Adversarial Ornament Attack

Michal Jurgielewicz
Rare Resolutions
rareresolutions@gmail.com

Abstract

This project investigates the surface modulation in architectural and landscape design seen through machine vision. Taking an architectural ornament and logic behind the adversarial attack on deep neural networks as the core elements of project, Ornament Attack explores the perturbations in image capture and recognition systems and their effects in built environment. With the influence of social-media services on tourism and consumerism trends, the current perception of both cities and remote locations are driven by their photogenic attributes, computational power of photo-editing software and recommendation/marketing algorithms networks. Monopoly of such is a disadvantage to the beauty of diversity in representation. Therefore the creation of a constantly evolving physical and digital ornament disrupting machine vision, parallel to the advancement of machine learning and deep neural networks, can not only shift our perception of space, but also add new categories and behaviors to it, along with a new mythology in which machines believe.

Machine eyes

"For art to face the machines, it needs to leave the church of humans and become fully processual and transmittable." [1]

Nowadays, we live in a global, highly connected and automated world. Every day we take an active part in an exponential flow of media, products, ideologies, money and technologies. That movement, equipped with tools and platforms aided by neural networks and machine learning, entered our everyday life and reshaped not only our built environment, but the way we experience it. Every time we look at our smartphone or browser, our world gets automatic auto-correction.

We wander streets, visiting places that somehow appear, on top of our search results in Google Maps or TripAdvisor. We communicate with hashtags on Instagram and through our satellite eye we travel to places, events, and other people's life moments while going to work every morning. We purchase products shipped to us through a network of ports and logistic centers located in remote locations operated by the same algorithms that stream our media. If you liked that, then you will love this - tells us our feed constantly. All this is pinned to the precise location of our own behavioral map. "Today's culture as global culture is very much the processes of de- and reterritorialization. It should be remarked, that "territory" in the ethnological sense, is understood as the environment of a group that cannot itself be objectively located, but is constituted by the patterns of interaction through which the group secures a certain stability and location." [2]

However, in this world of constant optimization and technological advancement we do not take the central place. Companies like "Google, Facebook or Amazon don't have users or customers [as we would like to think about ourselves]. Instead they have participants under the machine surveillance." [3] The same companies that provide us with platforms and tools for our everyday life, now design cities and "countryside" for machines that operate next to us. Always-watching autonomous cars and drones delivering our mail are only a prologue to true smart-cities with homes controlled by always listening Amazon Echo type -like assistants and, before we ask ourselves about its architecture, we should understand different relationships that exist in our environment. "Human to human, human to machine and machine to machine - what is the real nature of

these?" [4] How do machines see and how do they locate themselves in this complex network of assumptions about them? Finally, if architecture is not only a building, but also an infrastructure, what are the spatial implications of that? "What happens when the information necessary to comprehend and operate the environment is not immanent to that environment, but has become decoupled from it? When signs, directions, notifications, alerts and all the other instructions necessary to the fullest use of the city appear only in augmentive overlay and, as will inevitably be the case, that overlay is made available to some but not to others?" [5] On the other side, what are machines capable of seeing?

In planetary-scale operations, the Earth is being constantly rendered, unfolding new terrains, structures and behaviors unknown to our sensorium, yet intertwined with the landscape we occupy. In these conditions, Adversarial Ornament Attack becomes the semi-geological force shaping the environment with traces of technological progress new to human culture and machines. This project is a speculative fiction approach to explore the relationship between privacy, space and data. It is a story about the enclaves where you cannot take a photo because the façade patterns and areas are invisible to autonomous-car traffic by their architectural design. However, it is also the story about landscapes emerging in these conditions, perceived only by the machines, created by the collisions in the image classifiers. Adversarial Ornament Attack is filled with nostalgia for the unknown, cities, places and landscapes that exists in our imagination until visited. It mixes craftsmanship with fabrication and neural networks to construct new environments for humans and for the machines to explore, from machine eye perspective.

Adversarial Attack

Adversarial Attack on Deep Neural Network (DNN) is a subtle modification of an image, invisible to the human eye, which results with misclassification of the image by DNN interpreter. Recent findings show that these networks are very vulnerable to adversarial attacks, even when modified and printed images are captured by regular smartphone camera and tested. 3D objects with a slight change of the texture are misinterpreted as well. A turtle is a rifle, a baseball becomes an espresso cup.

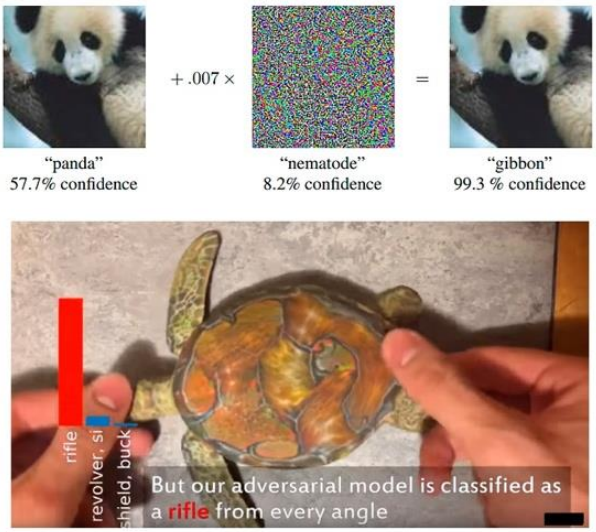

Fig 1. Top: Example Attack, *Explaining and Harnessing Adversarial Examples*, 2015, Ian J Goodfellow, Jonathon Shlens, Christian Szegedy, image, Cornell University Library, Bottom: Fooling Image Recognition with Adversarial Examples, *MITCSAIL Youtube Channel*, 2017, Anish Athalye, Logan Engstrom, Andrew Ilyas, Kevin Kwok, video, MIT

References

1. Mohammad Salemy, *Art after the Machines, Supercommunity: Diabolical Togetherness Beyond Contemporary Art* (London: Verso, 2017), 345.
2. Ryszard Wolny, "Gilles Deleuze and Felix Guttari's Concepts of Deterritorialisation and Retteriorialisation as Globalisation of Culture," 37.
3. Bruce Sterling, *An Epic Struggle of the Internet of Things* (Moscow, Strelka Press, 2014) 8.
4. Theodore Spyropoulus, *Future Culture* (London, AA Lecture Series, 2018).
5. Adam Greenfield, *Radical Technologies: The Design of Everyday Life* (London: Verso, 2018), 176.

Biography

Michal Jurgielewicz is an architect, founder of Rare Resolutions, an investigative architecture agency currently based in Bangkok, exploring

possible presents through constantly changing cultural, technological and geographical landscapes. He took part in international festivals, exhibitions, workshops and seminars in Poland, Italy, The Netherlands.