Kurt Saldırıları için Sentetik İrislerde Örnek Seçilimi
Sample Picking in Synthetic Irides for Wolf Attacks

Eyüp Kaan Akdeniz, Nesli Erdoğmuş
Bilgisayar Mühendisliği Bölümü
İzmir Yüksek Teknoloji Enstitüsü, İzmir, Türkiye
{eyupakdeniz, neslierdogmus}@iyte.edu.tr

***Özetçe* —Bu çalışmada, sentetik olarak üretilen iris imgeleri arasından kurt saldırılarında başarılı olma ihtimali daha yüksek örneklerin seçilimi yapılmış ve oluşturulan örnek kümesinin Sunum Saldırısı Tespiti (SST) modülü de içeren bir iris tanıma sistemi için, rastgele seçilen örneklere kıyasla daha büyük bir tehdit oluşturduğu gösterilmiştir. Derin Evrişimli Çekişmeli Üretici Ağlar kullanılarak üretilen iris imgeleri, öncelikle gerçek iris imgelerinin SST skorları dağılımı üzerinde kabul-ret örneklemesi kullanılarak filtrelenmiştir. Ardından, eğitim kümesindeki gerçek iris imgeleri ve bunlar üzerinde hesaplanan eş olan ve olmayan skor dağılımları kullanılarak her bir sentetik iris imgesinin hiç başarılı saldırı gerçekleştirememe olasılıkları hesaplanmış ve bu olasılığı en düşük olan örnekler nihai kümeye dahil edilmiştir. Bu kümenin kurt saldırılarında daha başarılı olacağı hipotezi rastgele seçilmiş kümelerin kandırma performansları ile karşılaştırma yapılarak test edilmiştir.**

Anahtar Kelimeler—iris kandırma saldırısı, sentetik iris, kurt saldırısı.

***Abstract*—In this study, samples with higher potential to succeed in wolf attacks are picked among synthetically generated iris images, and the composed subset is shown to pose a more significant threat toward an iris recognition system backed by a Presentation Attack Detection (PAD) module with respect to randomly selected samples. Iris images generated by Deep Convolutional Generative Adversarial Networks (DCGAN) are firstly filtered by rejection sampling on PAD score distribution of real iris image PAD scores. Next, the probability of zero success in all attack attempts is calculated for each synthetic iris image, using real iris images in the training set, and match and non-match score distributions are calculated on those. Synthetic images with the lowest probabilities of zero success are included in the final set. Our hypothesis that this set would be more successful in wolf attacks is tested by comparing its spoofing performances with randomly selected sample sets.**

Keywords—iris spoofing attack, synthetic iris, wolf attack.

I. Giriş

Sahip olduğu zengin örüntü içeriği ile iris, parmak izi ve yüz ile birlikte biyometrik modalitelerin "üç büyükler"ini oluşturmuş, yıllar içinde geniş bir kullanım alanına ve kullanıcı kitlesine erişmiştir. Pandeminin getirdiği artan temassız biyometri çözümleri ihtiyacının da etkisi ile gelecek yıllarda yerini daha da sağlama alacağı tahmin edilmektedir [1]. Bu sebeplerle iris tanıma sistemlerinin güvenliği ve güvenilirliği kritik bir öneme sahiptir.

Biyometri temelli kimlik tanıma sistemlerinde saldırıya açık birden fazla zayıf nokta mevcuttur [2]. Bunlar arasında, sistemde bulunan biyometrik sensörün hemen öncesinde ve hemen sonrasında yer alan iki açık sunum saldırıları için kullanılabilir. Sensör öncesinde saldırı, kağıda basılmış yüz resmi, yapay silikon bir parmak izi ya da iris gibi fiziksel ve sahte bir biyometrik kanıt kullanılarak gerçekleştirilebilir. Sonrasında ise sensör baypas edilerek, kaydedilmiş sahte bir biyometrik sinyal sisteme sokulabilir. Her iki durumda da biyometrik veriler gerçek bir kullanıcıdan gelebileceği gibi sentetik olarak üretilmiş de olabilir.

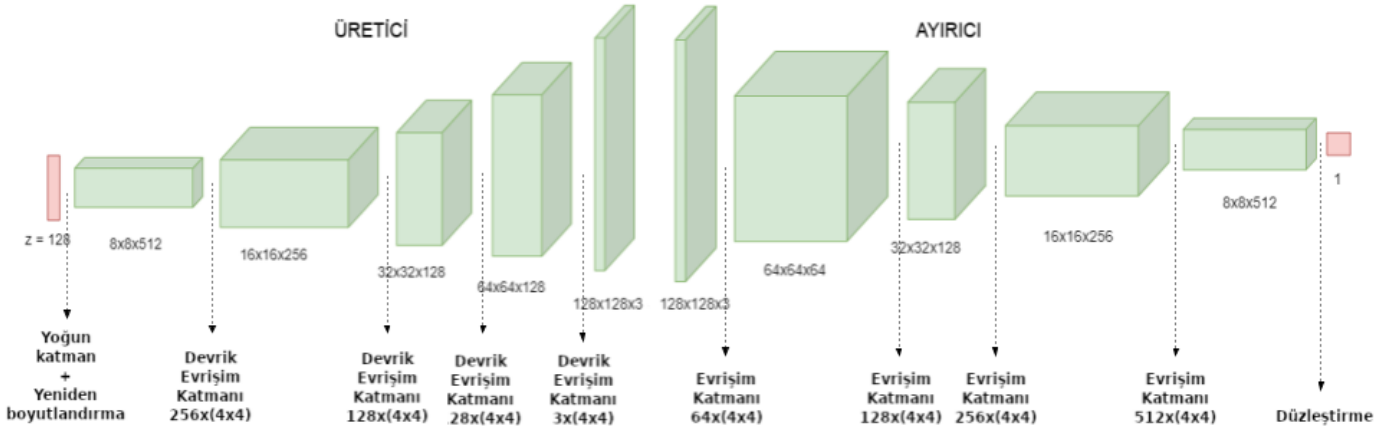
Sisteme gerçek bir kullanıcı verisini sokabilmek için önce bu veri elde edilmelidir. Bunun için, bazı özel saldırı yazılımları geliştirilmesi ve sisteme bu tehlikeye karşı dahil edilmiş gizli dinleme (sniffing) ya da veri ihlali tespiti araçlarının atlatılması gerekmektedir. Öte yandan, sentetik veri kullanımı tam bir sıfır çaba (zero effort) saldırısı olmasa da bu zorunlulukları ortadan kaldırır. Sentetik veri ile saldırı başarımı gerçek bir kullanıcı verisi ile elbette kıyaslanamaz, ancak teşebbüslerin sınırsızca tekrarlanabilir olması sisteme sızma tehlikesini arttırır.

Bu çalışmada, biyometrik algılama sonrasında, algılanan sinyalin yerine ortadaki adam saldırısı ile sentetik üretilmiş bir sinyal konması senaryosu ele alınmaktadır. Bunun da ötesinde, bir eğitim kümesi kullanılarak üretilen iris imgelerinin, aynı eğitim kümesindeki gerçek imgelerin istatistiki özellikleri ile karşılaştırılarak elenmesi ile kurt saldırıları gerçekleştirilebileceği savı incelenmektedir. Bu tarz saldırılar, biyometrik tanıma sistemlerine karşı, kayıtlı kullanıcı verilerine çok benzer ve genel özelliklere sahip örnekler, diğer bir deyişle "kurt örnekler" bulma ya da üretme yolu ile tehdit oluşturur [3]. Bu yöntemde amaç gerçek kullanıcı verilerini ele geçirmek değil, kayıtlı herhangi bir biyometrik şablona eşleştirilme olasılığı yüksek örnekler elde etmektir.

II. İris İmgesi Üretimi

Literatürde, iris imgelerinin sentetik üretimine yönelik farklı yaklaşımlar önerilmiştir. Bunların ilkinde [4], iris tanıma algoritmalarının geliştirilmesinde kullanılmak üzere, Temel Bileşenler Analizi ve süper çözünürlük temelli bir sentetik iris imgesi üretme yöntemi denenmiştir. Sonrasındaki çalışmalarda ise iris imgesi sentezlemenin amacı, geliştirilen iris tanıma algoritmalarının büyük ölçekli testlerinin yapılabilmesine imkan sağlamak olmuştur [5]–[8]. Sentezleme işlemi için [5]'de Markof Rasgele Alanı modellemesi ile iris benzeri örüntüler yaratılması fikri sunulmuştur. [6]'da 3 boyutlu silindirik lif

2023 31st Signal Processing and Communications Applications Conference (SIU) | 979-8-3503-4355-7/23/$31.00 ©2023 IEEE | DOI: 10.1109/SIU59756.2023.10223964



Şekil 1: Kullanılan DCGAN katmanları ve ağ boyunca elde edilen veri boyutları

yapıları ile stroma oluşturulup 2 boyuta izdüşümü alınmış, [8]'de bu yaklaşım farklı anatomik özelliklerin de ele alınması ile daha kapsamlı hale getirilmiştir. [9]'da ise iris imgeleri yama-tabanlı örnekleme yaklaşımı ile sentezlenmiştir.

Daha yakın tarihli çalışmalarda, iris imgesi üretimi derin sinir ağları kullanılarak yapılmaya başlanmıştır. Kohli v.d. iris imgelerini derin evrişimli çekişmeli üretici ağlar (DCGAN) [10] kullanarak üretimiştir [11]. Üretilen sentetik iris imgelerinin gerçeğe yakınlığı kalite metrik dağılımlarına bakarak incelenmiş ve bir sunum saldırısı tespit algoritması ile gerçek örneklerden ayırt edilebilir olup olmadıkları test edilmiştir. Yadav v.d. [12] ise iris sentezleme işlemi için göreceli ortalama standart çekişmeli üretici ağlar kullanmıştır [13]. Diğer çalışmalardan farklı olarak, üretilen iris imgelerinin eğitim kümesine dahil edilmesi ile daha önce tanık olunmamış tipte saldırıların tespitinde başarımın arttırılabileceği gösterilmiştir.

[11]'e benzer şekilde, bu çalışmada sentetik iris imgesi üretimi için bir DCGAN mimarisi (Şekil 1) kullanılmıştır. Dört devrik evrişim katmanı içeren üretici için son katmanda aktivasyon fonksiyonu olarak tanh, ayırıcı için ise yine dört evrişim katmanı sonrasında çıktı katmanı için sigmoit fonksiyonu kullanılmıştır. Diğer tüm katmanlarda aktivasyonlar Leaky-ReLU fonksiyonu ile hesaplanmıştır. Evrişim katmanlarında çekirdek boyutu 4 ve kaydırma adımı 2 olarak seçilmiştir.

III. Sentetik İris Örnek Seçilimi

Üretilen iris imgeleri sunum saldırısı tespit skorlarına ve saldırı başarılarına göre bir seçilime tabi tutulmuştur. Bunun için gerekli tüm hesaplamalar yalnızca üreticinin eğitiminde faydalanılan gerçek iris imgeleri kullanılarak yapılmıştır.

A. Sunum Saldırısı Tespit Skoruna göre Seçilim

Sunum saldırısı tespit skorlarının hesaplanması için D-NetPAD [14] yöntemi kullanılmıştır. Gerçek iris imgelerinden hesaplanan skorlar için normal olasılık dağılımı varsayımı ile ortalama ve standart sapma hesaplanmış, daha sonra bu dağılım üzerinde sentetik iris imgeleri için kabul-ret örneklemesi uygulanmıştır. Böylece üretilen irislerin sunum saldırısı tespit skoru dağılımının gerçek irislere yaklaşması sağlanmıştır.

Bu adımda sunum saldırısı tespit skorları en düşük imgeleri seçmek de bir seçenek olarak karşımıza çıkmaktadır. Ancak bunun sentetik imgeleri gerçeklikten uzaklaştırabileceği ve sunum saldırısı başarımını düşürebileceği düşünüldüğünden, istatistiki özellikleri gerçeğinkine benzeyen sentetik veriler ile ilerlemeye karar verilmiştir.

B. Sunum Saldırısı Başarısına göre Seçilim

Sunum saldırısı başarım oranlarının tespiti için kullanılan eşleştirme skorları VeriEye yazılımı [15] ile hesaplanmıştır. Tüm gerçek iris imgeleri birbirileriyle ve tüm sentetik iris imgeleri gerçek iris imgeleri ile karşılaştırılmış, böylece eş olan ve olmayan skorlar ile saldırı skorları elde edilmiştir.

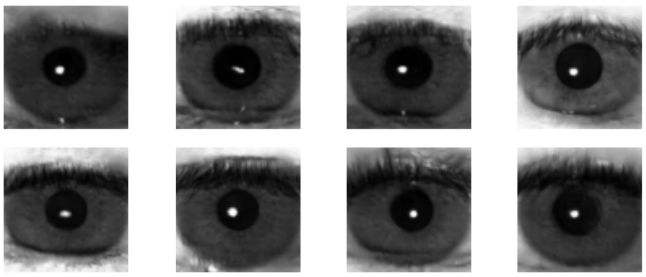
Kurt saldırısı gerçekleştirebilmek için sentetik iris imgelerinin biyometrik sistemde kayıtlı herhangi bir ya da daha fazla kullanıcıya eşleşme olasılığını olabildiğince arttırmak gerekmektedir. Bu amaçla, sentetik her bir imge için kayıtlı kullanıcılara yönelik yapılan saldırıların hiçbirinin başarılı olmaması ihtimali hesaplanmış ve bu ihtimali en düşük olanlar "kurt örnek"ler olarak seçilmiştir.

Bir sentetik iris imgesinin saldırısının başarısız olması için hiçbir kullanıcı ile eşleşememesi, bir diğer deyişle, bu saldırı için hesaplanan her eşleşme skorunun (s_i) eş olmayan ($\neg e$) skor olarak belirlenmesi gerekmektedir. Tek bir karşılaştırma için bunun olasılığı $P(\neg e|s_i)$'dir. Bu değeri bulmak için öncelikle, normal olasılık dağılımı varsayımı ile gerçek iris imgelerinden elde edilen eş olan ve olmayan skorların ortalama ve standart sapmaları hesaplanmıştır. Böylece herhangi bir skor için $P(s|\neg e)$ ve $P(s|e)$ kestirimi yapılabilmiştir. $P(\neg e|s_i)$ olasılıkları için Bayes kuralı kullanılmış, önsel olasılıklar $P(e)$ ve $P(\neg e)$ birbirine eşit ve 0,5 kabul edilmiştir (1).

$$P(\neg e|s_i) = \frac{P(s_i|\neg e) \times P(\neg e)}{P(s_i|\neg e) \times P(\neg e) + P(s_i|e) \times P(e)} \quad (1)$$

Sentetik bir iris imgesi tarafından gerçekleştirilen hiçbir saldırının eşleşmeme ($\neg E$) olasılığı, hesaplama kolaylığı bakımından logaritmik olasılık kullanılarak ve koşullu bağımsızlık varsayımı ile hesaplanmıştır (2).

$$\log P(\neg E) = \log \prod_{i=1}^{N} P(\neg e|s_i) = \sum_{i=1}^{N} \log P(\neg e|s_i) \quad (2)$$



Şekil 2: Üretilen sentetik iris imgelerine örnekler

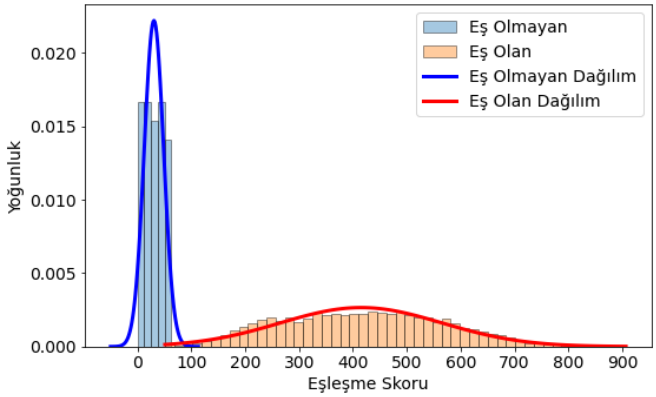
IV. Deneyler ve Bulgular

Araştırmanın tekrarlanabilirliği için kullanılan veri, yapay sinir ağı modelleri ve deney betimleri paylaşıma açılmıştır[1]. Sentetik iris imgelerinin üretilmesi, "kurt örnek"lerin seçilmesi ve bu örneklerin saldırı tespit sistemlerini alt etme ve sisteme sızma performanslarının kıyaslanması için toplam 387 farklı irise ait 2201 imgeden faydalanılmıştır. Bu imgeler aşağıda listelenen 3 farklı veri kümesinden elde edilmiştir:

1) MMU1 [16]: 46 kişinin 90 irisinden beşer imge
2) MMU2 [17]: 100 kişinin 199 irisinden beşer imge
3) CASIAv1 [18]: 108 iristen yedişer imge

387 iris, 5-katlı çapraz geçerlilik testleri için 5 eşit alt kümeye ayrılmış ve her bir katın deneylerinde, bu alt küme içindeki yaklaşık 440 gerçek iris imgesi test, diğerleri ise eğitim için kullanılmıştır. Her bir kat için şu adımlar gerçekleştirilmiştir:

- DCGAN ağının eğitilmesi ve sentetik imgelerin üretilmesi: Eğitim için kayıp fonksiyonu olarak ikili çapraz entropi seçilmiş ve bu kayıp Adam eniyileyici kullanılarak en aza indirilmiştir. Hem üretici hem ayırıcı eğitiminde küme normalizasyonu kullanılmış, öğrenme hızı 0,00001, küme boyutu 16 ve devir sayısı 300 olarak belirlenmiştir. Üretilen sentetik iris imgelerinden örneklere Şekil 2'de yer verilmiştir.
- Sunum saldırısı tespit skorlarına göre örnek seçilimi yapılması: Eğitim kümesinde bulunan gerçek ve DCGAN ile üretilen sentetik imgeler için sunum saldırısı tespit skorları D-NetPAD algoritması kullanılarak hesaplanmıştır. Gerçek imge skorları için tüm katlarda ortalamaların 0,49, standart sapmaların 0,06 olduğu görülmüştür. Kabul-ret örneklemesi öncesi skor ortalaması 0,59 ve standart sapması 0,07 olan sentetik imgelerin dağılım parametreleri örnekleme sonrası gerçek iris imgesi skorları dağılımına yaklaşarak sırasıyla 0,54 ve 0,05'e gerilemiştir.
- Sunum saldırısı başarısına göre örnek seçilimi yapılması: Eğitim kümesinde bulunan gerçek ve üretilen sentetik imgeler için VeriEye yazılımı kullanılarak eş olan ve olmayan skorlar ile saldırı skorları hesaplanmıştır (Şekil 3). Eş olan ve olmayan skorlar için normal dağılım parametreleri kestirimi yapılmış ve elde edilen dağılım fonksiyonları ile sentetik bir iris imgesinin her saldırı denemesi için hesaplanan skorun, eş olan ve olmayan skor sınıflarına ait olma olasılıkları ($P(s|e)$ ve $P(s|\neg e)$) bulunmuştur. Daha sonra bu olasılıklar, $P(\neg E)$ değerini hesaplamada kullanılmıştır (1,2). Bulunan sonuçlara göre, hiçbir saldırısının başarılı olmaması ihtimali en düşük 400 sentetik iris imgesi seçilmiştir.
- Sentetik iris imgelerinden rastgele örneklem alınması: Önerilen seçilim yöntemi ile, sunum saldırısı tespiti modülü ile donanmış bir iris tanıma sistemi için daha tehlikeli sentetik iris örneklerine sahip olunabileceği savı rasgele örneklemler ile karşılaştırma yapılarak desteklenmiştir. Bu doğrultuda, ilk etapta üretilen tüm sentetik iris imgelerinden 400 büyüklüğünde 5 farklı alt küme rastgele örneklenmiştir.



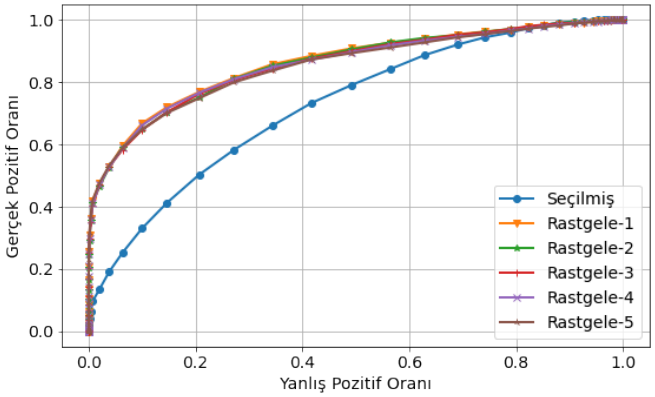
Şekil 3: Gerçek iris imgelerinden elde edilen eş olan ve eş olmayan skor dağılımları

Bu dört adım sonunda, her bir çapraz geçerlilik testi için 7 veri kümesi hazır hale getirilmiştir: Sentetik veri üretiminde ve seçiliminde kullanılmamış yaklaşık 440 gerçek iris imgesinden oluşan gerçek küme, 400 seçilmiş sentetik iris imgesinden oluşan seçilmiş sentetik küme ve 5 adet 400'er sentetik iris imgesinden oluşan rastgele sentetik küme. Elde edilen bu veri kümeleri ile, sentetik imge kümelerinin sunum saldırısı tespiti algoritmasından kurtulma ve kayıtlı kullanıcıların önceden görülmemiş iris verilerine (gerçek küme) eşleşme oranları incelenmiştir.

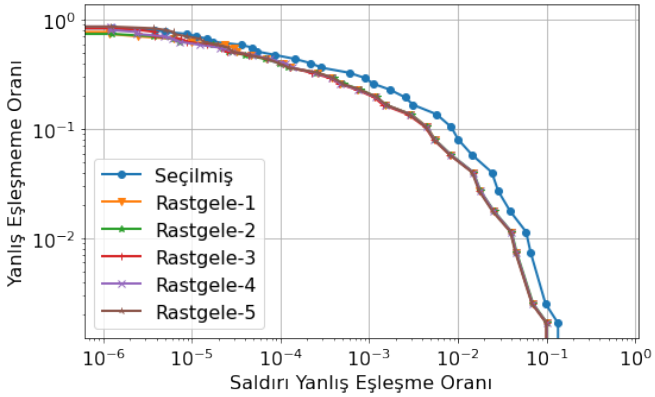
Sunum saldırısı tespiti deneyinin sonuçları Şekil 4'de verilmiştir. Bu grafikte her bir sentetik veri kümesinin gerçek ve yanlış pozitif oranlarının 5-kat ortalaması gösterilmektedir. Farkedildiği üzere, seçilmiş sentetik kümenin sunum saldırısı tespitinden kaçınma kabiliyeti rastgele sentetik kümeden çok daha yüksektir. Ortalama eşit hata oranı rastgele sentetik kümeler için %22,5 seviyelerinde iken, seçilmiş küme ile %34,2 seviyesine çıkmıştır.

Sentetik imgelerin kurt saldırısı senaryosu kapsamında kayıtlı gerçek irislere eşleştirilmesi deneylerinin sonuçları Şekil 5'de verilmiştir. Bu grafikte de her bir sentetik veri kümesi için "saldırı yanlış eşleşme" (Spoofing False Match Rate) ve yanlış eşleşmeme (False Non-Match Rate) ROC eğrilerinin 5-kat ortalaması sunulmuştur. Aradaki fark sunum saldırısı tespiti deneyindeki kadar yüksek olmasa da saldırı başarımındaki artış açıkça görülebilmektedir. Sonuçlar, kayıtlı kullanıcılara ait hiçbir veriye erişim olmaksızın, yalnızca ayrışık bir eğitim kümesi

[1] https://github.com/kaanakdeniz/synthetic_iris_dcgan



Şekil 4: Sunum saldırısı tespiti deneyi sonucunda farklı sentetik veri kümeleri için elde edilen ortalama ROC eğrileri



Şekil 5: Kurt saldırısı deneyi sonucunda farklı sentetik veri kümeleri için elde edilen ortalama ROC eğrileri

kullanılarak yapılan bu seçilim ile biyometrik sistem için daha tehlikeli "kurt örnek"ler elde edilebileceğini göstermiştir.

Şekil 3'de görüldüğü üzere benzersizliği ile iris, sıfır çaba saldırılarına çok dayanıklı olan bir biyometrik modalitedir ve gerçek "kurt örnek"leri bulmak neredeyse imkansızdır. Ancak sentetik veri üretimi ve önerilen seçilim yaklaşımı ile çok daha tehlikeli saldırılar gerçekleştirmek mümkün olmaktadır.

Rastgele sentetik küme için ortalama eşit hata oranları %2,15 iken, seçilmiş küme ile %2,8'e ulaşmıştır. Yanlış eşleşme oranının %0,17, %1,1 ve %10,4 olduğu farklı çalışma noktalarında rastgele sentetik kümelerin saldırı yanlış eşleşme oran ortalamaları sırası ile %10,1, %4,0 ve %0,4 iken, seçilmiş sentetik küme ile %13,5, %5,9 ve %0,8 olmuştur.

V. Sonuç ve Gelecek Çalışmalar

Eşsiz örüntü yapısından dolayı irisin diğer biyometrik özelliklere göre daha güvenilir olduğu kanısı yaygındır. Bu çalışmada, DCGAN kullanılarak üretilen sentetik iris imgeleri arasından, bir iris tanıma sistemine başarılı saldırılar gerçekleştirme olasılığı daha yüksek "kurt örnek"lerin seçilimi hedeflenmiştir. Yapılan deneylerle, biyometrik sistemde kayıtlı kullanıcıların bilinmediği, verilerine erişilemediği bir senaryoda, herhangi bir gerçek iris veri kümesinden çıkartılan istatistiki bilgiler kullanılarak sisteme sızma kapasitesi açısından daha tehlikeli örneklerin tespit edilebileceği gösterilmiştir.

İleriki çalışmalarda sunum saldırısı tespit skorlarına ve gerçek iris ile eşleştirme skorlarına ek olarak kalite metriklerinin kullanılmasına, belirlenecek olan bir "kurt örnek" ölçütü ile üretici sinir ağı kayıp fonksiyonunun uyarlanmasına ve seçilmiş iris kümesinin üretici sinir ağının eğitiminde kullanılması ile saldırı başarımı yüksek iris imgelerinin doğrudan üretilebilmesine yönelik çalışmalar planlanmaktadır.

Kaynaklar

[1] Research Dive, "Biometrics Market Report," https://www.researchdive.com/5051/biometrics-market, Son Erişim Tarihi: 04.07.2023.

[2] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Systems Journal*, vol. 40, no. 3, pp. 614–634, 2001.

[3] M. Une, A. Otsuka, and H. Imai, "Wolf attack probability: A new security measure in biometric authentication systems," in *International Conference on Biometrics*. Springer, 2007, pp. 396–406.

[4] J. Cui, Y. Wang, J. Huang, T. Tan, and Z. Sun, "An iris image synthesis method based on pca and super-resolution," in *Proceedings of the 17th International Conference on Pattern Recognition, 2004. ICPR 2004.*, vol. 4. IEEE, 2004, pp. 471–474.

[5] S. Makthal and A. Ross, "Synthesis of iris images using markov random fields," in *2005 13th European Signal Processing Conference*. IEEE, 2005, pp. 1–4.

[6] J. Zuo and N. A. Schmid, "A model based, anatomy based method for synthesizing iris images," in *International Conference on Biometrics*. Springer, 2006, pp. 428–435.

[7] S. Shah and A. Ross, "Generating synthetic irises by feature agglomeration," in *2006 international conference on image processing*. IEEE, 2006, pp. 317–320.

[8] J. Zuo, N. A. Schmid, and X. Chen, "On generation and analysis of synthetic iris images," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 1, pp. 77–90, 2007.

[9] Z. Wei, T. Tan, and Z. Sun, "Synthesis of large realistic iris databases using patch-based sampling," in *2008 19th International Conference on Pattern Recognition*. IEEE, 2008, pp. 1–4.

[10] A. Radford, L. Metz, and S. Chintala, "Unsupervised representation learning with deep convolutional generative adversarial networks," *arXiv preprint arXiv:1511.06434*, 2015.

[11] N. Kohli, D. Yadav, M. Vatsa, R. Singh, and A. Noore, "Synthetic iris presentation attack using idcgan," in *2017 IEEE International Joint Conference on Biometrics (IJCB)*. IEEE, 2017, pp. 674–680.

[12] S. Yadav, C. Chen, and A. Ross, "Synthesizing iris images using rasgan with application in presentation attack detection," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops*, 2019, pp. 0–0.

[13] A. Jolicoeur-Martineau, "The relativistic discriminator: a key element missing from standard gan," *arXiv preprint arXiv:1807.00734*, 2018.

[14] R. Sharma and A. Ross, "D-netpad: An explainable and interpretable iris presentation attack detector," in *2020 IEEE International Joint Conference on Biometrics (IJCB)*. IEEE, 2020, pp. 1–10.

[15] Neurotechnology, "VeriEye eye iris identification technology, algorithm and SDK for PC, smartphones and Web," https://www.neurotechnology.com/verieye.html, Son Erişim Tarihi: 04.07.2023.

[16] Malaysia MultiMedia University, "MMU Iris Dataset - Iris Database for Biometric Attendance System," https://www.kaggle.com/naureenmohammad/mmu-iris-dataset, Son Erişim Tarihi: 04.07.2023.

[17] Malaysia Multi-Media University, "MMU2 Iris Dataset," https://github.com/thuyngch/Iris-Recognition, Son Erişim Tarihi: 04.07.2023.

[18] Center for Biometrics and Security Research, "Iris Databases," http://www.cbsr.ia.ac.cn/IrisDatabase.htm, Son Erişim Tarihi: 04.07.2023.