Prevention of Adversarial Patches Attack

Terrelle Thomas†  
 Computer & Information Sciences  
 Florida A&M University  
 Tallahassee Florida, USA  
 terrelle1.thomas@famu.edu

Idongesit Mkpong-Ruffin  
 Computer & Information Sciences  
Florida A&M University  
 Tallahassee, FL, USA  
 [idongesit.ruffin@famu.edu](mailto:idongesit.ruffin@famu.edu)

Chutima Boonthum-Denecke  
 Computer Science  
 Hampton University  
Hampton, VA. USA  
 chutima.boonthum@hamptonu.edu

ABSTRACT

Previous research, such as “X-Detect: Explainable Adversarial Patch Detection for Object Detectors in Retail” by Omar Hofman et al. and others, has shown that attackers meticulously select computerized, human-edited inputs—such as 3D image-like patches, for example, toaster-placed in a tabletop scene alongside a banana and notebook—to deceive or manipulate AI models. This type of attack is known as an adversarial patch attack. Attackers deploy adversarial patches with varying characteristics across different scene sections where object detection occurs. We aim to emulate their methodology to understand better how adversarial patches are created and then plan to implement a defense strategy using a Generative Neural Architecture (GNA) with a three-pipeline anomaly detection system to mitigate the use of adversarial patches. This strategy is based on the research “Anomaly Unveiled: Securing Image Classification against Adversarial Patch Attacks” by Nandish Chattopadhyay et al. As the three-step pipeline progresses through the network, the data undergoes a comprehensive process of comparison, analysis, and refinement, all centered around anomaly detection. This process continues until the data is returned in a refined state, effectively neutralizing its potential to function as an adversarial patch.

This approach is accomplished with two neural networks in a generative adversarial setup. Initially, in the segmentation phase, the image is divided into smaller segments, with the GNA model analyzing each segment to detect deviations from the norm, which are indicative of potential adversarial patches. In the second isolation phase, each segment exhibiting deviations is flagged. Lastly, in the blocking phase, the segments with deviations are modified to contain standardized or neutral values, with the goal being that they would be unable to act as adversarial patches, effectively mitigating their intended effect. This process will test against initial algorithms to determine whether a Generative Neural Architecture can effectively mitigate adversarial patch attacks.

CCS CONCEPTS

KEYWORDS

Video Authentication; Adversarial Patches; Object-Detection

ACKNOWLEDGMENTS

REFERENCES

[1] Patricia S. Abril and Robert Plant, 2007. The patent holder's dilemma: Buy, sell, or troll? *Commun. ACM* 50, 1 (Jan, 2007), 36-44. DOI: <https://doi.org/>10.1145/1188913.1188915.

[2] Sten Andler. 1979. Predicate path expressions. In *Proceedings of the 6th. ACM SIGACT-SIGPLAN Symposium on Principles of Programming Languages (POPL '79)*. ACM Press, New York, NY, 226-236. DOI:https://doi.org/10.1145/567752.567774

[3] Ian Editor (Ed.). 2007. *The title of book one* (1st. ed.). The name of the series one, Vol. 9. University of Chicago Press, Chicago. DOI:https://doi.org/10.1007/3-540-09237-4.

[4] David Kosiur. 2001. *Understanding Policy-Based Networking* (2nd. ed.). Wiley, New York, NY..

[5] Hofman, Omer & Giloni, Amit & Hayun, Yarin & Morikawa, Ikuya & Shimizu, Toshiya & Elovici, Yuval & Shabtai, Asaf. (2023). X-Detect: Explainable Adversarial Patch Detection for Object Detectors in Retail.