	1	1	1	1	1	1	0
2	1	1	0	1	0	1	1	1	0	0	0	1	0	1
3	0	0	1	0	1	1	1	0	1	0	1	0	1	1
4	1	1	1	0	0	0	1	0	0	0	0	1	0	1
5	1	0	0	1	1	0	1	0	0	0	1	1	0	0
6	0	1	1	0	1	0	1	0	1	1	1	1	1	1
7	0	0	1	1	1	1	1	1	0	0	0	0	0	0
8	1	1	1	1	0	1	1	0	1	1	0	0	1	1
9	1	1	1	1	0	0	0	1	1	0	0	1	0	1
10	1	1	1	0	0	1	1	0	1	1	0	1	1	1

Tablo 5.14.'de görüldüğü gibi, ilk partikül popülasyonu önerilen yöntemde ikili bir biçimde dağıtılır ve ilk popülasyonların her biri, KDD veri setinde bulunan özelliklerin bir alt kümesini seçmek için bir çözüm gösterir. Ayarlanan parametrelere göre, başlangıç popülasyon matrisi, MOPSO'nun bir girdisi olarak kullanılır. Ek olarak, önerilen algoritma, ayarlanmış parametreleri ve ilk popülasyonu dikkate alırken ilk adımdaki uygunluk fonksiyonuna dayalı olarak başlangıç popülasyonunu değerlendirir. Daha sonra her bir çözümün yetkinlik düzeyini elde eder. Bu nedenle, bulunan çözümlerin sayısı, aşamaların daha fazla tekrarı ile artacak ve durma durumuna ulaşıncaya kadar yinelemeler devam edecektir. Sonuçta sunulan çözümler değerlendirilir ve mevcut çözümler arasından en iyi çözüm seçilir. MOPSO, ilk popülasyonu alır ve yetkinliğini değerlendirir. İlk adımda, algoritma baskın olmayan çözümleri veya baskın çözümü bulur ve bunları çözüm havuzuna kaydeder. Bir sonraki aşamada, diğer çözeltiler ve parçacıklar çözeltiye yönlendirilir. Buna göre, her aşamada, uygunluk fonksiyonunun değeri eşikten daha yüksek olabilen ve solunumda depolanan bir dizi baskın çözüm bulunabilir. Önerilen yöntemde, yetkinlik miktarının iki hedefin bir araya getirilmesine eşit olması ve bir çözümün yetkinliği ne kadar yüksekse, seçilen özelliklerin sayısı o kadar düşük ve sınıflandırma ve saldırı tespitinin doğruluğu en yüksek FLN sınıfına dayalı özellikler. Bu nedenle, baskın çözümler önerilen yöntemde kullanılan her iki hedefi de iyileştirir. Şekil 2.1., problem alanındaki çözümlerin dağılımını ve ilk adımdaki baskın çözümleri göstermektedir.



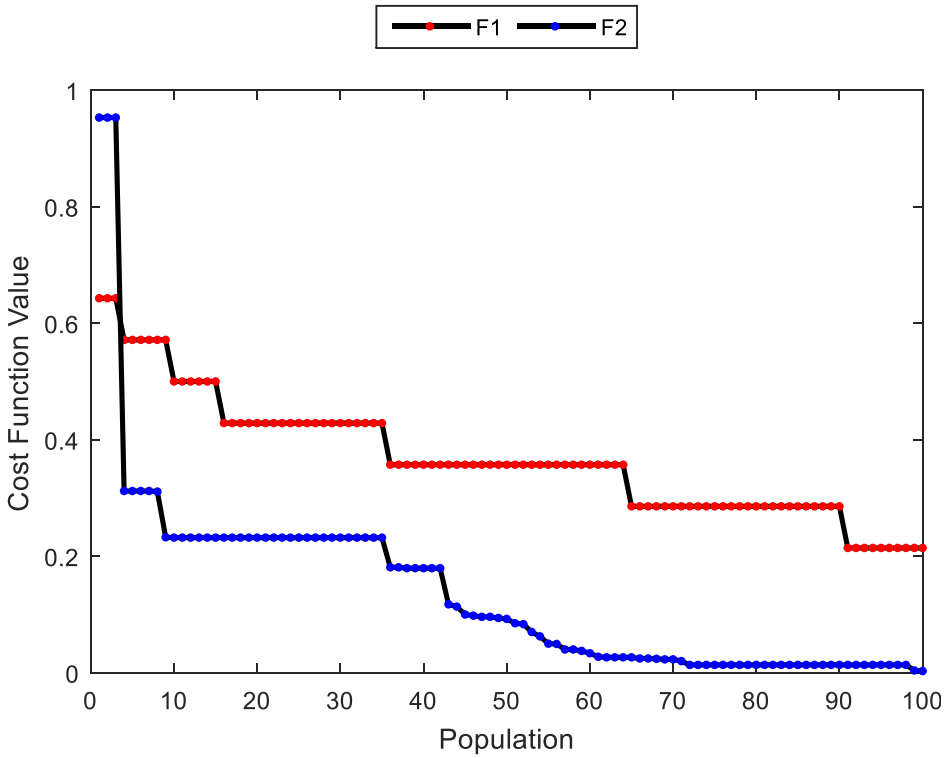
Şekil 5.11. Uzman çözümlerin dağıtımı

Şekil 5.11.'de görüldüğü gibi, önerilen yöntemde MOPSO'nun ilk adımında çözümler problem alanına rastgele dağıtılmıştır. Sorun alanı, F1 ve F2'nin iki amacını içerir; birincisi, veri kümesindeki tüm özelliklerden seçilen özelliklerin sayısını azaltmak için mevcut ve ikincisi, seçilen özelliklere dayalı olarak sınıflandırma hatası oranını azaltmak için Şekil 5.15.'teki dikey eksene karşılık gelir. Başlangıçtaki partikül popülasyonunun rastgele seçimi verildiğinde ve partiküllerin doğası ikili olduğundan, her partikülde bir özelliğin varlığı veya yokluğu, her çözüm için elde edilen sonuçları etkileyebilir. Bu nedenle, sorun alanıyla ilgili olarak, Pareto cephesi, her iki hedefin de minimum olduğu koordinatların kökenine yönelir.

Sonuç olarak MOPSO'da çok amaçlı uygunluk fonksiyonuna dayanan en önemli özelliklerin {"Srv_count" başlıklı {2,7,13,19,26,27} indeksli özellikler olduğu ifade edilebilir. "Count", "Wrong_Fragment", "land", "ds_host_srv_serror_rate" ve "dst_same_srv_rate"}. Önerilen yöntemin ilk popülasyonda uygulanmasıyla ilgili olarak, söz konusu çözümler uzman bir nesil olarak seçildi, tüm yinelemelerde mevcuttu ve buna göre iyileştirildi. Son nesil yinelemede, çoğu parçacık, önceki adımlarda tekrarlanan ve havuzda saklanan uzman parçacıklara veya baskın parçacıklara yöneldi. Bu nedenle, uygunluk işlevinin değerleri, son yinelemede tüm parçacıklar için optimuma yakındı. Daha önce bahsedildiği gibi, uygunluk işlevinin değeri iki F1 ve F2 işlevinin bir kombinasyonundan elde edildi. Buna göre, nihai çözümler, seçilen özelliklerin alt kümesindeki özelliklerin sayısını azaltmanın yanı sıra

önerilen yöntemin hatalarını da azaltmıştır. Şekil 5.11., F1 ve F2 fonksiyonlarının optimal noktaya yakınsamasını göstermektedir.

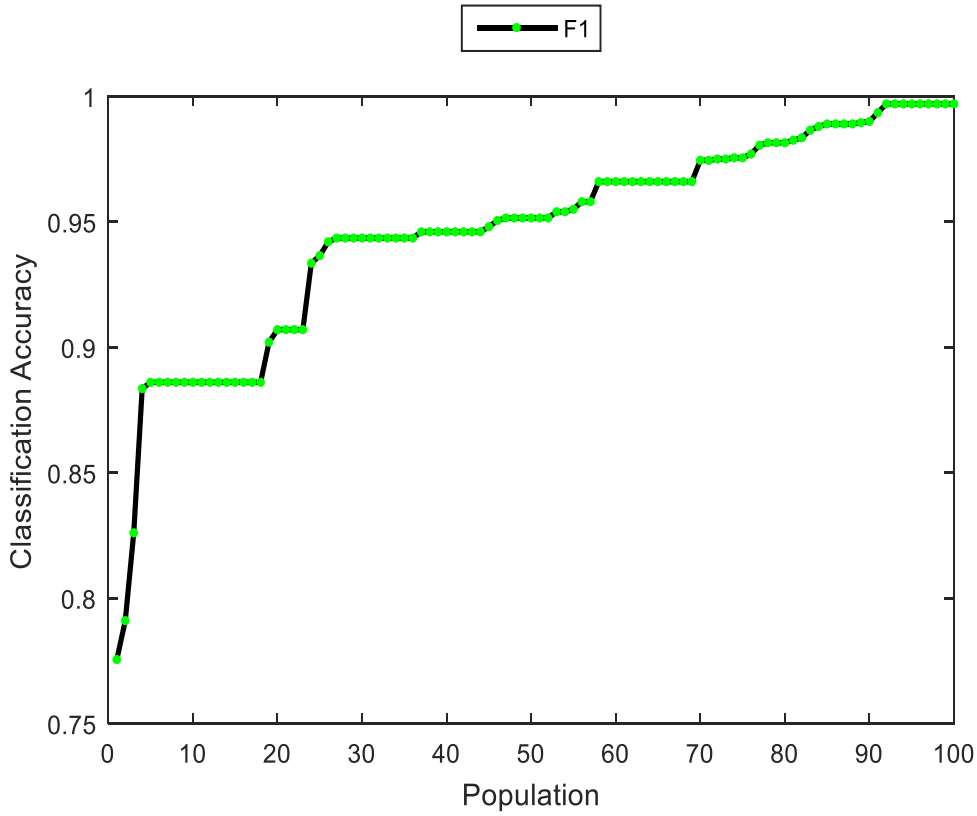
Şekil 5.12.'te görüldüğü gibi, her iki hedef fonksiyonun doğasının minimizasyon olduğu düşünüldüğünde, iki hedefin optimal durumu F1 ve F2 fonksiyonlarında daha düşük değerlere sahipti. Dolayısıyla Şekil 5.11.'te sunulan veriler, seçilen özelliklerin sayısını gösteren F1 fonksiyonuna ilişkin diyagramın kademeli olarak azaldığını ve sonunda 0.2'ye ulaştığını ortaya koymuştur. Diyagram, toplam KDD verilerinin% 20'si ile bir saldırı sisteminin kurulabileceğini ve geri kalan verilerin veri setindeki düğümlerle ilgili grubu belirlemede hiçbir faydası olmadığını gösterdi. Ayrıca Şekil 5.11.'teki F2 fonksiyonu ile ilgili diyagrama göre önerilen yöntemin hataları kademeli olarak azalmış ve nihayetinde sıfıra ulaşmıştır.



Şekil 5.12. Hedef işlevlerin değerlerinin optimum miktara yakınsaması

Şekil 5.12.'ün genel bir yorumu, önerilen tekniğin, veri setinde bulunan özelliklerin sayısını azaltarak ve en uygun özellikleri seçerek saldırı tespit sisteminin hatalarını en düşük seviyeye indirebildiğini göstermiştir. Yöntemde FLN kullanımı göz önüne

alındığında, F2 uygunluk fonksiyonunda elde edilen değerlerin önerilen teknikte FLN sınıflandırma hatası olarak kullanılabileceği ifade edilebilir. Bu nedenle, ağdaki saldırı tespit tekniklerini eğitmek için FLN yönteminin doğruluğu Şekil 5.13.'te gösterilmiştir.



Şekil 5.13. Yetkisiz giriş algılama modelleri için FLN doğruluğu

Şekil 5.13.'te görüldüğü gibi, önerilen yöntemin doğruluğu, çözümlerin MOPSO'nun baskın çözümlerine yönelik eğilimi açısından optimal olma eğilimindeydi ve% 99,7'ye ulaştı. Bu nedenle, test veri setinin tahmin edildiği, önerilen PSO algoritmasından elde edilen en uygun çözümü çıkardık.

5.4.1. Önerilen model değerlendirmesi

Bir önceki bölümde de görüldüğü gibi, FLN bu makalede ağdaki yıkıcı düğümlerin sınıflandırılması ve tahmini için geliştirilmiş ve simülasyon sonuçları MOPSO'ya göre bir özellik alt kümesinin seçimine göre belirlenmiştir. Önerilen yöntemin

performansını değerlendirmek için birkaç kriter vardır, bunlardan en önemlileri performans kriteri, hata oranı kriteri ve doğru tahmin oranı kriteridir. Performans kriteri, geliştirilen modelin performansını izler, yani ideal performans, veri sınıflarının etiketine sahip olarak çizilebilir. Ek olarak, karışıklık matrisine dayalı değerlendirme kriterleri, ağdaki izinsiz girişi tespit etmek ve düğüm sınıflandırma hatalarını azaltmak için önerilen yöntemin kalitesini değerlendirmek için iki sınıflı bir problem için kullanılabilir. Bu kriterler arasında doğruluk, geri çağırma, kesinlik, sınıflandırma oranı (CR), saptama oranı (DR), yanlış pozitif oran (FPR) ve aşağıdaki gibi tanımlanan F ölçümü yer almaktadır :

$$\text{Accuracy} = \frac{TP + TN}{TP+TN+FP+FN} \tag{5.1}$$

$$\text{Precision} = \frac{TP}{TP+FP} \tag{5.2}$$

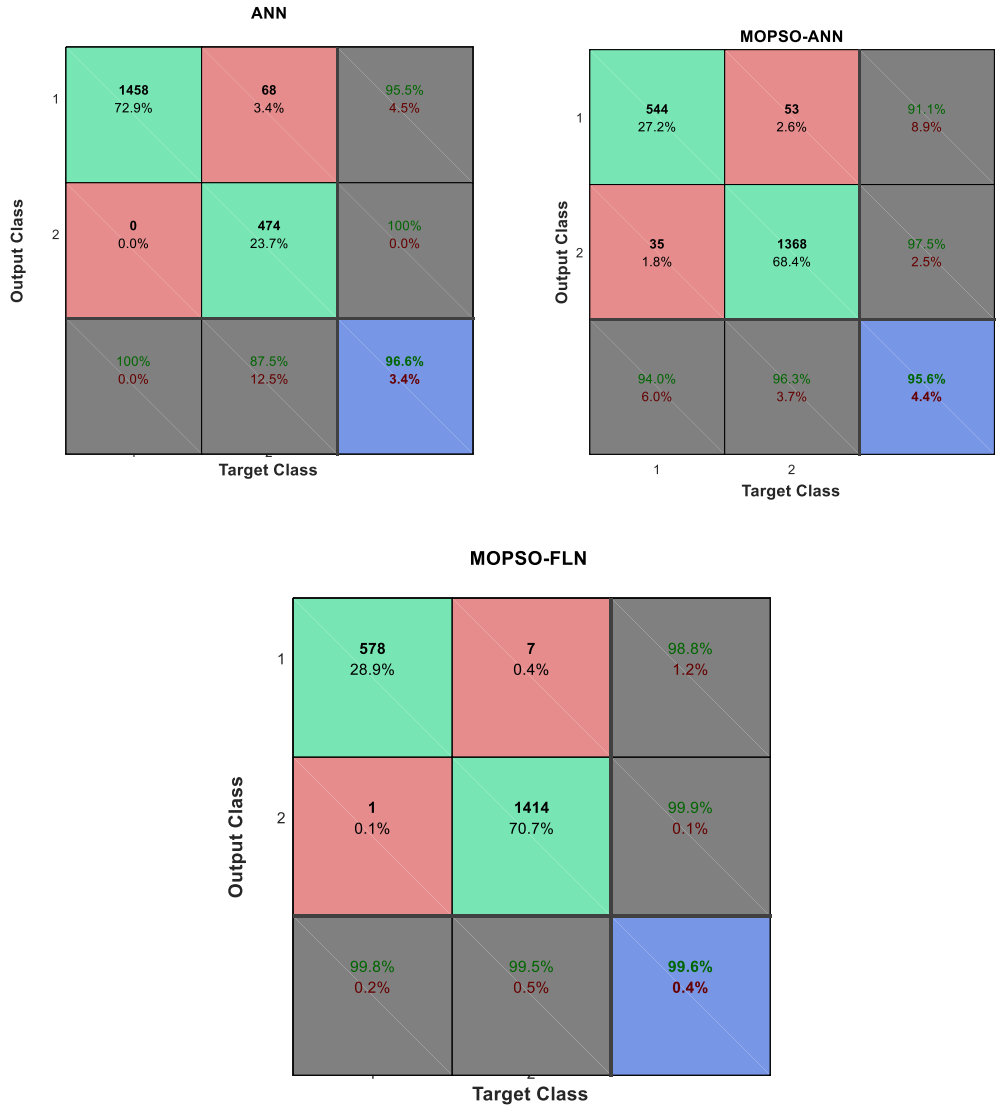
$$\text{Recall} = \frac{TP}{TP+FN} \tag{5.3}$$

$$\text{Classification Rat(CR)} = \frac{TP + TN}{TP+TN+FP+FN} \tag{5.4}$$

$$\text{Detection rate} = \frac{TP}{TP+FN} \tag{5.5}$$

$$\text{False Positive rate (FPR)} = \frac{FP}{FP+TN} \tag{5.6}$$

Sunulan değerlendirme kriterleri, önerilen yöntemin etkinliğini değerlendirmek ve onu mevcut diğer tekniklerle karşılaştırmak için bir araç olarak kullanılır. Bu nedenle, önce YSA kullanmadan önerilen yöntemle sinir ağları, MOPSO-YSA tabanlı özellik seçimine göre sinir ağı yaklaşımı ve önerilen MOPSO-FLN yöntemini karşılaştırdık. Şekil 5.14., önerilen yöntem ve sinir ağı ile ilgili karışıklık matrisinin karşılaştırmasını göstermektedir.



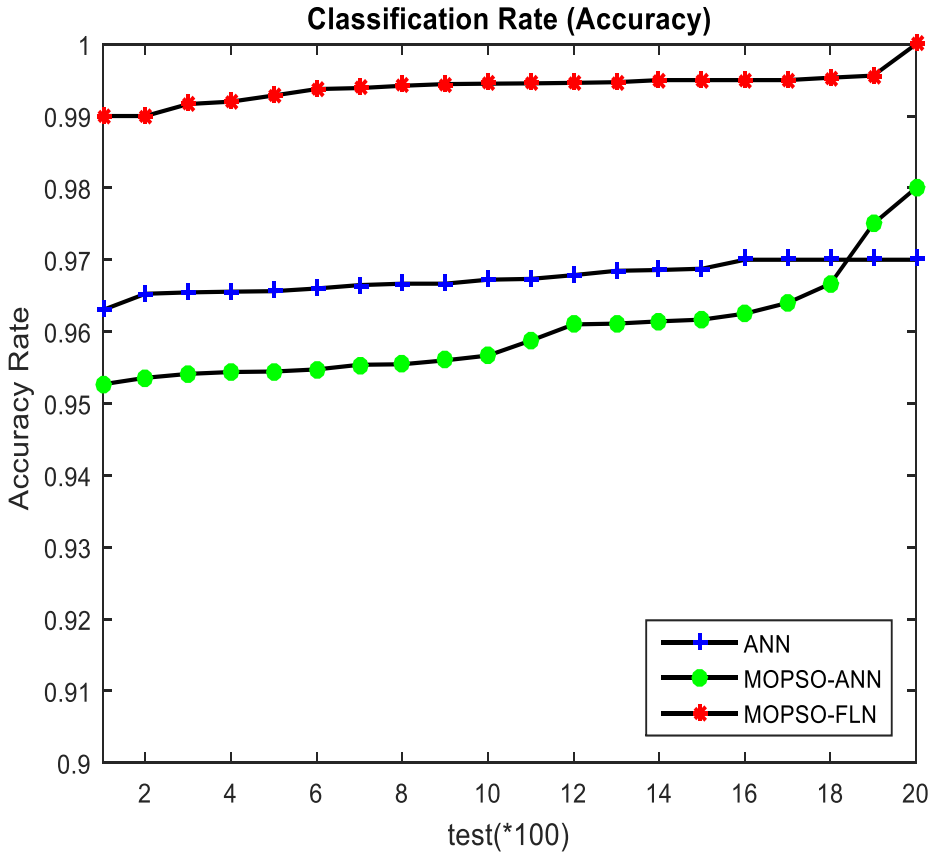
Şekil 5.14. Önerilen yöntemin kafa karışıklığı matrisinin ve sinir ağının karşılaştırılması

Şekil 5.14.'da görüldüğü gibi, önerilen yöntemde toplam verilerin% 99,6'sı doğru bir şekilde sınıflandırılmıştır. Bu arada verilerin sırasıyla% 96,6 ve% 95,6'sı YSA ve MOPSO-YSA yöntemlerinde doğru şekilde sınıflandırılmıştır. Tablo, önerilen yöntem, YSA ve MOPSO-YSA ile ilgili değerlerin bir karşılaştırmasını göstermektedir.

Tablo 5.15. Değerlendirme kriterleri ile ilgili değerlerin karşılaştırılması.

Method	CR (Accuracy)	False positive rate (FPR)	Precision	DR (Recall)	F-measure
MOPSO-FLN	99.45	0.0137	99.44	99.79	99.61
MOPSO - ANN	95.6	0.0888	96.27	97.51	96.88
ANN	96.6	0.0446	84.7	99.99	91.71

Tablo 5.15.'de görüldüğü gibi önerilen yöntemin, değerlendirme kriterleri açısından YSA ve MOPSO-YSA yöntemlerine göre daha yeterli bir performansa sahip olduğu görülmüştür. Şekil 5.14., 10 kat çapraz doğrulama 10 adımda MOPSO-FLN, YSA ve MOPSO-ANN arasındaki sınıflandırma oranı kriterinin (doğruluk) karşılaştırmasını göstermektedir.

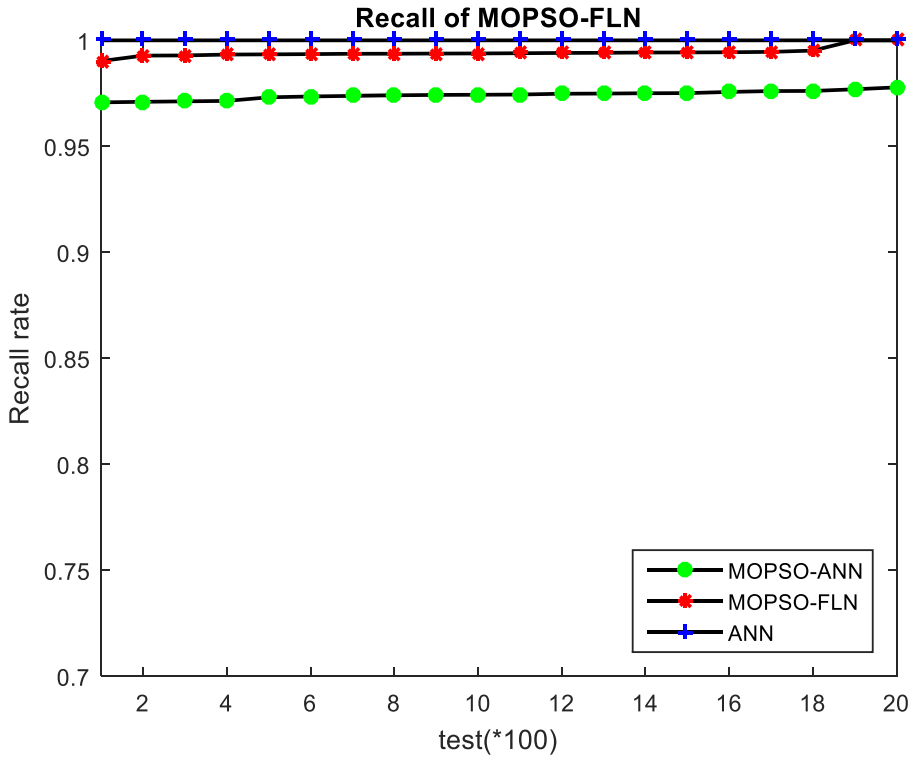


Şekil 5.15. Sınıflandırma oranı kriterinin karşılaştırılması (doğruluk).

Şekil 5.15.'ya göre, önerilen yöntemde YSA ve MOPSO-YSA ile karşılaştırıldığında sınıflandırma oranı (doğruluk) ile ilgili gelişmeler olmuştur. Sinir ağı yönteminde, eğitim sürecinin tamamen yürütüldüğü göz önüne alındığında modelde aşırı uyum yaşanabilir. Bu olguda model, eğitim örneklerine odaklanır ve eğitim örnekleri arasındaki tüm özellikleri ve ilişkileri öğrenir. Ek olarak, eğitim numunelerinin sınıflandırılmasında doğruluğu en üst düzeye çıkarılmıştır. Artık model tarafından daha önce gözlemlenmemiş yeni test örnekleri sisteme girildiğinde, model, eğitim örneklerinden farklı olan yeni örneklerin özellikleri arasındaki ilişkileri tespit etmek

için yeterli doğrulukta olmayabilir, bu da sistemin daha az verimli performansı. Buna göre önerilen yöntem, aşırı uyumu önlemek ve bir IDS'nin performansını artırmak için istenen doğruluğa ulaşıncaya kadar eğitim adımlarına devam eder. Bu nedenle, FLN yönteminin yapay sinir ağları yöntemine kıyasla daha iyi doğruluğu olduğu görülüyor. Aslında, önerilen yöntem daha yüksek bir saldırı yüzdesini ve sağlıklı düğümleri doğru bir şekilde tespit edebildi. Şekil , MOPSO-FLN, ANN ve MOPSO-ANN arasındaki algılama oranı kriterlerini (doğruluk) karşılaştıran bir diyagramı göstermektedir.

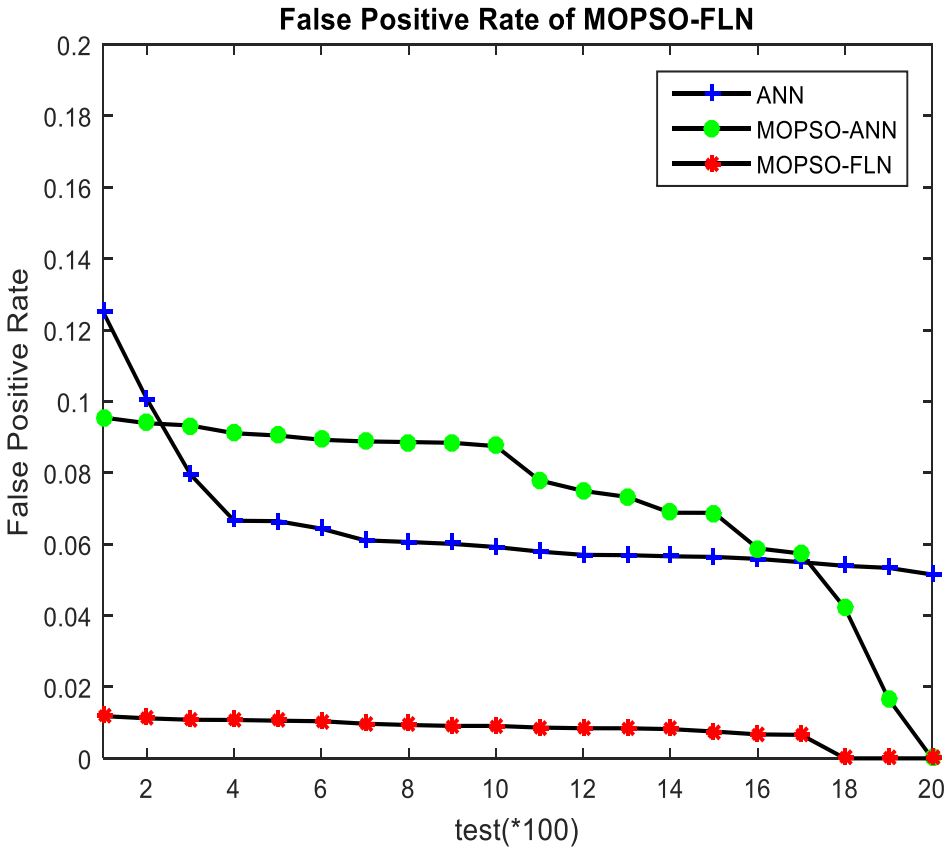
Önerilen yöntemdeki doğruluk oranı, tespit edilen sağlıklı düğümlerin, doğru tespit edilebilen veya yanlış negatif örnekler arasında olabilecek veri setinde bulunan tüm sağlıklı düğümler arasındaki oranı şeklinde olabilir. Sınıflandırma oranı aslında tüm gerçek pozitif ve yanlış negatif numunelerdeki gerçek pozitif numunelerin toplamıdır. Gerçek pozitif, doğru olarak tespit edilen sağlıklı düğümleri ifade ederken, yanlış negatif, yanlışlıkla saldırı düğümleri olarak algılanan sağlıklı düğümleri ifade eder. Bu ilişki, önerilen modelin sağlıklı düğümleri doğru bir şekilde algılama yeteneğini gösterir. Bu ilişkinin değeri ne kadar yüksekse, tahmini sınıfın negatif düğümlere sahip olduğu ve gerçek sınıfın sağlıklı düğümlere sahip olduğu yanlış negatifle ilgili örneklerin sayısı o kadar düşük olur. Yanlış negatif örneklerin daha düşük değerleri, sağlıklı düğümlerin tespit edilmesinde önerilen yöntemin performansını artırır.



Şekil 5.16. Algılama oranı kriterinin karşılaştırılması (doğruluk)

Şekil 5.16.'ya göre, önerilen yöntem YSA ve MOPSO-YSA ile karşılaştırıldığında algılama oranı (doğruluk) açısından iyileştirilmiştir. FLN, belirtilen teknikten daha düşük eğitimi göz önüne alındığında, sinir ağlarına kıyasla daha yüksek bir algılama oranına sahiptir.

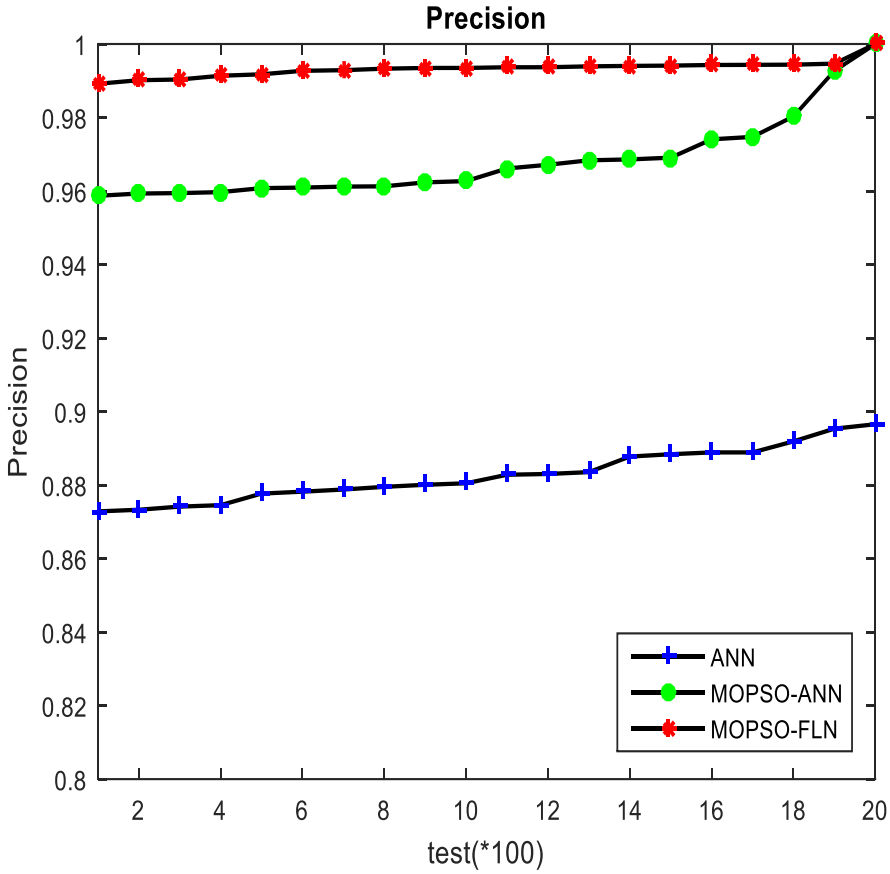
Doğru öğrenme ağlarının yapısı ile ilgili olarak, eğitim süreci durdurulur ve istenen doğruluğa ulaşıldığında sonuçlar çıktıya aktarılır. Bu nedenle, sağlıklı düğümlerin özellikleri tam olarak öğrenilemeyebilir, ancak önerilen yöntemin bir avantajı olan süreçte aşırı uyumdan kaçınılır. Aslında önerilen teknik, yeni ve bilinmeyen örnekler için yüksek doğruluğa sahiptir. Önerilen yöntemdeki tespit oranına ek olarak, keşfedilen numunelerin pozitif hata oranı kriteri de büyük önem taşımaktadır. Şekil, MOPSO-FLN, ANN ve MOPSO-ANN arasındaki pozitif hata oranı kriterinin karşılaştırılmasına ilişkin bir diyagramı göstermektedir.



Şekil 5.17. Pozitif hata oranı kriterinin karşılaştırılması

Şekil 5.17.'de görüldüğü gibi, önerilen yöntem YSA ve MOPSO-YSA ile karşılaştırıldığında pozitif hata oranı açısından daha düşük bir değere sahiptir. Bu bağlamda, önerilen yöntemdeki pozitif hata oranı, IDS tarafından tespit edilemeyen saldırılara atıfta bulundu. Aslında, FLN, saldırılara odaklandığı düşünüldüğünde, sinir ağları yöntemine kıyasla daha düşük bir pozitif hata oranına sahipti. Eğitim veri setinde bulunan saldırılarla ilgili tam eğitime rağmen, sinir ağları hakkında önceden eğitim almadıkları bazı yeni saldırıları tespit edemiyorlar. Bu arada, önerilen yöntem, eğitim örnekleri ile ağın hızı arasında bir denge oluşturarak yeni saldırıları tespit edebildi. Olumlu bir hata oranından sonra, önerilen yöntemin saldırı tespit doğruluğunu değerlendirdik. IDS'lerde doğruluk, gerçek pozitif örneklerin gerçek pozitif örneklere ve gerçek negatif örneklere oranının biçimidir ve bu, sınıflandırma yöntemlerinde saldırı algılama yeteneğinin bir yansımasını tahmin eder. Bu değer ne kadar yüksekse, sınıflandırma yönteminin yeni saldırıları algılama ve tanımlama yeteneği o kadar yüksek olur. Şekil 5.17., MOPSO-FLN, ANN ve MOPSO-ANN

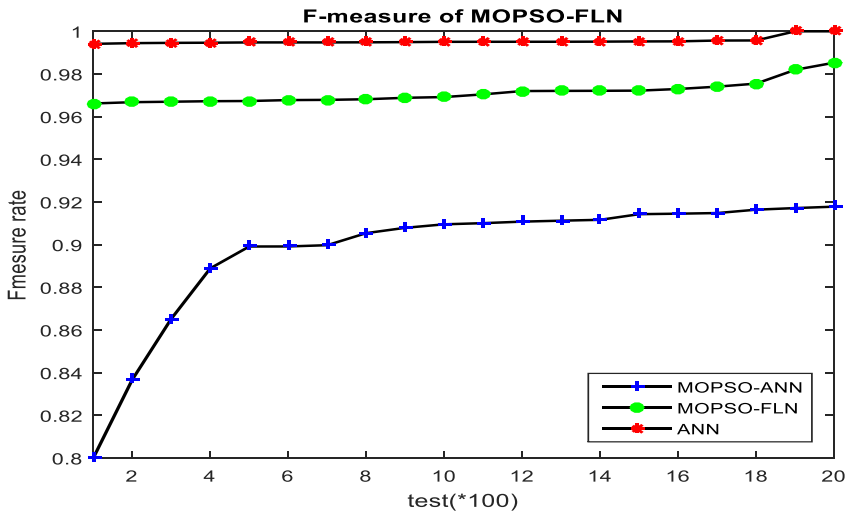
arasındaki pozitif doğruluk kriterinin karşılaştırılmasıyla ilgili bir diyagramı göstermektedir.



Şekil 5.18. Önerilen yöntemin ve sinir ağının doğruluk kriterinin karşılaştırılması

Şekil 5.18.'e göre, önerilen yöntem YSA ve MOPSO-YSA ile karşılaştırıldığında doğruluk kriteri açısından iyileştirilmiştir. Önerilen yöntemin doğruluğu, FLN'nin saldırılara odaklanması ve sinir ağlarına kıyasla yeni saldırıları önemli ölçüde tespit etme yeteneği dikkate alındığında arttı. Şekil 5.18., sinir ağlarında aşırı uyumun varlığının ve önerilen yöntemde bu fenomenin yokluğunun tam bir temsilidir. Genel olarak, fazla uydurma, bir modelin doğruluğunu yeni örneklere göre azaltır. Aslında FLN, yeni örnekler arasında bulunan ve modelde daha önce gözlemlenmemiş çoğu saldırıyı algılayabilir. Bu çalışmada değerlendirilen son kriter, iki doğruluk ve tespit oranı kriterinin bir kombinasyonu olan F-ölçümü idi. Kriter, sınıflandırma yöntemlerinin ve IDS'lerin performansının genel bir kriteri olarak kabul edildi. Kriterin değeri ne kadar yüksekse, IDS'nin sağlıklı örnekleri sınıflandırma ve eğitim

veri kümesindeki saldırıları ve sisteme giren yeni saldırıları tahmin etme yeteneği o kadar yüksek olur. MOPSO-FLN, ANN ve MOPSO'nun F-ölçümü ile ilgili karşılaştırması ile ilgili bir diyagramı göstermektedir.

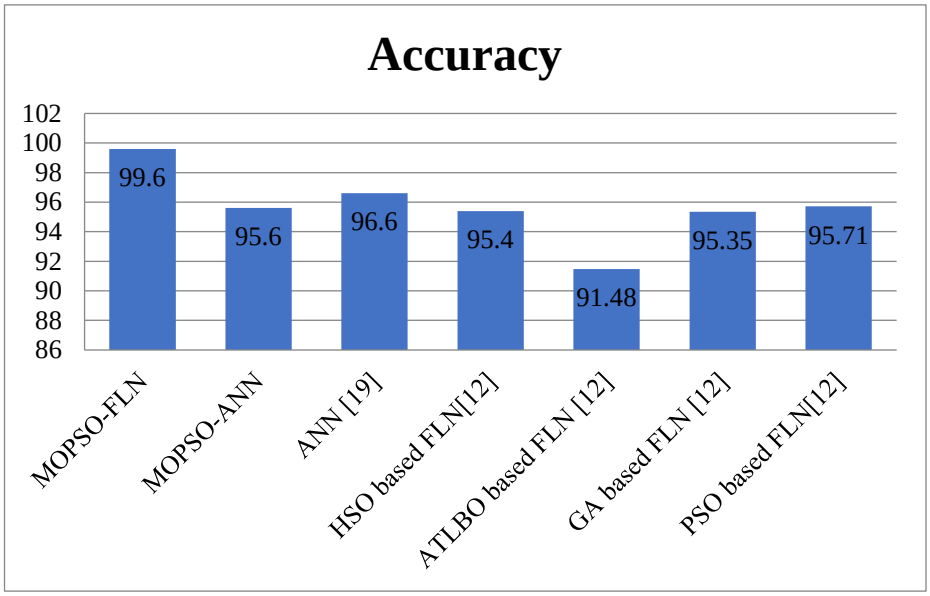


Şekil 5.19. F-Score karşılaştırması

Şekil 5.19.'a göre, önerilen yöntem YSA ve MOPSO-YSA ile karşılaştırıldığında F-ölçüm kriteri açısından gelişmiştir. Başka bir deyişle, FLN, sinir ağlarına kıyasla, MOPSO tabanlı özellik alt küme seçimi ile birleştirildiğinde ağdaki sağlıklı düğümleri ve yeni saldırıları tespit etmede daha iyi bir performansa sahipti.

5.4.2. Önerilen yöntemin önceki tekniklerle karşılaştırılması

Bu alt kümede, tahmin doğruluğu kriteri açısından önerilen yöntemin geçerliliğini değerlendirmek için MOPSO-FLN'yi yayınlarda [12] bulunan diğer yöntemlerle karşılaştırdık. Şekil 5.20., önerilen yöntemin önceki tekniklerle bir karşılaştırmasını göstermektedir. Şekil 5.20.'ye göre, MOPSO-FLN, önceki yöntemlere kıyasla daha yüksek saldırı algılama ve tahmin doğruluğuna sahipti.



Şekil 5.20. Önerilen yöntemin önceki tekniklerle karşılaştırılması

BÖLÜM 6. TARTIŞMA VE SONUÇ

Bu projede izinsiz girişin iki farklı yönünü biyometrik sahtekarlık tespiti ve ağ saldırı tespitine dayalı olarak tartıştık. bu iki konu, herhangi bir Çevrimiçi platformun korunması için birbirine bağlıdır. Saldırganların veritabanına saldırdığı ve farklı biyometrik bilgileri bir sisteme enjekte ettiği bir senaryo varsayın, bu durumda davetsiz misafir biyometrik erişim kontrolünü kolayca doğrulayabilir. Veya saldırgan biyometrik sahtekarlık yardımıyla sunucu bilgilerine ulaşır ve sistemleri atlar. Bu tür ağ saldırı tespitlerinin biyometrik sahtekarlık tespitiyle büyük ölçüde ilişkili olduğu açıktır. Bu nedenle, ağ saldırı tespiti için makine öğrenmesine dayalı dört farklı yaklaşım sunduk.

IOT tabanlı yüz sahtekarlığı tespiti çalışmada, yüz sahtekarlığı tespiti için IoT-bulut tabanlı çerçeve önerilmiş ve uygulanmıştır. Önerilen sistem, yeni derin öğrenme çerçevesini uygulayarak yüz sahteciliği saldırısını tespit eder. Bu yaklaşım, eğitim aşamasında hem işlem maliyetini hem de veri boyutunu azaltan daha az veri depolayarak bulut tabanlı ortamda güvenilir bir şekilde kullanılabilir. Dahası, önerilen çok renkli derin özellik tabanlı yaklaşım, Replay-attack veritabanındaki temel yöntemlerden daha iyi performans gösterirken, ROSE-Youtu veritabanında rekabetçi sonuçlar elde etti. Replay-attack ve ROSE-Youtu veritabanları için elde edilen sonuçlar, arka plan değişiklikleri, el sıkışması, yüksek çözünürlüklü kamera ve aydınlatma gibi çevresel faktörlerin ve senaryoların önerilen yaklaşımımızın etkinliğini sınırlamadığını kanıtladı. Ayrıca, önerdiğimiz yaklaşım, yazdırma, görüntüleme ve yeniden oynatma saldırıları gibi senaryolarda tatmin edici sonuçlar elde etti. Kırpma olmadan, kırpma, üst kısım kesim, alt kısım kesim ve iki göz ve ağız kırpılmış maske gibi farklı senaryolarda maske saldırıları olması durumunda, önerilen yaklaşım uyumlu sonuçlar sunarken, ilerideki çalışmalarda ekleyerek araştıracağız.

Yüz sahtekarlığı algılama yaklaşımı çalışmada ,Tanıma alanlarında yüz sahtekarlığı tespiti için RPCA ve Derin inanç ağına dayalı yeni bir boru hattı önerdik. Önerilen yaklaşım, daha az eğitim seti ile daha sağlam doğruluk ve performans elde etmek için derin öğrenme modellerine beslenen hareket analizi ve doku özellik setleri olarak her bir videonun hayati özelliklerini içeriyordu. Deneysel sonuçlar, önerilen yaklaşımımızın, sınıflandırma doğruluğu için EER ve HTER değerlerine dayanan en yeni algoritmalara kıyasla önemli sonuçlar verdiğini göstermiştir.

MOPSO tabanlı özellik seçimi yaklaşımının kullanılmasıyla ilgili olarak, veri setindeki tüm özellikleri temsil eden en iyi özelliklerin bulunmasının yanı sıra, sınıflandırma modelindeki performans hatalarının azaltılması ve test örneklerinin tahmin edilmesi amaçlanmıştır. MOPSO tarafından önerilen yöntemde çıkarılan optimum özellikler, Pareto cephesinde parçacıkların yüksek değerlere sahip parçacıklara doğru hareket hızını artırmak ve her adımda bu özelliklere dayalı veri sınıflandırma hatalarını azaltmak için optimizasyon algoritması yinelemesinin her aşamasında değerlendirilmiştir. Bu nedenle, bu özelliklerin seçilmesi, sınıflarla ilgili örneklerin sınıflandırma modeli ve yüksek sınıflandırma doğruluğu ile basitçe ayırt edilmesine kadar.

MOPSO tabanlı özellik seçimi yaklaşımının kullanılmasıyla ilgili olarak, veri setindeki tüm özellikleri temsil eden en iyi özelliklerin bulunmasının yanı sıra, sınıflandırma modelindeki performans hatalarının azaltılması ve test örneklerinin tahmin edilmesi amaçlanmıştır. MOPSO tarafından önerilen yöntemde çıkarılan optimum özellikler, Pareto cephesinde parçacıkların yüksek değerlere sahip parçacıklara doğru hareket hızını artırmak ve her adımda bu özelliklere dayalı veri sınıflandırma hatalarını azaltmak için optimizasyon algoritması yinelemesinin her aşamasında değerlendirilmiştir. Bu nedenle bu özelliklerin seçimi, sınıflara ilişkin örneklerin sınıflandırma modeli ve yüksek sınıflandırma doğruluğu ile basit ayrımına kadar tekrar edilmiştir.

Ayrıca, önerilen yöntem makalelerde sunulan diğer popüler yaklaşımlarla karşılaştırıldı. Sonuçlara göre, sinir ağı, kablosuz ağlarda izinsiz girişle ilgili veri

kümesinden önemli özellikler alt kümesi seçilmeden ve bağımsız olarak kullanıldığında önerilen yönteme kıyasla nispeten daha düşük bir doğruluğa sahipti. Önerilen yöntemin ve sinir ağı tabanlı yöntemin doğruluğundaki yaklaşık% 4'lük fark, FLN kullanarak bir özellik alt kümesinin seçilmesinin öneminin bir başka kanıtıydı.

Önerilen yöntem ayrıca, meta-sezgisel optimizasyon algoritmasına dayalı özellik alt kümesi seçimini kullanan diğer birkaç yaklaşımla karşılaştırıldı. Sonuçlara göre, önerilen yöntem, MOPSO tabanlı özellik seçimi ve hızlı sinir ağının bir kombinasyonu olan izinsiz giriş algılama yaklaşımına kıyasla daha yüksek test örneği tahmin doğruluğuna sahipti. Buna göre, önerilen yöntemin MOPSO tabanlı öznitelik alt küme seçimini kullanarak önemli öznitelikleri çıkarabildiği sonucuna varılabilir. Ayrıca model, bir dizi özellik ve sınıflandırma hatasının bir kombinasyonu olan bir değerlendirme fonksiyonu kullanarak kablosuz ağlarda izinsiz girişin tespiti ve tahmini açısından kabul edilebilir sonuçlar vermiştir.

Bulanık mantık yardımıyla ağ anomalisi tespiti çalışmada , Günümüzde bilim ve teknolojinin ilerlemesi ve insanoğlunun bilinç ve bilgi düzeyinin artmasıyla, her geçen gün görüldüğü gibi, çeşitli ticari, iletişim, bilgi ve diğer ağlara yönelik yaygın saldırılar yaşanmaktadır. Bu saldırıların bir kısmı, bu ağlarda bulunan önemli ve hassas verileri, bilgileri hedef alır. Bir kısmı da kullanıcılara farklı hizmetler sunan kaynaklar ve sunuculardaki iletişim yollarında fazladan trafik oluşturmaya çalışarak yetkili kullanıcılar için bu hizmetleri, sunucuları kullanılamaz hale getirir ya da ağ performansını birkaç dakika ya da saat için bozar. Bilgisayar korsanlarını tanımlamanın bir yolu, saldırı olasılığını çeşitli şekillerde tespit etmeye veya tahmin etmeye çalışan saldırı tespit sistemlerini (IDS) kullanmaktır. Bu yollardan biri ağ trafiğini kontrol etmek ve ağda çok fazla trafik oluşturarak saldırıları tespit etmeye çalışmaktır. Bu yazıda, bu tür bir saldırıyı ele aldık ve hedef ağdaki kötü amaçlı trafiği meta-sezgisellerin manuel olarak algılaması için NN modelinin yardımıyla Suricata IDS / IPS'yi dağıtmak için yeni bir yöntem önerdik. Önerilen çözümde, ek dosyaları veya bilinmeyen protokoller içeren trafik, anormallik trafiği olarak tespit edilene dayalı olarak bulanık mantık tarafından işlenecektir. Makine öğrenimi yöntemlerini

kullanarak IDS / IPS için önerilen çözümün yerleştirilmesi için bir sanal ortam dağıtıldı.

6.1. Gelecekteki Çalışma

İzinsiz giriş tespit sistemleri çalışması sırasında da belirtildiği gibi, mevcut bilgilere dayanılarak simülasyon hibrit saldırıları için bir platform bulunmadığı söylenebilir. ayrıca sistemi bu tür hibrit saldırılara karşı korumak için makine öğrenimi algoritmasının yardımıyla algılama sistemlerini incelemeyi planlıyoruz.

KAYNAKLAR

[1] Y. Mirsky, T. Doitshman, Y. Elovici, and A. Shabtai, "Kitsune: An ensemble of autoencoders for online network intrusion detection," arXiv, no. February, pp. 18–21, 2018, doi: 10.14722/ndss.2018.23204.

[2] Z. Ali, M. S. Hossain, G. Muhammad, I. Ullah, H. Abachi, and A. Alamri, "Edge-centric multimodal authentication system using encrypted biometric templates," Futur. Gener. Comput. Syst., vol. 85, pp. 76–87, 2018, doi: 10.1016/j.future.2018.02.040.

[3] S. Garg, S. Mittal, P. Kumar, and V. A. Athavale, "DeBNet: Multilayer deep network for liveness detection in face recognition system," 2020 7th Int. Conf. Signal Process. Integr. Networks, SPIN 2020, pp. 1136–1141, 2020, doi: 10.1109/SPIN48934.2020.9070853.

[4] T. Bouwmans, S. Javed, H. Zhang, Z. Lin, and R. Otazo, "On the Applications of Robust PCA in Image and Video Processing," Proc. IEEE, vol. 106, no. 8, pp. 1427–1457, 2018, doi: 10.1109/JPROC.2018.2853589.

[5] M. Gomez-Barrero, E. Maiorana, J. Galbally, P. Campisi, and J. Fierrez, "Multi-biometric template protection based on Homomorphic Encryption," Pattern Recognit., vol. 67, pp. 149–163, 2017, doi: 10.1016/j.patcog.2017.01.024.

[6] P. Kumari and P. Thangaraj, "Microprocessors and Microsystems A fast feature selection technique in multi modal biometrics using cloud framework," Microprocess. Microsyst., vol. 79, no. August, p. 103277, 2020, doi: 10.1016/j.micpro.2020.103277.

[7] K. A. Shakil, F. J. Zareen, M. Alam, and S. Jabin, "BAMHealthCloud: A biometric authentication and data management system for healthcare data in cloud," J. King Saud Univ. - Comput. Inf. Sci., vol. 32, no. 1, pp. 57–64, 2020, doi: 10.1016/j.jksuci.2017.07.001.

[8] B. Sree Vidya and E. Chandra, "Entropy based Local Binary Pattern (ELBP) feature extraction technique of multimodal biometrics as defence mechanism for cloud storage," Alexandria Eng. J., vol. 58, no. 1, pp. 103–114, 2019, doi: 10.1016/j.aej.2018.12.008.

[9] M. Masud et al., “Deep learning-based intelligent face recognition in IoT-cloud environment,” Comput. Commun., vol. 152, no. January, pp. 215–222, 2020, doi: 10.1016/j.comcom.2020.01.050.

[10] X. Song, X. Zhao, L. Fang, and T. Lin, “Discriminative representation combinations for accurate face spoofing detection,” Pattern Recognit., vol. 85, pp. 220–231, 2019, doi: 10.1016/j.patcog.2018.08.019.

[11] G. Pan, L. Sun, Z. Wu, and S. Lao, “Eyeblink-based anti-spoofing in face recognition from a generic webcamera,” Proc. IEEE Int. Conf. Comput. Vis., 2007, doi: 10.1109/ICCV.2007.4409068.

[12] A. Gumaei, R. Sammouda, A. M. S. Al-Salman, and A. Alsanad, “Anti-spoofing cloud-based multi-spectral biometric identification system for enterprise security and privacy-preservation,” J. Parallel Distrib. Comput., vol. 124, pp. 27–40, 2019, doi: 10.1016/j.jpdc.2018.10.005.

[13] Z. Boulkenafet, J. Komulainen, and A. Hadid, “On the generalization of color texture-based face anti-spoofing,” Image Vis. Comput., vol. 77, pp. 1–9, 2018, doi: 10.1016/j.imavis.2018.04.007.

[14] Z. Boulkenafet, J. Komulainen, and A. Hadid, “Face Spoofing Detection Using Colour Texture Analysis,” IEEE Trans. Inf. Forensics Secur., vol. 11, no. 8, pp. 1818–1830, 2016, doi: 10.1109/TIFS.2016.2555286.

[15] L. Li, Z. Xia, X. Jiang, F. Roli, and X. Feng, “CompactNet: learning a compact space for face presentation attack detection,” Neurocomputing, vol. 409, pp. 191–207, 2020, doi: 10.1016/j.neucom.2020.05.017.

[16] D. T. Nguyen, T. D. Pham, N. R. Baek, and K. R. Park, “Combining deep and handcrafted image features for presentation attack detection in face recognition systems using visible-light camera sensors,” Sensors (Switzerland), vol. 18, no. 3, 2018, doi: 10.3390/s18030699.

[17] L. Li, X. Feng, Z. Boulkenafet, Z. Xia, M. Li, and A. Hadid, “An original face anti-spoofing approach using partial convolutional neural network,” 2016 6th Int. Conf. Image Process. Theory, Tools Appl. IPTA 2016, no. i, pp. 1–6, 2017, doi: 10.1109/IPTA.2016.7821013.

[18] M. Habib, I. Aljarah, H. Faris, and S. Mirjalili, “Multi-objective Particle Swarm Optimization: Theory, Literature Review, and Application in Feature Selection for Medical Diagnosis,” in Evolutionary Machine Learning Techniques: Algorithms and Applications, S. Mirjalili, H. Faris, and I. Aljarah, Eds. Singapore: Springer Singapore, 2020, pp. 175–201.

[19] S. Muruganandam, J. A. Renjit, and R. S. Kumar, “A Survey: Comparative study of security methods and trust manage solutions in MANET,” 5th Int. Conf. Sci. Technol. Eng. Math. ICONSTEM 2019, pp. 125–131, 2019, doi: 10.1109/ICONSTEM.2019.8918697.

[20] K. J. Sarma, R. Sharma, and R. Das, “A survey of Black hole attack detection in Manet,” Proc. 2014 Int. Conf. Issues Challenges Intell. Comput. Tech. ICICT 2014, pp. 202–205, 2014, doi: 10.1109/ICICICT.2014.6781279.

[21] M. Kaur, M. Rani, and A. Nayyar, “A Comprehensive Study of Jelly Fish Attack in Mobile Ad hoc Networks,” vol. 3, no. 4, pp. 199–203, 2014.

[22] G. Kumar Ahuja and G. Kumar, “Evaluation Metrics for Intrusion Detection Systems-A Study,” Int. J. Comput. Sci. Mob. Appl., vol. 2, no. June 2015, pp. 11–17, 2014.

[23] P. Yang, Z. Li, P. Yang, and Y. Dong, “Information-centric mobile ad hoc networks and content routing: A survey,” Ad Hoc Networks, vol. 58, pp. 255–268, 2017, doi: 10.1016/j.adhoc.2016.04.005.

[24] A. Sultana and M. A. Jabbar, “Intelligent network intrusion detection system using data mining techniques,” Proc. 2016 2nd Int. Conf. Appl. Theor. Comput. Commun. Technol. iCATccT 2016, pp. 329–333, 2017, doi: 10.1109/ICATCCT.2016.7912017.

[25] F. H. Tseng, L. Der Chou, and H. C. Chao, “A survey of black hole attacks in wireless mobile ad hoc networks,” Human-centric Comput. Inf. Sci., vol. 1, no. 1, pp. 1–16, 2011, doi: 10.1186/2192-1962-1-4.

[26] J. Määttä, A. Hadid, and M. Pietikäinen, “Face Spoofing Detection From Single Images Using Micro-Texture Analysis,” IEEE 6th Int. Conf. Biometrics Theory, Appl. Syst. BTAS 2013, vol. 1, no. 1, pp. 3–10, 2012, doi: 10.1049/iet-bmt.2011.0009.

[27] Z. Boulkenafet, J. Komulainen, and A. Hadid, “Face anti-spoofing based on color texture analysis,” Proc. - Int. Conf. Image Process. ICIP, vol. 2015-Decem, pp. 2636–2640, 2015, doi: 10.1109/ICIP.2015.7351280.

[28] I. Chingovska, A. Anjos, and S. Marcel, “On the effectiveness of local binary patterns in face anti-spoofing,” Proc. Int. Conf. Biometrics Spec. Interes. Group, BIOSIG 2012, pp. 1–7, 2012.

[29] Q. T. Phan, D. T. Dang-Nguyen, G. Boato, and F. G. B. De Natale, “FACE spoofing detection using LDP-TOP,” Proc. - Int. Conf. Image Process. ICIP, vol. 2016-Augus, pp. 404–408, 2016, doi: 10.1109/ICIP.2016.7532388.

[30] L. Li, X. Feng, Z. Boulkenafet, Z. Xia, M. Li, and A. Hadid, “An original face anti-spoofing approach using partial convolutional neural network,” 2016 6th Int. Conf. Image Process. Theory, Tools Appl. IPTA 2016, no. i, pp. 16–21, 2017, doi: 10.1109/IPTA.2016.7821013.

[31] G. B. De Souza, S. Member, D. Felipe, R. G. Pires, A. N. Marana, and J. P. Papa, “Deep Texture Features for Robust Face Spoofing Detection,” IEEE Trans. Circuits Syst. II Express Briefs, vol. 64, no. 12, pp. 1397–1401, 2017.

[32] Z. Xu, S. Li, and W. Deng, “Learning temporal features using LSTM-CNN architecture for face anti-spoofing,” Proc. - 3rd IAPR Asian Conf. Pattern Recognition, ACPR 2015, pp. 141–145, 2016, doi: 10.1109/ACPR.2015.7486482.

[33] Z. Zhang, J. Yan, S. Liu, Z. Lei, D. Yi, and S. Z. Li, “A face antispoofing database with diverse attacks,” Proc. - 2012 5th IAPR Int. Conf. Biometrics, ICB 2012, pp. 26–31, 2012, doi: 10.1109/ICB.2012.6199754.

[34] X. Tan, Y. Li, J. Liu, and L. Jiang, “Face liveness detection from a single image with sparse low rank bilinear discriminative model,” Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 6316 LNCS, no. PART 6, pp. 504–517, 2010, doi: 10.1007/978-3-642-15567-3_37.

[35] H. Li, S. Wang, and A. C. Kot, “Face spoofing detection with image quality regression,” 2016 6th Int. Conf. Image Process. Theory, Tools Appl. IPTA 2016, pp. 1–6, 2017, doi: 10.1109/IPTA.2016.7821027.

[36] T. Edmunds and A. Caplier, “Motion-based countermeasure against photo and video spoofing attacks in face recognition,” J. Vis. Commun. Image Represent., vol. 50, no. December 2017, pp. 314–332, 2018, doi: 10.1016/j.jvcir.2017.12.004.

[37] A. Anjos and S. Marcel, “Counter-measures to photo attacks in face recognition: A public database and a baseline,” 2011 Int. Jt. Conf. Biometrics, IJCB 2011, 2011, doi: 10.1109/IJCB.2011.6117503.

[38] Q. Phan, G. Boato, and F. G. B. De Natale, “Using LDP-TOP in Video-Based Spoofing Detection,” Image Anal. Process. - ICIAP, vol. 10485, pp. 614–624, 2017, doi: 10.1007/978-3-319-68548-9_56.

[39] G. Zhao and M. Pietikäinen, “Dynamic texture recognition using local binary patterns with an application to facial expressions,” IEEE Trans. Pattern Anal. Mach. Intell., vol. 29, no. 6, pp. 915–928, 2007, doi: 10.1109/TPAMI.2007.1110.

[40] W. Bao, H. Li, N. Li, and W. Jiang, “A liveness detection method for face recognition based on optical flow field,” Proc. 2009 Int. Conf. Image Anal. Signal Process. IASP 2009, pp. 233–236, 2009, doi: 10.1109/IASP.2009.5054589.

[41] N. Erdogmus and S. Marcel, “Spoofing in 2D face recognition with 3D masks and anti-spoofing with Kinect,” IEEE 6th Int. Conf. Biometrics Theory, Appl. Syst. BTAS 2013, 2013, doi: 10.1109/BTAS.2013.6712688.

[42] I. Pavlidis and P. Symosek, “The imaging issue in an automatic face/disguise detection system,” IEEE Work. Comput. Vis. Beyond Visible Spectr. Methods Appl., pp. 15–24, 2002, doi: 10.1109/cvbvs.2000.855246.

[43] Z. Zhang, D. Yi, Z. Lei, and S. Z. Li, “Face liveness detection by learning multispectral reflectance distributions,” 2011 IEEE Int. Conf. Autom. Face Gesture Recognit. Work. FG 2011, pp. 436–441, 2011, doi: 10.1109/FG.2011.5771438.

[44] L. Feng et al., “Integration of image quality and motion cues for face anti-spoofing: A neural network approach,” J. Vis. Commun. Image Represent., vol. 38, pp. 451–460, 2016, doi: 10.1016/j.jvcir.2016.03.019.

[45] Y. A. U. Rehman, L. M. Po, and M. Liu, “SLNet: Stereo face liveness detection via dynamic disparity-maps and convolutional neural network,” Expert Syst. Appl., vol. 142, p. 113002, 2020, doi: 10.1016/j.eswa.2019.113002.

[46] J. Komulainen, A. Hadid, M. Pietikainen, A. Anjos, and S. Marcel, “Complementary countermeasures for detecting scenic face spoofing attacks,” Proc. - 2013 Int. Conf. Biometrics, ICB 2013, 2013, doi: 10.1109/ICB.2013.6612968.

[47] S. Tirunagari, N. Poh, D. Windridge, A. Iorliam, N. Suki, and A. T. S. Ho, “Detection of face spoofing using visual dynamics,” IEEE Trans. Inf. Forensics Secur., vol. 10, no. 4, pp. 762–777, 2015, doi: 10.1109/TIFS.2015.2406533.

[48] F. Haneef, “a Feature Selection Technique for Intrusion Detection System Based on Iwd and Aco,” Int. J. Adv. Res. Comput. Sci., vol. 8, no. 9, pp. 270–275, 2017, doi: 10.26483/ijarcs.v8i9.4857.

[49] A. Davahli, M. Shamsi, and G. Abaei, “A Lightweight Anomaly Detection Model using SVM for WSNs in IoT through a Hybrid Feature Selection Algorithm based on GA and GWO,” vol. 7, no. 1, pp. 63–79, 2020.

[50] W. L. Al-Yaseen, “Improving intrusion detection system by developing feature selection model based on firefly algorithm and support vector machine,” IAENG Int. J. Comput. Sci., vol. 46, no. 4, pp. 1–7, 2019.

[51] H. Alazzam, A. Sharieh, and K. E. Sabri, “A feature selection algorithm for intrusion detection system based on Pigeon Inspired Optimizer,” Expert Syst. Appl., vol. 148, 2020, doi: 10.1016/j.eswa.2020.113249.

[52] Y. Liu, Z. Xu, J. Yang, L. Wang, C. Song, and K. Chen, “A novel meta-heuristic-based sequential forward feature selection approach for anomaly detection systems,” Proc. - 2016 Int. Conf. Netw. Inf. Syst. Comput. ICNISC 2016, pp. 218–227, 2017, doi: 10.1109/ICNISC.2016.20.

[53] L. Calvet, J. De Armas, D. Masip, and A. A. Juan, “Learnheuristics: Hybridizing metaheuristics with machine learning for optimization with dynamic inputs,” Open Math., vol. 15, no. 1, pp. 261–280, 2017, doi: 10.1515/math-2017-0029.

[54] K. C. Lin, Y. H. Huang, J. C. Hung, and Y. T. Lin, “Feature Selection and Parameter Optimization of Support Vector Machines Based on Modified Cat Swarm Optimization,” Int. J. Distrib. Sens. Networks, vol. 2015, 2015, doi: 10.1155/2015/365869.

[55] Y. Zhou, G. Cheng, S. Jiang, and M. Dai, “Building an efficient intrusion detection system based on feature selection and ensemble classifier,” Comput. Networks, vol. 174, no. April, 2020, doi: 10.1016/j.comnet.2020.107247.

[56] O. Osanaiye, O. Ogundile, F. Aina, and A. Periola, “Feature selection for intrusion detection system in a cluster-based heterogeneous wireless sensor network,” Facta Univ. - Ser. Electron. Energ., vol. 32, no. 2, pp. 315–330, 2019, doi: 10.2298/fuee1902315o.

[57] M. GÜNAY and Z. ORMAN, “A MODIFIED FIREFLY ALGORITHM-BASED FEATURE SELECTION METHOD AND ARTIFICIAL IMMUNE SYSTEM FOR INTRUSION DETECTION Melike,” Uludağ Univ. J. Fac. Eng., vol. 25, no. 1, pp. 269–288, 2020, doi: 10.17482/uumfd.649003.

[58] A. Chiche and M. Meshesha, “Towards a Scalable and Adaptive Learning Approach for Network Intrusion Detection,” J. Comput. Networks Commun., vol. 2021, 2021, doi: 10.1155/2021/8845540.

[59] X. Li, P. Yi, W. Wei, Y. Jiang, and L. Tian, “LNNLS-KH: A Feature Selection Method for Network Intrusion Detection,” Secur. Commun. Networks, vol. 2021, 2021, doi: 10.1155/2021/8830431.

[60] M. H. Kamarudin, C. Maple, T. Watson, and N. S. Safa, “A New Unified Intrusion Anomaly Detection in Identifying Unseen Web Attacks,” Secur. Commun. Networks, vol. 2017, 2017, doi: 10.1155/2017/2539034.

[61] Z. A. Khan and P. Herrmann, “Recent advancements in intrusion detection systems for the internet of things,” Secur. Commun. Networks, vol. 2019, 2019, doi: 10.1155/2019/4301409.

[62] G. Li, Z. Yan, Y. Fu, and H. Chen, “Data Fusion for Network Intrusion Detection: A Review,” Secur. Commun. Networks, vol. 2018, 2018, doi: 10.1155/2018/8210614.

[63] A. Khraisat, I. Gondal, P. Vamplew, J. Kamruzzaman, and A. Alazab, “Hybrid intrusion detection system based on the stacking ensemble of C5 decision tree classifier and one class support vector machine,” Electron., vol. 9, no. 1, 2020, doi: 10.3390/electronics9010173.

[64] J. Snehi, A. Bhandari, V. Baggan, and M. Snehi, “Diverse Methods for Signature based Intrusion Detection Schemes Adopted,” Int. J. Recent Technol. Eng., vol. 9, no. 2, pp. 44–49, 2020, doi: 10.35940/ijrte.a2791.079220.

[65] D. Mudzingwa and R. Agrawal, “A study of methodologies used in intrusion detection and prevention systems (IDPS),” Conf. Proc. - IEEE SOUTHEASTCON, 2012, doi: 10.1109/SECon.2012.6197080.

[66] L. H. U. A. Yeo, C. H. E. Xiangdong, and S. Lakkaraju, “Understanding modern intrusion detection systems: A survey,” arXiv, 2017.

[67] M. A. Aydin, A. H. Zaim, and K. G. Ceylan, “A hybrid intrusion detection system design for computer network security,” Comput. Electr. Eng., vol. 35, no. 3, pp. 517–526, 2009, doi: 10.1016/j.compeleceng.2008.12.005.

[68] Y.-Q. Wang, “An Analysis of the Viola-Jones Face Detection Algorithm,” Image Process. Line, vol. 4, pp. 128–148, 2014, doi: 10.5201/ipol.2014.104.

[69] O. M. Parkhi, A. Vedaldi, and A. Zisserman, “Deep Face Recognition,” no. Section 3, pp. 41.1-41.12, 2015, doi: 10.5244/c.29.41.

[70] L. Li, X. Feng, Z. Xia, X. Jiang, and A. Hadid, “Face spoofing detection with local binary pattern network,” J. Vis. Commun. Image Represent., vol. 54, no. December 2017, pp. 182–192, 2018, doi: 10.1016/j.jvcir.2018.05.009.

[71] K. Simonyan and A. Zisserman, “Very deep convolutional networks for large-scale image recognition,” in 3rd International Conference on Learning Representations, ICLR 2015 - Conference Track Proceedings, 2015, pp. 1–14.

[72] C. Perez, J. Tapia, P. Estévez, and C. Held, “Gender Classification from Face Images Using Mutual Information and Feature Fusion,” Int. J. Optomechatronics, vol. 6, no. 1, pp. 92–119, 2012, doi: 10.1080/15599612.2012.663463.

[73] W. R. and Z. Wang, “Deep Convolutional Neural Networks for Image Classification: A Comprehensive Review,” Neural Comput., vol. 2733, pp. 2709–2733, 2017, doi: 10.1162/NECO.

[74] M. Toğaçar, B. Ergen, and Z. Cömert, “A Deep Feature Learning Model for Pneumonia Detection Applying a Combination of mRMR Feature Selection and Machine Learning Models,” Irbm, vol. 1, pp. 1–11, 2019, doi: 10.1016/j.irbm.2019.10.006.

[75] Y. A. U. Rehman, L. M. Po, M. Liu, Z. Zou, W. Ou, and Y. Zhao, “Face liveness detection using convolutional-features fusion of real and deep network generated face images,” J. Vis. Commun. Image Represent., vol. 59, pp. 574–582, 2019, doi: 10.1016/j.jvcir.2019.02.014.

[76] H. Peng, Fuhui Long, and Chris Ding, “Feature Selection Based on Mutual Information: Criteria of Max-Dependency, Max-Relevance, and Min-Redundancy,” IEEE Trans. PATTERN Anal. Mach. Intell., vol. 27, no. 8, pp. 1–6, 2005, doi: 10.1109/cita.2015.7349827.

[77] C. Ding and H. Peng, “Minimum redundancy feature selection from microarray gene expression data,” Proc. 2003 IEEE Bioinforma. Conf. CSB 2003, vol. 3, no. 2, pp. 523–528, 2003, doi: 10.1109/CSB.2003.1227396.

[78] Z. Akhtar, G. Fumera, G. L. Marcialis, and F. Roli, “Evaluation of serial and parallel multibiometric systems under spoofing attacks,” 2012 IEEE 5th Int. Conf. Biometrics Theory, Appl. Syst. BTAS 2012, pp. 283–288, 2012, doi: 10.1109/BTAS.2012.6374590.

[79] N. Kose and J. L. Dugelay, “Mask spoofing in face recognition and countermeasures,” Image Vis. Comput., vol. 32, no. 10, pp. 779–789, 2014, doi: 10.1016/j.imavis.2014.06.003.

[80] B. K. Bao, G. Liu, C. Xu, and S. Yan, “Inductive robust principal component analysis,” IEEE Trans. Image Process., vol. 21, no. 8, pp. 3794–3800, 2012, doi: 10.1109/TIP.2012.2192742.

[81] P. Zhong, Z. Gong, S. Li, and C. B. Schonlieb, “Learning to Diversify Deep Belief Networks for Hyperspectral Image Classification,” IEEE Trans. Geosci. Remote Sens., vol. 55, no. 6, pp. 3516–3530, 2017, doi: 10.1109/TGRS.2017.2675902.

[82] Y. Chen, X. Zhao, and X. Jia, “Spectral-Spatial Classification of Hyperspectral Data Based on Deep Belief Network,” IEEE J. Sel. Top. Appl. Earth Obs. Remote Sens., vol. 8, no. 6, pp. 2381–2392, 2015, doi: 10.1109/JSTARS.2015.2388577.

[83] G. E. Hinton, “Training products of experts by minimizing contrastive divergence,” Neural Comput., vol. 14, no. 8, pp. 1771–1800, 2002, doi: 10.1162/089976602760128018.

[84] E. J. Teoh, K. C. Tan, and C. Xiang, “Estimating the number of hidden neurons in a feedforward network using the singular value decomposition,” IEEE Trans. Neural Networks, vol. 17, no. 6, pp. 1623–1629, 2006, doi: 10.1109/TNN.2006.880582.

[85] I. Chingovska, A. Anjos, and S. Marcel, “On the effectiveness of local binary patterns in face anti-spoofing,” Proc. Int. Conf. Biometrics Spec. Interes. Group, BIOSIG 2012, 2012.

[86] Z. Yang, W. Chen, F. Wang, and B. Xu, “Unsupervised Domain Adaptation for Face Anti-Spoofin,” IEEE Trans. Inf. Forensics Secur., vol. 2018-Augus, no. 7, pp. 338–343, 2018, doi: 10.1109/ICPR.2018.8546053.

[87] Z. Boulkenafet, J. Komulainen, L. Li, X. Feng, and A. Hadid, “OULU-NPU: A Mobile Face Presentation Attack Database with Real-World Variations,” Proc. - 12th IEEE Int. Conf. Autom. Face Gesture Recognition, FG 2017 - 1st Int. Work. Adapt. Shot Learn. Gesture Underst. Prod. ASL4GUP 2017, Biometrics Wild, Bwild 2017, Heteroge, pp. 612–618, 2017, doi: 10.1109/FG.2017.77.

[88] Y. Liu, A. Jourabloo, and X. Liu, “Learning Deep Models for Face Anti-Spoofing: Binary or Auxiliary Supervision,” Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit., pp. 389–398, 2018, doi: 10.1109/CVPR.2018.00048.

[89] C. Szegedy, V. Vanhoucke, S. Ioffe, J. Shlens, and Z. Wojna, “Rethinking the Inception Architecture for Computer Vision,” Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit., vol. 2016-Decem, pp. 2818–2826, 2016, doi: 10.1109/CVPR.2016.308.

[90] C. Szegedy, S. Ioffe, V. Vanhoucke, and A. A. Alemi, “Inception-v4, inception-ResNet and the impact of residual connections on learning,” 31st AAAI Conf. Artif. Intell. AAAI 2017, pp. 4278–4284, 2017.

[91] G. Wang, H. Han, S. Shan, and X. Chen, “Unsupervised Adversarial Domain Adaptation for Cross-domain Face Presentation Attack Detection,” IEEE Trans. Inf. Forensics Secur., vol. XX, no. XX, pp. 1–1, 2020, doi: 10.1109/tifs.2020.3002390.

[92] H. Li, P. He, S. Wang, A. Rocha, X. Jiang, and A. C. Kot, “Learning Generalized Deep Feature Representation for Face Anti-Spoofing,” IEEE Trans. Inf. Forensics Secur., vol. 13, no. 10, pp. 2639–2652, 2018, doi: 10.1109/TIFS.2018.2825949.

[93] M. M. Hasan, M. S. U. Yusuf, T. I. Rohan, and S. Roy, “Efficient two stage approach to detect face liveness : Motion based and Deep learning based,” 2019 4th Int. Conf. Electr. Inf. Commun. Technol. EICT 2019, no. December, pp. 20–22, 2019, doi: 10.1109/EICT48899.2019.9068813.

[94] T. De Freitas Pereira, A. Anjos, J. M. De Martino, and S. Marcel, “Can face anti-spoofing countermeasures work in a real world scenario?,” Proc. - 2013 Int. Conf. Biometrics, ICB 2013, 2013, doi: 10.1109/ICB.2013.6612981.

[95] Z. Boulkenafet, J. Komulainen, X. Feng, and A. Hadid, “Scale space texture analysis for face anti-spoofing,” 2016 Int. Conf. Biometrics, ICB 2016, pp. 1–6, 2016, doi: 10.1109/ICB.2016.7550078.

[96] X. Yang et al., “Face anti-spoofing: Model matters, so does data,” Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit., vol. 2019-June, pp. 3502–3511, 2019, doi: 10.1109/CVPR.2019.00362.

[97] W. Sun, Y. Song, C. Chen, J. Huang, and A. C. Kot, “Face Spoofing Detection Based on Local Ternary Label Supervision in Fully Convolutional Networks,” IEEE Trans. Inf. Forensics Secur., vol. 15, pp. 1–1, 2020, doi: 10.1109/tifs.2020.2985530.

ÖZGEÇMİŞ

Adı Soyadı **:** Sajad EİNY

ÖĞRENİM DURUMU

Derece	**Eğitim Birimi**	**Mezuniyet Yılı**
Doktora	Sakarya Üniversitesi / Fen Bilimleri Enstitüsü / Bilgisayar ve Bilişim Mühendisliği	Devam Ediyor
Yüksek Lisans	JNTU Üniversitesi / Fen Bilimleri Enstitüsü / Bilişim Teknolojileri Mühendisliği	2013
Lisans	PNU Üniversitesi / Mühendislik Fakültesi / Bilgisayar Mühendisliği	2010
Lise	Shahed Fen Lisesi	2004

İŞ DENEYİMİ

Yıl	**Yer**	**Görev**
2016-Halen	Istanbul Aydin Üniversitesi	Öğretim Görevlisi

YABANCI DİL

İngilizce

ESERLER (makale)

1. Sajad Einy, Cemil Oz, ve Yahya Dorostkar Navaei “The Anomaly- and Signature-Based IDS for Network Security Using Hybrid Inference Systems”, Mathematical Problems in Engineering , ISSN / eISSN: 1024-1230 / 1563-5147, vol. 2021, 2021, doi: 10.1155/2021/6639714.

HOBİLER

Yüzme