Deep-Rooted Images: Situating (Extra) Institutional Appropriations of Deepfakes in the US and India

Kailyn Slater and Akriti Rastogi

The paper aims to map institutional and extra-institutional affordances and appropriations of deepfake images through an analytical framework that accounts for the socio-political contexts of the US and India. Our main argument involves the inevitable leakage of technologies outside institutions and its redressal through corporatized comebacks. Utilizing vernacular and global examples, we trace the perceived ownership and extended modalities of deepfake images and videos. While compositing (Manovich 2006) and habitual media (Chun 2016) predetermine our deep mediatized world (Hepp 2019), deepfakes, as a visual cultural technology newly popular within the political economy of media, offer a novel entry point into locating the neoliberal ethos of both socio-political contexts and their respective apparatuses and valences of control. Thus, the paper articulates the coordinates of deepfake affordances to situate the technological power and political rhetoric that governs our international media situation across differing but interrelated socio-political contexts.

Introduction

To look at a deepfake image is to encounter synthetic media of the highest order. In other words, deepfake imagery offers verisimilitude to the actual image in a way that the specter of indexical truth comes back to haunt us with a vengeance. Indeed, if we examine the event of local elections in 2022 in India’s capital city New Delhi, deepfake videos of the member of governing bodies threatened to collapse the existing ruling government body.1 In its nascent days, the institutional appropriation of deepfake technology resurfaced the debates around the ontological questions around images (Lund 2021). For contexts downstream of the technological innovation like India, these appropriations translated into pirated renditions where any technophile could manipulate and re-appropriate the technology for mass customized images. Combing through Instagram profiles of deepfake enthusiasts, ephemeral pages carrying deepfake images of Hindi film actors and actresses kept appearing and disappearing from the platform. What remains in a yearlong observation of the keyword “deepfake Bollywood” is the remediation of a Kardashian figure with a Bollywood actor’s face. Deepfake enthusiasts like Indian Deepfaker (now dormant on Instagram) drew images from mr.deepfakes.com—a website originating from the US and finding translations across the globe.

Deepfakes are typically known as short videos that directly impose the likeness of someone onto someone else, particularly someone who is quickly culturally recognizable and in such a fashion that the imposition complicates the viewer’s visual, subjective perception of both the preliminary body and the intended mimicry that is projected onto the target of the video. These videos are deemed controversial due to this altering of perception and are found throughout most national contexts as memes that go viral, heralded as a widespread technological phenomenon that confuses and disrupts the previously seamless image to convey a different—and usually objectionable—message. Their categorization among the cringe spectrum of memes varies, from shoddy and obvious face-swaps with poorly matched voiceovers to impeccably fabricated, seamless narratives that the human senses could barely distinguish differences between (Paris and Donovan 2018).
Journalists, as well as scholars in communication, media studies, and computer science, have discussed the problems posed by deepfakes and the machine learning technology they are made synonymous with, particularly concerning the phenomenon’s potential and realized applications as mechanisms for abjection (Cole 2020a, 2020b, Cole & Maiberg, 2020, van der Nagel 2018). While not making a specifically psychoanalytic argument, we contend that what stems from the anxiety surrounding deepfake technology is a generalized fear of the unknown and the unmeasurable, particularly as these anxieties fuel the polarized political environment of the United States. The construction of identity in democratic societies relies heavily upon the consistency of the image as it correlates to concrete identifying information, stored and maintained by carceral and governing organizations (in order to prove you are whom you say you are, you must have a picture ID that corresponds to a first and last name, the address in which you reside, on your person in case of trouble, or else). In a neoliberal democracy, any aesthetic mechanism meant to disrupt that consistency is duly perceived to disrupt social norms and cause panic among those whose image and information have always aligned. For these reasons and more, deepfake videos pose many ethical and moral dilemmas for intellectual and institutional debate across disciplinary contexts.

Deepfake videos go viral because they cause us to second-guess our perceptions of people we come to know through their appearance and performance of sociocultural identity, like celebrities, influencers, and politicians—and depending on the circumstances, we may find that confusion hilarious. A type of meme, deepfakes make adjacent commentary on the assembled relationship between the intention of the posted image (or video) and the subversive meaning meant to be gleaned by the viewer. However, deepfakes differ from memes in their active, rather than passive, ability to construct the visual imaginary—one produced by the performance of an in-group or culturally relevant identity—as darkly abject. There is synthetic meaning in the form of overlapping edges, data moshed differences, and forcibly-intersected identities to be grasped by the viewer of a deepfake.

Deepfake videos as composite digital objects

How do we come to understand deepfakes synthetic demonstration of subjectivity? To pin down what exactly is at stake when discussing deepfakes as vehicles of meaning, we first assert that videos are a specific type of digital object, produced through the tripartite relation of fabricated material to substantive concept to perceptible movement. Yuk Hui (2012: 380-1) defines digital objects as “simply objects on the Web...that [are] composed of data and formalized by schemes or ontologies that one can generalize as metadata” and “constitute a ubiquitous milieu from which we cannot escape.” They are all around us, on any digital device we may interface with, and provide the fodder for our everyday lives as we log onto social media platforms, video streaming services, and any application that relies on wired connections to produce something within screen-based view. An innumerable amount of videos conveying synthesis exist on and because of the Internet. However, some were constructed through analog means, particularly in artistic circumstances like celluloid film production and performance utilizing audiovisual sequencer machines to produce electronic colors and sounds. Marking this material distinction between analog and digital in making videos is crucial because it informs our understanding of the objects and tools utilized in producing deepfakes and their subsequent existence as digital objects as they relate to other audiovisual forms of media displayed on mediated screens. While analog-processed video can be used as footage for digital videos, for this paper, we are focusing on videos that are meant to be digitized, intentionally involve pre-and post-production software editing processes, and come to exist as digital objects to be shared on digital and physical viewing platforms.

Hui forms the digital object in part from Simondon’s notion of the technical object (1980), further expanding to the technical individual and its subsequent interaction system. Technical objects regain their materiality by engaging with an associated milieu and thus attain a differing degree of perfection from what mechanical systems expect regarding cybernetics (Hui 2012, p. 386). Hui then contrasts Simondon with Heidegger’s two modes of categorization of technical objects: things get rendered as objects to be either ready-to-hand or present-at-hand, depending on the subject’s desire for essentialization or functional interaction. Knowing the essence of a thing fully versus being
simply able to use it, for Heidegger (2001), are two distinctly different modes of understanding technical objects as they coordinate with the social milieu, rather than the granularly technical, such as Simondon (ibid.). With this understanding, in challenging the discourse of deepfakes, we specifically absorb Hui’s inference that Heidegger’s approach toward technical objects has been taken up by “AI researchers as a challenge in the design of intelligence” (Hui 2012, p. 387). We draw on these philosophers to better mitigate discussions in the study of artificial intelligence that stratify the issues of human ability and machine function to an intensely ubiquitous scale as the manageable effector for all of society’s ills, i.e., tech-solutionism. Recent conversations about what constitutes the ‘metaverse’ of digital technologies as they are constructed through virtual reality provide a necessary ground for the discursive frame for which we interrogate Hui’s inference.

Altogether an issue of objectivity versus subjectivity, deepfakes are aestheticized and politicized through their association with gimmick and controversy (Ngai 2020). The inability of platforms to moderate ethically casts reasonable doubt on the way media industries and social institutions could process this influence of deepfakes, as what we argue to be sociocultural and political devices situated within discourses of reactionary politics, uncanny embodiment as represented through abjection, and the ever-present potential of life-disrupting disinformation. Individuals with a decent level of coding ability or an artistic eye are able to detect that these videos—made from a haphazard collection of images trained to modify the likeness of a figure through algorithmic pattern recognition—are deeply fake. For everyone else, the ability to notice the difference between tricky actors in a deepfake relies on digital literacy, sensitivity to cultural nuance, and the “acute mediation of the ways affect can take form in a crisis-intensified historical present,” or what Lauren Berlant in Cruel Optimism (2011) called intuition: “the process of dynamic sensual data-gathering through which affect takes shape in forms whose job it is to make reliable sense of life.” In these contexts, users are subject to a double-bind of intuition: platforms retain operational control over how creative, cultural media is both produced and consumed, structuring the digital political economy on precarity, illusion, and ignorance (Cunningham, 2019; Gillespie, 2010).

The appeal of deepfake videos as meme-like gimmicks emerged as a viral widespread culture phenomenon at the end of the 2010s. While many popular deepfakes go viral for their uncanny resemblance to real people and real-life scenarios, the artificially intelligent technology instrumentalized to fabricate these videos is being used for sowing misinformation and intentionally obfuscating an individual’s identity for disinformation and socio-political disruption. As the Western perspective on artificial intelligence idealizes Silicon Valley’s capitalization of digital aesthetics, deepfakes can easily be fashioned as a vessel for image manipulation done to marginalized publics at the hands of those in power, i.e. platforms and their agents therein. Institutional discourses continue to purport deepfakes as an issue of national security related to terrorism and the protection provided by consistent diplomatic messaging. American legislation like the Deepfakes Accountability Act has introduced the notion of synthetic media into legal discussions of digital pornography.

Deepfake videos as tools for disinformation

While it should be recognized that disinformation is a conceptual extension of propaganda, the harms being caused by deepfakes and their corresponding modes of production are amplified by infrastructures of face-based surveillance, like facial recognition technology (FRT) and biometric graphing, e.g., fixed identity-based digital affordances (Wojewidka 2020). The increasing integration of automated machine learning practices in the dispersion of information, such as in the interest-based display of news content and indexing of search results, promotes discord over notions of community belonging and collective truth that could otherwise be ascertained without an intense focus on individual and personalized interest. Deepfakes, as animated manifestations of intensified interest set on disrupting the image and likeness of a socially relevant figure, invite an attitude of communicative entitlement based on individually-constructed preference and, we argue, shape the value one can reasonably place on susceptibility to harm in online environments.
Deepfakes, made from pixels, necessitate the need for a combined aesthetic and communicative analysis in order to understand them as individual videos, images, or likenesses manipulated by procedurally automated scripts. Deepfakes affect political publics, destabilizing the activity that glues industry standards to infrastructure and exposing faulty moderating systems in political law and technological programming. Ultimately, deepfakes have the potential to trick inefficiently automated systems into revealing the technological, communicative, and aesthetic mistakes made by its creators, distributors, and users alike. The purpose of this paper is then to draw attention to the problems that deepfakes pose to the constructions of cultural memory and digital sovereignty under an infrastructure that prioritizes techno-capitalism (Chun 2016), spotlighting the United States and India.

Social media platforms like Facebook, purported by Meta, provide the foundation for disinformation to spread with their notorious hands-off approach to content moderation that privileges the right of any individual actor to speak rather than appeal for the right not to be harmed. Meta’s control over various other social media platforms and messaging applications, like Instagram and WhatsApp, expand their vector of power over the parameters of social discussion and connection across international borders. In an effort to inform the interested public of developments in their software, Meta keeps an active blog to report innovations in company artificial intelligence research.3

The Black Box of Deepfakes

Deepfakes are created using machine learning frameworks called generative adversarial networks (GANs). Utilizing found footage to compound, manipulate and warp the image of another that similarly aligns with features of an original image or through the video’s color values and representation of edges and lines, deepfakes are not simple by any means. In fact, we argue that deepfakes in their application are meant to complicate the data presented to the viewer in the form of image manipulation, seeking to invoke the stylistic intent of the producer as a fabrication of and as a mechanism for the display of power through automation and alteration of meaning. GANs operate through two channels: as a generator of data and a discriminator of data. The generative channel of a GAN seeks to synthesize data that appears to be the new data as it is being trained against the latter system of discernment and discrimination. In order for the discriminator channel to discern what is real and what is fake, the discriminator channel functions to accurately classify the synthetic data as fake and the training data as accurate (Harrod 2020). The GAN’s objective then becomes embedded in a mechanistic authentication network, discriminating data trained against the other set incorporated into the network to determine whether it is accurate or fake. In this process, the GAN does not produce an ultimately absolute or true piece of data but comprises a dual synthesis system and the reassurance of that synthesis. What is produced by the GAN cannot be separated from the algorithmic framework it was constructed in—except when this synthesis process is recorded and captured on the screen in the post-production stage, becoming what we observe as the source material of a deepfake video. As generator channels become better at recognizing aspects of the synthesis occurring between the content placed in the network, discriminator channels are enabled to make increasingly quick decisions about how to change the image or video to suit the objective of the GAN. The architecture of the GAN identifies “unique artifacts” in an image or video, and the results from the generator/discriminator mechanism “deteriorate[s] when the GAN architecture is changed” (Yu et al. 2019). Nevertheless, what are these unique artifacts, and how do they become materially distinct from the GAN’s architecture? We know that GANs leave behind something adjacent to what we would call digital watermarks or image fingerprints: visual indicators or vectored remnants that represent the residual reconstruction of images after being implemented into a GAN model (Yu et al. 2019).

Watermarking places a name or other representative signifier on an image or video to denote the object as owned by an individual or organization and typically involves an explicit security structure and the intent to preserve intellectual property. GANs iterate model-specific types of feature-based signification to keep the visual integrity of the image cohesive at all stages of the network’s process, as designated through interaction with the training data and the imposition of an “initialization seed” (Yu et al. 2019). This process of organizing model-specific types is how aspects of the human face stay together cohesively as the deepfake video mutates. Measuring bands of frequency and

FAST CAPITALISM

Volume 19 • Issue 1 • 2022
patches of color by combining two or more images integrated into the GAN, Yu et al. (2019) postulate that a deepfake-specific fingerprint can be attributed to and lifted from the final deepfaked image by pooling together the pixels that correspond to statistical frequencies chosen in response to the GAN’s trained to function. The attribution of aspects in a deepfake that determine its authenticity and, therefore, its identity, “comes down to attributing a depiction of bias” presented by whoever initializes the models set in place at the beginning of GAN training (Zhang et al. 2021). Past this manual attribution, experiments utilize auto-encoding techniques and other designated parameters provided by the producer (or group of producers) to reconstruct extracted samples of the images and accomplish a visualization of its unique imprint (Karras et al. 2019; Qi et al. 2020; Tolosana et al. 2020; Yu et al. 2019; Zhang et al. 2021).

Deepfake videos, in particular, can thus maintain their own unique identity generated, discerned, and optimized from their GAN and cannot be thoroughly authenticated or verified if the models integrated into the GAN do not correlate with what application processing interfaces, or APIs, have been trained to look for. Deepfakes are auto-encoded at every stage of the production process: once finalized and made into a complete video post-GAN, the fabricated videos are virtually indistinguishable from other sorts of video files that happen to be imported into content production applications and onto video streaming websites. It is for this reason that we discussed the importance of differentiating analog from digital video, as the construction of deepfakes in effect mimics the production process of analog video; the implementation of source material into a perceptive apparatus. Already embedded with their own, typically black-boxed, systems of security protocol, websites that enable the uploading of videos tend to encode media as it is being imported into its system for the purposes of analytical tracking and high, clear quality for observation (Cole 2020b). Our paper seeks to understand how, if at all, video streaming sites can stabilize the onslaught of unverifiable, yet obviously fabricated, amateur videos such as deepfake pornography (van Der Nagel 2020).

Detection methods that emphasize discerning or discriminating the real from the fake through techniques similar to FRT have commercial relevance, like services to find and warn individuals if someone made a deepfake of them or someone they know through Sensity.AI (Ajder et al. 2020). Because each deepfake video is generated in model-dependent and -specific ways, approaches that only investigate the discriminator channel will always be behind methods that can pinpoint the aspects of images that are abstracted, manipulated, and obfuscated with automated ease within the GAN (Harrod 2020).

StyleGAN, an alternative generator architecture for GANs known for its utilization in the This Person Does Not Exist project, provides a functional model of ascertained stochastic features found in a Flickr dataset of faces (termed “facesets”) in order to normalize standard sets of human facial expressions (Karras et al. 2019). Seeking to optimize the process of style transfer as the network trains against authentic or other synthetic images, StyleGAN focuses its vectors of alteration on the generator channel rather than improving simply on the discriminator end (Huang et al. 2017; Karras et al. 2019). We argue that this factor of normalization that can be integrated into the GAN through the StyleGAN (and later StyleGAN2) models are relevant because this integration of stylistic type 1) recognizes embodied characteristic as they are exemplified in the image or video, and 2) emphasizes the ability of style transfer, or perhaps more aptly named style power, to grasp the modes of changeability and material presence of the facesets that are implemented into typical GAN models, in a visual way that goes beyond code and algorithmic configuration.

Experimental methods that intervene for the generative channel, like DeepRhythm, are able to graph the blood flow and heartbeat occurring within the targeted individual in order to examine deepfake videos through remote visual photoplethysmography: the monitoring of minuscule changes in skin color over a while, to detect whether the human person represented in the video is real or fake (Qi et al. 2020). With these experiments that measure levels of oscillation in heart rhythms to determine proof of life, there is little to no discussion of sociopolitical limitations, e.g., the ethnically apparent and racially specific boundaries that are crossed when fabricating a deepfake someone who is white into someone that is not. By examining frequency rather than, for example, the demarcation of red or blue hues found in the face, approaches like DeepRhythm are interesting for GAN-detection methods that detect human liveness by measuring frequencies. In the next section, we turn toward the vernacular appropriation of deepfakes.
Pirate Affordances

The emergence of an almost cottage industry of deepfake creation has led to resurfacing of debates about technological appropriations and affordances. While complaint and redressal mechanisms (Ahmed 2021) offer one the modalities to channel the technology back into the institutional rendition, what remains a long-standing precondition concerning technology is the inherent leakages in the supply chain of technologies. To position this debate with respect to technologies and institutions, we revisit the argument of pirate appropriations as proposed by Ravi Sundaram (2011). Little has changed in the way technologies translate on the local surface in vernacular usage. Moreover, with social media platforms becoming the primary sites for institutional encounters, including election campaigns, deepfake technology disperses as a vernacular practice of playing photoshop with celebrity images on one end and fudged representations of electoral candidates on the other end. The range of these vernacular appropriations varies between entry-level amateur to a more sophisticated IT cell-driven maneuver made to influence voting institutions. While click farms are another dimension to this pirate appropriation and manufacture of numbers on social media accounts of public figures, deepfake images offer a new rendition of informal technological leakages.

We trace the affordance evidence on Instagram pages of deepfake creator accounts concerning Indian celebrities. One of the visible examples here is The Indian Deepfaker – with a follower count of almost ten thousand followers, deepfakes created by the account often comment upon the socio-political events of the world. In a recent turn of events, the account has posted about the tense Ukraine situation, in addition to posts that address some of the most vocal public figures from the Hindi film industry. In a direct message conversation with one such account, they commented how easy it was to get access to stock images of celebrities, and indeed, with better tools and access, they could recreate the image with actions (sic). The gestural economy of most public figures then emerges as a contentious site that is usually mapped using artificial intelligence tools.

Further, deepfake technologies also find ample institutionalized appropriation in advertising platforms in India. The food and beverage giant Cadbury chocolates created deepfake videos of Hindi film star Shahrukh Khan in an advertising campaign. We refer to the video posted on their channel on YouTube, where the advertisers have designed the campaign foregrounding the use of deepfake technology to revive the small and medium local businesses during the harvest festival of the fall season called Diwali or the festival of lights. The advertisement opens with the citation: “This is not just a Cadbury ad. The stories mentioned in this ad are part of thousands of local stories that Cadbury is promoting this Diwali.” Quickly followed by the mise-en-scène of festivities unfolding in an Indian household with Shahrukh’s deepfake pronouncing support for the names of local proprietors like home-grown bakers and confectioners, sweet shops, and other miscellaneous businesses in the festive season. The advertisement stands out because it uses Shahrukh’s gestural economy to connect with the audiences with emotional contagion. The timing of the advertisement wherein the advertisement gathered viral view counts owing to star power and holiday season tractions. The advertisement ends with the caption: “Make your ad on NotJustACadburyAd.com.” Conceptualized by Ogilvy and Wavemaker ad agencies, the outreach of the campaign was hyperlocal—covering nearly three hundred plus pin codes across India. Further, the advertisement promotes the use of Shahrukh Khan’s deepfake videos to support local businesses and that the campaign is participatory. Perception building around the brand’s ad campaign pushed for shifting the business requirements of local vendors and mainstreaming the appropriation and usage of deepfakes more openly and publicly. While the ad campaign in and of itself does not mean that internet users in the vernacular contexts shifted to deepfake creation, the process of deepfake creation here, became a site of novelty and aspiration for tech enthusiasts.

Conclusion

In a deep mediatized (Hepp 2019) world, deepfakes complicate and muddy the waters of image economies for nearly every stakeholder in the ecosystem. While deepfakes find appropriations across contexts, it becomes critical to understand the deep-rooted political economy governing this technology. Not only in the Silicon Valley, but this imaging technology feeds into the big corporates connected with celebrity footing, as in the example of the...
Cadbury Ad. Deepfakes are products of instruments for audio and video synthesis that come to have meaning in sociocultural and political contexts through their entrenchment in powerful apparatuses of media control, as objects, catalysts for disinformation, and profit through machine learning techniques. Further, in the age of Web 3.0, with non-fungible tokens (NFTs) emerging as digital possessions for the Metaverse, the next discursive ecosystem of synthetic media appears to follow the same logics of commerce as that of “real” media ecosystems in existing media industries of the world.
Endnotes


2 Popular American cable news programs like 60 Minutes spotlighted these problems posed by deepfakes in a special broadcasted on October 10, 2021, interviewing author of Deepfakes: The Coming Infocalypse Nina Schick and deepfake artist Chris Ume.

3 How these innovations are meant to demonstrably effect these interested publics beyond the creation of the Metaverse is yet to be seen.

4 Source: https://www.youtube.com/watch?v=R3FnhpelBR0, last accessed on September 13, 2022

5 Source: https://www.wpp.com/featured/work/2021/03/ogilvy-and-wavemaker-notjustacadburyad, last accessed on September 13, 2022
References


Applications, 6, 100134.


