COUNTERFACTUALS UNCOVER THE MODULAR STRUCTURE OF DEEP GENERATIVE MODELS

Anonymous authors
Paper under double-blind review

ABSTRACT

Deep generative models can emulate the perceptual properties of complex image datasets, providing a latent representation of the data. However, manipulating such representation to perform meaningful and controllable transformations in the data space remains challenging without some form of supervision. While previous work has focused on exploiting statistical independence to disentangle latent factors, we argue that such requirement can be advantageously relaxed and propose instead a non-statistical framework that relies on identifying a modular organization of the network, based on counterfactual manipulations. Our experiments support that modularity between groups of channels is achieved to a certain degree on a variety of generative models. This allowed the design of targeted interventions on complex image datasets, opening the way to applications such as computationally efficient style transfer and the automated assessment of robustness to contextual changes in pattern recognition systems.

Figure 1: Counterfactual manipulation of samples of a BigGan trained on ImageNet (see section 4.2).

1 INTRODUCTION

Deep generative models, by learning a non-linear function mapping a latent space to the space of observations, have proven successful at designing realistic images in a variety of complex domains (objects, animals, human faces, interior scenes). In particular, two kinds of approaches emerged as state-of-the-art (SOTA): Generative Adversarial Networks (GAN) (Goodfellow et al. 2014), and Variational Autoencoders (VAE) (Kingma & Welling 2013; Rezende et al. 2014).

Efforts have been made to have such models produce disentangled latent representations that can control interpretable properties of images (Kulkarni et al. 2015; Higgins et al. 2017). However, the resulting models are not necessarily mechanistic (or causal) in the sense that interpretable properties of an image cannot be ascribed to a particular part, a module, of the network architecture. Gaining access to a modular organization of generative models would benefit the interpretability and allow extrapolations, such as generating an object in a background that was not previously associated with this object, as illustrated in a preview of our experimental results in Fig. 1.

Such extrapolations are an integral part of human representational capabilities (consider common expressions such as "like an elephant in a china shop") and consistent with the modular organization of its visual system, comprising specialized regions encoding objects, faces and places (see e.g. Grill-Spector & Malach 2004). Extrapolations moreover likely support adaptability to environmental changes and robust decision making (Dvornik et al. 2018). How to leverage trained deep generative architectures to perform such extrapolations is an open problem, largely due to the non-linearities and high dimensionality that prevent interpretability of computations performed in successive layers.
In this paper, we propose a causal framework to explore modularity, which relates to the causal principle of Independent Mechanisms, stating that the causal mechanisms contributing to the overall generating process do not influence nor inform each other (Peters et al., 2017). We study the effect of direct interventions in the network from the point of view that the mechanisms involved in generating data can be modified individually without affecting each other. This principle can be applied to generative models to assess how well they capture a causal mechanism (Besserve et al., 2018).

We introduce a general framework to formulate precisely the notion of disentanglement and bridge it to causal concepts. This theory section will be presented informally to ease high level understanding. Readers interested in the mathematical aspects can refer to Appendix A where we provide all details.

### Related work

Our work relates to the interpretability of convolutional neural networks, which has been intensively investigated in discriminative architectures (Zeller & Fergus, 2014; Dosovitskiy & Brox, 2016; Fong & Vedaldi, 2017; Zhang et al., 2017a). Generative models require a different approach, as the downstream effect of changes in intermediate representations are high dimensional. InfoGANs, β-VAEs and other works (Chen et al., 2016; Mathieu et al., 2016; Kulkarni et al., 2015; Higgins et al., 2017) address supervised or unsupervised disentanglement of latent variables related to what we formalize as extrinsic disentanglement of transformations acting on data points. We introduce the novel concept of intrinsic disentanglement to uncover the internal organization of networks, arguing that many interesting transformations are statistically dependent and are thus unlikely to be disentangled in the latent space. This relates to Bau et al. (2018) who proposed a framework based on interventions on internal variables of a GAN which, in contrast to our fully unsupervised approach, requires semantic information. Higgins et al. (2018) suggest a definition of disentanglement based on group representation theory. Compared to this proposal, our approach (introduced independently in (Anonymous, 2018)) is more flexible as it applies to arbitrary continuous transformations, free from the strong requirements of representation theory (see Appendix F).

### 2 FROM DISENTANGLEMENT TO COUNTERFACTUALS AND BACK

We introduce a general framework to formulate precisely the notion of disentanglement and bridge it to causal concepts. This theory section will be presented informally to ease high level understanding. Readers interested in the mathematical aspects can refer to Appendix A where we provide all details.

#### 2.1 A CAUSAL GENERATIVE MODEL (CGM) FRAMEWORK

We consider a generative model $M$ that implements a function $g_M$ which maps a latent space $\mathcal{Z}$ to a manifold $\mathcal{Y}_M$ where the learned data points live, embedded in ambient Euclidean space $\mathcal{Y}$ (Fig. 2a). A sample from the model is generated by drawing a realization $z$ from a prior latent variable distribution with mutually independent components, fully supported in $\mathcal{Z}$. We will use the term representation to designate a mapping $r$ from $\mathcal{Y}_M$ to some representation space $\mathcal{R}$ (we also call $r(y)$ the representation of a point $y \in \mathcal{Y}_M$). In particular, we will assume (see Def. 6 and Prop. 4 in Appendix A) that $g_M$ is (left)-invertible, such that $g_1$ is a representation of the data, called the latent representation.

Assuming the generative model is implemented by a non-recurrent neural network, we can use a causal graphical model representation of the entailed computational graph implementing the mapping $g_M$ through a succession of operations (called functional assignments in causal language), as illustrated in Fig. 2b that we will call Causal Generative Model (CGM). In addition to the latent representation, we can then choose a collection of possibly multi-dimensional endogenous (internal) variables represented by nodes in the causal graph, such that the mapping $g_M$ is computed by composing the endogenous variable assignment $v_M$ with the endogenous mapping $\tilde{g}_M$ according to the diagram

\[
\mathcal{Z} \xrightarrow{v_M} \mathcal{Y}_M \xrightarrow{\tilde{g}_M} \mathcal{Y}_M.
\]

A paradigmatic choice for the internal representation is to use the collection of output activation of each channel in one hidden layer of a convolutional neural network, as illustrated in Fig. 2c. As for...
the latent case, we use mild conditions that guarantee $\tilde{g}_M$ to be left-invertible, defining the internal representation of the network (see Def. 6 and Prop. 3 in Appendix A). Given the typical choice of dimensions for latent and endogenous variables, the $V_k$’s are also constrained to take values in subsets $V_k^\mathcal{E}$ of smaller dimension than their Euclidean ambient space $V^k$. As detailed in Appendix A, we will denote the endogenous image sets of the form $\mathcal{V}_M^\mathcal{E} = \{v \in \prod_{k \in \mathcal{E}} V_k^k : v = (v_k(z))_{k \in \mathcal{E}}, z \in Z\}$ for a subset of variables indexed by $\mathcal{E}$ (amounting to $\mathcal{V}_M$ when $\mathcal{E}$ includes all endogenous variables).

This CGM framework allows defining counterfactuals in the network following Pearl (2014).

**Definition 1** (Unit level counterfactual, informal). Given CGM $M$, the interventional model $M_h$ is obtained by replacing assignments of the subset variables $\mathcal{E}$ and by the vector of assignments $h$. Then for any latent input $z$, called unit, the unit-level counterfactual is the output of $M_h$: $g_M h(z)$.

Def. 1 is also in line with the concept of potential outcome (Imbens & Rubin, 2015). Importantly, counterfactuals induce a transformation of the output of the generative model.

**Definition 2** (Counterfactual mapping). Given an embedded CGM, we call the transformation

$$\hat{Y}_h^\mathcal{E} : y \mapsto g_M h \left( g_M^{-1}(y) \right)$$

the $h$-counterfactual mapping. We say it is faithful to $M$ whenever $\hat{Y}_h^\mathcal{E} [\mathcal{Y}_M] \subset \mathcal{Y}_M$.

We introduce faithfulness of a counterfactual mapping to account for the fact that not all interventions on internal variables will result in an output that could have been generated by the original model. In the context of generative model, non-faithful counterfactuals generate examples that leave the support of the distribution learned from data, possibly resulting in an artifactual output (assigning a large value to a neuron may saturate downstream neurons), or allowing extrapolation to unseen data.

### 2.2 Unsupervised Disentanglement: From Statistical to Causal Principles

The classical notion of disentangled representation (e.g. Bengio et al. (2013); Kulkarni et al. (2015)), posits individual latent variables “sparsely encode real-world transformations”. Although the concept of real-world transformations remains elusive, this insight, agnostic to statistical concepts, has driven supervised approaches to disentangling representations, where relevant transformations are well-identified and manipulated explicitly using appropriate datasets and training procedures.

In contrast, unsupervised learning approaches to disentanglement need to learn such real-world transformations from unlabeled data. In order to address this challenge, SOTA approaches seek to
We propose a non-statistical definition of disentanglement by first phrasing mathematically the notion of disentanglement. As illustrated in the CGM of Fig. 2b, in contrast to latent variables, properties encoded by endogenous variables of the graphical model are not necessarily statistically independent due to common latent variables available to encode other properties. More explicitly we have

\[ T(z_1, \ldots, z_K) \rightarrow (z_1, f(z_k), \ldots, z_K), \quad \text{and} \quad T(g_M(z)) = g_M(T'(z)). \]

It is then natural to qualify two transformations \( T_1 \) and \( T_2 \) as disentangled (from each other), whenever they modify different components of the latent representation (see Def. 9). This amounts to saying that the transformations follow the causal principle of independent mechanisms. We thus need to exploit a different representation to uncover possibly statistically related properties, but disentangled in the sense of our definition.

### 2.3 Disentangling by Manipulating Internal Representations

As illustrated in the CGM of Fig. 2b, in contrast to latent variables, properties encoded by endogenous variables of the graphical model are not necessarily statistically independent due to common latent cause, but may still reflect interesting properties of the data that can be intervened on independently, following the principle of independence of mechanisms. We thus extend our definition of disentanglement to allow transformations of the internal variables of the network as follows.

**Definition 3 (Intrinsic disentanglement, informal).** In a CGM \( M \), a transformation \( T : \mathcal{Y}_M \rightarrow \mathcal{Y}_M \) is intrinsically disentangled with respect to a subset \( \mathcal{E} \) of endogenous variables, if there is transformation \( T' \) acting on the internal representation space such that for any endogenous value \( v \)

\[ T(\tilde{g}_M(v)) = \tilde{g}_M(T'(v)) \]

where \( T'(v) \) only affects the variables indexed by \( \mathcal{E} \).

Fig. 2c illustrates this second notion of disentanglement, where the split node indicates that the value of \( V_2 \) is computed as in the original CGM (Fig. 2b) before applying transformation \( T^2 \) to the outcome. While the above definition applies to a single transformation, straightforward extensions of this concept to families of transformations are provided in Appendix F. Faithful counterfactuals represent examples of disentangled transformations:

**Proposition 1 (Counterfactuals and disentanglement, informal).** Consider an intervention on subset \( \mathcal{E} \), its associated counterfactual mapping is faithful if and only if it is disentangled. For interventions on variables that remain within the support of the original marginal distribution, it is sufficient that \( \mathcal{E} \) and its complement \( \overline{\mathcal{E}} \) do not have common latent ancestors.
Under review as a conference paper at ICLR 2020

Latent sample $z_1$  

Original 1

E

Latent sample $z_2$

Original 2

Hybrid sample

Figure 3: Generation of influence maps. (a) Principle of sample hybridization through counterfactuals. (b) Left: Clustering of influence maps for a BEGAN trained on the CelebA dataset (see text). Center: example EIM of each cluster. Right: samples of the hybridization procedure using as module all channels of the intermediate layer belonging to the cluster of corresponding row.

This indicates that finding faithful counterfactuals can be used to learn disentangled transformations.

3 FINDING MODULARITY IN DEEP GENERATIVE MODELS

3.1 DEFINING MODULARITY

Building on Sec. 2, we define modularity as a structural property of the internal representation, allowing (with the immediately following Prop. 2) to implement arbitrary disentangled transformations.

Definition 4 (Modularity). A subset of endogenous variables $E$ is called modular whenever $\mathcal{V}_E$ is the Cartesian product of $\mathcal{V}_M^E$ by $\mathcal{V}_N^E$.

Proposition 2 (Modularity implies disentanglement). If $E$ is modular, then and transformation applied to it staying within its input domain is disentangled.

The proof is a natural extension of Proposition 1. Both the definition and the proposition have obvious extensions to multiple modules (based on Appendix F).

3.2 HYBRIDIZATION AS A DISENTANGLED TRANSFORMATION

As stated in Sec. 2, a functional definition of disentanglement, leaves unanswered how to find relevant transformations. Prop. 1 and 2 provide the following hints: (1) Once a modular structure is found in the network, a broad class of disentangled transformations are available, (2) Transformations that stay within their input domain are good candidates of disentanglement, (3) Counterfactual interventions implicitly defines transformation. We follow these guidelines by assigning a constant value $v_0$ to a subset of endogenous variables $E$ to define counterfactuals (i.e. $h$ is a constant function), aiming for faithful ones by constraining $v_0$ to belong to $\mathcal{V}_M^E$. To avoid characterizing $\mathcal{V}_M^E$, we rely on sampling from the (joint) marginal distribution of the variables in $E$.

To illustrate the procedure, we consider a standard feed-forward multilayer neural network and choose endogenous variables to be the collection of all output activations of channels of a given layer $\ell$. Let $E$ be a subset of these channels, the hybridization procedure, illustrated in Fig. 3a goes as follows. We take two independent examples of the latent variable $z_1$ and $z_2$, that will generate two original examples of the output $(y_1, y_2) = (g_M(z_1), g_M(z_2))$ (that we call Original 1 and Original 2). We also memorize the tuple $v(z_2)$ gathering values of variables indexed by $E$ when generating Original 2, and $\bar{v}(z_1)$ the tuple of values taken by all other endogenous variables on this layer, but when generating Original 1. Assuming the choice of $E$ identifies a modular structure, $\bar{v}(z_1)$ and $v(z_2)$ would encode different aspects of their corresponding generated images, such that one can generate a
We first investigated modularity of generative models trained on the CelebFaces Attributes Dataset (CelebA) (Liu et al., 2015). We first used a basic architecture: a plain β-VAE (https://github.com/pixelwise/vae-celebA) (Higgins et al., 2017). We ran the full procedure described in Sec. 3, comprised

hybrid example mixing these features by assigning the collection of output values of layer ℓ with the concatenated tuple (v(z₁), v(z₂)) and feeding it to the downstream part of the generator network.

3.3 Measuring causal effects

The above counterfactual hybridization framework allows assessing how a given module E affects the output of the generator. For this purpose we quantify its causal effect by repetitively generating pairs (z₁, z₂) from the latent space, where both vectors are sampled independently of each other. We then generate and collect hybrid outputs following the above described procedure for a batch of samples and use them to estimate an influence map as the mean absolute effect:

\[ IM(E) = \mathbb{E}_{z_2 \sim P(z)} \mathbb{E}_{z_1 \sim P(z)} |Y^E_{v(z_2)}(z_1) - Y(z_1)| \] (2)

where \( Y(z_1) = g_M(z_1) \) is the non-intervened output of the generator for latent input \( z_1 \). In eq. 2, the difference inside the absolute value can be interpreted as a unit-level causal effect in the potential outcome framework (Imbens & Rubin, 2015), and taking the expectation is analogous to computing the average treatment effect. Our approach has however two specificities: (1) we take the absolute value of the unit-level causal effects, as their sign may not be consistent across units, (2) the result is averaged over many interventions corresponding to different values of \( z_2 \).

While \( IM \) has the same dimension as the output image, we then average it across color channels to get a single grayscale heat-map pixel map. We also define a scalar quantity to quantify the magnitude of the causal effect, the individual influence of module \( E \), by averaging \( IM \) across output pixels.

3.4 Unsupervised detection of modules and counterfactual images

A challenge with the hybridization approach is to select the subsets \( E \) to intervene on, especially with networks containing a large amount of units or channels per layer. We use a fine to coarse approach to extract such groups, that we will describe in the context of convolutional layers. First, we estimate elementary influence maps (EIM) associated to each individual output channel \( c \) of each convolutional layer of the network (i.e. we set \( E = \{c\} \) in equation (2)). Then influence maps are grouped by similarity to define modules at a coarser scale.

Representative EIMs for channels of convolutional layers of a VAE trained on the CelebA face dataset (see result section) are shown in Supplementary Fig. 6 and suggest channels are functionally segregated, with for example some influencing finer face feature (eyes, mouth,...) and others affecting the background of the image or the hair. This supports the idea that individual channels can be grouped into modules that are mostly dedicated to one particular aspect of the output.

In order to achieve this grouping in an unsupervised way, we perform clustering of channels using their EIMs as feature vectors as follows. We first pre-process each influence map by: (1) performing a local averaging with a small rectangular sliding window to smooth the maps spatially, (2) thresholding the resulting maps at the 75% percentile of the distribution of values over the image to get a binary image. After flattening image dimensions, we get a (channel×pixels) matrix \( S \) which is then fed to a Non-negative Matrix Factorization (NMF) algorithm with manually selected rank \( K \), leading to the factorization \( S = WH \). From the two resulting factor matrices, we get the \( K \) cluster template patterns (by reshaping each rows of \( H \) to image dimensions), and the weights representing the contribution of each of these pattern to individual maps (encoded in \( W \)). Each influence map is then ascribed a cluster based on which template pattern contributes to it with maximum weight. The choice of NMF is justified by its success in isolating meaningful parts of images in different components (Lee & Seung, 1999). However, we will also compare our approach to the classical k-means clustering algorithm.

4 Experiments

4.1 DCGAN, β-VAE and BEGAN on the CelebA dataset

We first investigated modularity of generative models trained on the CelebFaces Attributes Dataset (CelebA) (Liu et al., 2015). We first used a basic architecture: a plain β-VAE (https://github.com/pixelwise/vae-celebA) (Higgins et al., 2017). We ran the full procedure described in Sec. 3 comprised
of EIM calculations, clustering of channels into modules, and hybridization of generator samples using these modules. Hybridization procedures were performed by intervening on the output of the intermediate convolutional layer (indicated in Supplemental Fig. 7). The results are summarized in Supplemental Fig. 8. We observed empirically that setting the number of clusters to 3 leads consistently to highly interpretable cluster templates as illustrated in the figure, with one cluster associated to the background, one to the face and one to the hair. This observation was confirmed by running the following cluster stability analysis: we partition at random the influence maps in 3 subsets, and we use this partition to run the clustering twice on two thirds of the data, both runs overlapping only on one third. The obtained clusters were then matched in order to maximize the label consistency (the proportion of influence maps assigned the same label by both runs) on the overlapping subset, and this maximum consistency was used to assess robustness of the clustering across the number of clusters. The consistency results are provided in Supplemental Fig. 9 and show 3 clusters is a reasonable choice as consistency is large (> 90%) and drops considerably for 4 clusters. Moreover, these results also show that the NMF-based clustering outperforms clustering with the more standard k-means algorithm. In addition, we also assessed the robustness of the clustering by looking at the cosine distance between the templates associated to matching clusters, averaged across clusters. The results, also provided in Supplemental Fig. 9 are consistent with the above analysis with an average cosine similarity of .9 (scalar product between the normalized feature vectors) achieved with 3 clusters (maximum similarity is 1 for perfectly identical templates). Exemplary influence maps shown in Supplemental Fig. 8 (center panel) reflect also our general observation: some maps may spread over image locations reflecting different clusters.

Interestingly, applying the hybridization procedure to the resulting 3 modules obtained by clustering leads to a replacement of the features associated to the module we intervene on, as shown in Supplemental Fig. 8 (center panel), while respecting the overall structure of the image (no discontinuity introduced). For example, on the middle row we see the facial features of the Original 2 samples are inserted in the Original 1 image (shown on the left), while preserving the hair.

While the $\beta$-VAE is in principle optimal for extrinsic disentanglement, these above results could also be reproduced in the official tensorlayer DCGAN implementation, equipped with a similar architecture (https://github.com/tensorlayer/dcgan) (see Appendix E). This suggests that our approach can be applied to models that have not been optimized for disentanglement. After these experiments with basic models, we used a pretrained (https://github.com/Heumi/BEGAN-tensorflow) Boundary Equilibrium GAN (BEGAN) (Berthelot et al., 2017), which used to set a milestone in visual quality for higher resolution face images. The good quality and higher resolution of the generated images combined with the relatively simple generator architecture of BEGAN allows us to test our hypothesis with minimal modifications of the computational graph. Most likely due to the increase in the number of layers, we observed that obtaining counterfactuals with noticeable effects required interventions on channels from the same cluster in two successive layers. The results shown in Fig. 10 obtained by intervening on layers 5 and 6, reveal a clear selective transfer of features from Original 2 to Original 1. As the model was trained on face images cropped with a tighter frame than for the above models, leaving little room for the hair and background, we observe only one module associated to these features (Fig. 3 middle row) showing a clear hair transfer. The remaining two modules are now encoding different aspects of face features: eye contour/mouth/nose for the top row and eyelids/face shape for the bottom row module. We further evaluated the relative quality of the counterfactual images with respect to the original generated images using the Frechet Inception Distance (FID) (Heusel et al., 2017) (Table 2 in the appendix), supporting that the hybridization procedure only mildly affects the image quality, in comparison to the original samples.

4.2 BigGAN on the ImageNet dataset

In order to check whether our approach could scale to high resolution generative models, and generalize to complex image datasets containing a variety of objects, we used the BigGAN-deep architecture (Brock et al., 2018), pretrained (https://tfhub.dev/deepmind/biggan-deep-256/) on the ImageNet dataset (http://www.image-net.org/). This is a conditional GAN architecture comprising 12 so-called Gblocks, each containing a cascade of 4 convolutional layers (see Appendix C for details). Each Gblock also receives direct input from the latent variables and the class label, and is bypassed by a skip connection. We then checked that we were able to generate hybrids by mixing the features of different classes. As for the case of BEGAN, intervening on two successive layers within a Gblock was more effective to generate counterfactuals (examples are provided for the 7th Gblock). Examples provided in Fig. 4...
Figure 4: Examples of BigGAN hybridizations across classes. Left: ostrich-cock, right: koala-teddy.

Figure 5: Analysis of classifier robustness to counterfactual changes (bars indicate standard error).

(cock against ostrich) show that it is possible to generate high quality counterfactuals with modified background while keeping a very similar object in the foreground. In a more challenging situation, with objects of different nature (Koala-teddy bear on the same figure), meaningful combinations of each original samples are still generated: e.g. a teddy bear in a tree (bottom row), or a “teddy-koala” merging teddy texture with the color of a koala on a uniform indoor background with a slight wooden texture (top row).

In order to investigate how the generated counterfactual images can be used to probe and improve the robustness of classifiers to contextual changes, we compared the ability of several SOTA pretrained classifier available on Tensorflow-hub ([https://tfhub.dev/](https://tfhub.dev/), see Appendix C for details) to recognize one of the original classes. Fig. 5 shows the average recognition rate of the most recognized original class (teddy-bear or koala), as a function of layer depth tends overall to increase. We first observe that high recognition rates are in line with the small pixel distance between hybrids and original when intervening at layers closest to the output (right panel). Interestingly, at intermediate blocks 5-6, there is a clear contrast between classifiers, with the Inception resnet performing better than the others. Interestingly, examples of non-consensual classification results in Supplementary Table 3 together with the associated hybrids (Supplementary Fig. 12) suggest different SOTA classifiers rely on different aspects of the image content to take their decision (e.g. background versus object).

**CONCLUSION**

We introduced a mathematical definition of disentanglement, related it to the causal notion of counterfactual and used it for the unsupervised characterization of the representation encoded by different groups of channels in deep generative architectures. We found evidence for interpretable modules of internal variables in four different generative models trained on two complex real world datasets. Our framework opens a way to a better understanding of complex generative architectures and applications such as the style transfer [Gatys et al., 2015] of controllable properties of generated images at low computational cost (no further optimization is required), and the automated assessment of robustness of object recognition systems to contextual changes. From a broader perspective, this research direction contributes to a better exploitation of deep neural networks obtained by costly and highly energy-consuming training procedures, by (1) enhancing their interpretability and (2) allowing them to be used for tasks where not trained for. This offers a perspective on how more sustainable research in Artificial Intelligence could be fostered in the future.
REFERENCES


Supplementary information

APPENDIX A: FORMAL DEFINITIONS AND RESULTS FOR CAUSAL GENERATIVE MODELS (SECTION 2)

We rely on the assumption that a trained generator architecture can be exploited as a mechanistic model, such that parts of this model can be manipulated independently. A mathematical representation of such models can be given using structural causal models (SCMs), that rely on structural equations (SEs) of the form \( Y := f(X_1, X_2, \ldots, X_N, \epsilon) \), denoting the assignment of a value to variable \( Y \), computed from the values of other variables \( X_k \) in the system under consideration, and of putative exogenous influences \( \epsilon \), imposed by factors outside the system under study. As in the above equation, we will use uppercase letters to indicate variables being the outcome of a structural assignment, while specific values taken by them will be lower case. SEs stay valid even if right-hand side variables undergo a change due to interventions \cite{Pearl2009, Peters2017}, and can model the operations performed in computational graphs of modern neural network implementations. Such graphs then depict SCMs made of interdependent modules, for which assignments’ dependencies are represented by a directed acyclic graph \( \mathcal{G} \). Without loss of generality, we introduce a Causal Generative Model (CGM) \( M \) capturing the computational relations between a selected subset of variables comprising: (1) the input latent variables \( \{z_k\} \), (2) the generator’s output \( Y \) (typically multi-dimensional), and (3) a collection of possibly multi-dimensional endogenous (internal) variables forming an intermediate representation such that the generator’s output can be decomposed into two successive steps as \( \{Z_k\} \rightarrow \{V_k\} \rightarrow Y \). In a feed-forward neural network, one \( V_k \) may for instance represent one channel of the output of a convolutional layer (e.g. after application of the ReLU non-linearity).

**Definition 5** (Causal Generative Model (CGM)). Given \( K \) real-valued latent variables \( z = (z_k) \) taking arbitrary values on domain \( Z = \prod_{k=1}^{K} Z_k \), where all \( Z_k \)'s are closed intervals, the CGM \( M = \mathcal{G}(Z, S, G) \) comprises a directed acyclic graph \( \mathcal{G} \) and a set \( S \) of \( N + 1 \) deterministic continuous structural equations that assign:

- \( N \) endogenous variables \( \{V_k := f_k(Pa_k)\}_{k=1..N} \) taking values in Euclidean spaces \( (\mathcal{V}_k)_{k=1..N} \), based on their endogenous or latent parents \( Pa_k \) in \( \mathcal{G} \).
- one output \( Y := f_y(Pa_y) \) taking values in Euclidean space \( \mathcal{Y} \), parents \( Pa_y \) in \( \mathcal{G} \) being endogenous.

Moreover, \( z_k \)'s are the only sources and \( Y \) is the only sink.

The graph of an example CGM is exemplified on Fig. \ref{fig:example_cgm} consisting of 3 endogenous variables, 2 latent inputs and the output. This aligns with the definition of a deterministic structural causal model by \cite{Pearl2009} chapter 7), once our latent variables are identified with exogenous ones. CGMs have however specificities reflecting the structure of models encountered in practice. For instance, variable assignments may or may not involve latent/exogenous variables in their right-hand side, which is unusual in causal inference. This allows modeling feed-forward networks consisting in a first layer receiving latent inputs followed by a cascade of deterministic operations in downstream layers. The above definition guaranties several basic properties found in the computational graph of existing generative networks: (1) all endogenous variables \( V_k \) are unambiguously assigned once \( z \) is chosen, (2) the output \( Y \) is unambiguously assigned once either \( z \) is chosen, or, alternatively, if an appropriate subset of \( V_k \)'s, such as \( Pa_y \), is assigned. This allows us to introduce several useful mappings.

In an ideal case, while the support of the latent distribution covers the whole latent space \( Z \), internal variables and outputs typically live on manifolds of smaller dimension than their ambient space. These can be defined as the images\(^4\) of \( Z \) by operations of the graph: the output image \( \mathcal{Y}_M = Y[Z] \), the endogenous images \( \mathcal{V}_{kM} = V_k[Z] \) for a single variable, \( \mathcal{V}_{\mathcal{E}M} = \{v \in \prod_{k \in \mathcal{E}} V_k : v = (v_k(z))_{k \in \mathcal{E}}, z \in Z\} \) for a subset of variables indexed by \( \mathcal{E} \), and \( \mathcal{V}_M \) when \( \mathcal{E} \) includes all endogenous variables.

\(^1\) A is a parent of (child) B whenever there is an arrow \( A \rightarrow B \).
\(^2\) Sources are parentless nodes, sinks are childless.
\(^3\) An image \( f[A] \) is the subset of outputs of \( f \) for a subset \( A \) of input values.

\(^4\) A image \( f[A] \) is the subset of outputs of \( f \) for a subset \( A \) of input values.
Functions assigning $Y$ from latent variables and from endogenous variables, respectively, are

$$g_M : \mathcal{Z} \rightarrow \mathcal{Y}_M , \quad g_M (z) \quad \text{and} \quad \tilde{g}_M : \mathcal{V}_M \rightarrow \mathcal{Y}_M , \quad \tilde{g}_M (v)$$

and we call them latent and endogenous mappings, respectively. Given the typical choice of dimensions for latent and endogenous variables, the $V_k$’s and $Y$ are constrained to take values in subsets of their euclidean ambient space. We will assume that $\tilde{g}_M$ and $g_M$ define proper embeddings, in particular implying that they are both invertible. We call a CGM satisfying these assumptions an embedded CGM.

With this vocabulary we can for example verify the example of Fig. 2b contains exactly two layers (in green). Note $g_M$ and $\tilde{g}_M$ are well defined because the output can be unambiguously computed from their inputs by successive assignments along $G$, and are both surjective due to appropriate choices for domains and codomains. All defined image sets ($\mathcal{V}_M, \mathcal{Y}_M, ...$) are constrained by the parameters of $M$, and are typically not easy to characterize. For example $\mathcal{V}_M$ is likely a strict subset of the Cartesian product $\prod_k \mathcal{V}_M$.

Importantly, the image set $\mathcal{Y}_M$ of a trained model is of particular significance, as it should approximate at best the support of the data distribution we want to model. Learning the generator parameters such that $\mathcal{Y}_M$ precisely matches the support of the target data distribution is arguably a major goal for generative models (see e.g. Sajjadi et al. (2018)).

As we will manipulate properties of the output, we restrict ourselves to transformations that respect the topology of $\mathcal{Y}_M$, and use embeddings as the basic structure for it, allowing inversion of $g_M$.

**Proposition 3.** If $\mathcal{Z}$ of CGM $M$ is compact (all $\mathcal{Z}_k$’s are bounded), then $M$ is embedded if and only if $g_M$ is injective.

Proof is provided in Appendix B. This implies that generative models based on uniformly distributed latent variables (the case of many GANs), provided they are injective, are embedded CGMs. While VAEs’ latent space is typically not compact (due to the use of normally distributed latent variables), we argue that restricting it to a product of compact intervals (covering most of the probability mass) will result in an embedded CGM that approximates the original one for most samples.

Based on this precise framework, we can now provide the formal definitions and results described informally in main text.

The CGM framework allows defining counterfactuals in the network following Pearl (2014).

**Definition 6 (Embedded CGMs).** If $f : \mathcal{X} \rightarrow \mathcal{Y}$ is a continuous injective function with continuous inverse $f^{-1} : f[\mathcal{X}] \rightarrow \mathcal{Y}$, we call $f$ an embedding of $\mathcal{X}$ in $\mathcal{Y}$. We say that a CGM $M$ is embedded if $g_M$ and $\tilde{g}_M$ are respective embeddings of $\mathcal{Z}$ and $\mathcal{V}_M$ in $\mathcal{Y}$.

Since Definition 6 imposes continuous structural equations, which is satisfied for all operations in standard generative models, injectivity of $g_M$ is the key additional requirement for embedded CGMs.

**Proposition 3.** If $\mathcal{Z}$ of CGM $M$ is compact (all $\mathcal{Z}_k$’s are bounded), then $M$ is embedded if and only if $g_M$ is injective.

Proof is provided in Appendix B. This implies that generative models based on uniformly distributed latent variables (the case of many GANs), provided they are injective, are embedded CGMs. While VAEs’ latent space is typically not compact (due to the use of normally distributed latent variables), we argue that restricting it to a product of compact intervals (covering most of the probability mass) will result in an embedded CGM that approximates the original one for most samples.

Based on this precise framework, we can now provide the formal definitions and results described informally in main text.

The CGM framework allows defining counterfactuals in the network following Pearl (2014).

**Definition 7 (Unit level counterfactual).** Given CGM $M$, for a subset of endogenous variables $\mathcal{E} = \{e_1, ..., e_n\}$, and a tuple of values $v_0 \in \prod_k \mathcal{Y}_k$ jointly taken by these variables, we define the interventional CGM $M_\mathcal{E}$ obtained by replacing structural assignments for $\mathcal{V}_\mathcal{E}$ by assignments $\{V_{e_k} := h_k(z) \}_{e_k \in \mathcal{E}}$. Then for a given value $z$ of the latent variables, called unit, the unit-level counterfactual is the output of $M_\mathcal{E}$: $Y_k^\mathcal{E}(z) = g_{M_\mathcal{E}}(z)$.

Definition 7 is also in line with the concept of potential outcome (Imbens & Rubin 2015). Importantly, counterfactuals induce a transformation of the output of the generative model.

**Definition 2 (Counterfactual mapping).** Given an embedded CGM, we call the continuous map

$$\hat{Y}_h^\mathcal{E} : y \mapsto Y_h^\mathcal{E} (g_M^{-1}(y))$$

the ($\mathcal{E}, h$)-counterfactual mapping. We say it is faithful to $M$ whenever $\hat{Y}_h^\mathcal{E} \mathcal{Y}_M \subset \mathcal{Y}_M$.

Our approach then relates counterfactuals to a form of disentanglement allowing transformations of the internal variables of the network as follows.
**Definition** (Intrinsic disentanglement). In a CGM $M$, endomorphism $T : Y_M \rightarrow Y_M$ is intrinsically disentangled with respect to a subset $E$ of endogenous variables, if it exists a transformation $T'$ of endogenous variables such that for any latent $z \in Z$, leading to the tuple of values $v \in V_M$,

$$T(Y(v)) = Y(T'(v))$$

where $T'(v)$ only affects the variables indexed by $E$.

In this definition, $Y(v)$ corresponds to the unambiguous assignment of $Y$ based on endogenous values. Fig. 2d illustrates this second notion of disentanglement, where the split node indicates that the value of $V_2$ is computed as in the original CGM (Fig. 2b) before applying transformation $T_2$ to the outcome.

Intrinsic disentanglement relates to a causal interpretation of the generative model’s structure in the sense that it expresses a form of robustness to perturbation of one of its subsystems. Counterfactuals represent examples of such perturbations, and as such, may be disentangled given their faithfulness.

**Proposition** (Counterfactuals and disentanglement, formal). For an embedded CGM $M$ and continuous assignment $h$, the $(E, h)$-counterfactual mapping $\tilde{Y}_{E}^h$ is faithful if and only if it is intrinsically disentangled with respect to subset $E$. Moreover, if $h[Z] \subset V_M$, it is sufficient that $E$ and $E$ do not have common latent ancestors for $\tilde{Y}_{E}^h$ to be faithful.

The proof is provided in Appendix B.

**APPENDIX B: ADDITIONAL DETAILS FOR SECTION 2**

**Topological concepts**

**Continuity.** We recall the classical definition of continuity of $f : X \rightarrow Y$. Given the respective topologies $\tau_X$ and $\tau_Y$ of domain and codomain (the sets of all open sets), $f$ is continuous whenever for all $A \in \tau_Y$, $f^{-1}(A) \in \tau_X$.

**Euclidean topology.** For defining continuity between Euclidean spaces, we rely on the Euclidean (or standard) topology naturally induced by the metric: as set is open if and only if it contains an open ball around each if its points.

**Subset topology.** When restricting the domain or codomain of a mapping to a subset $A$ of the Euclidean space, we rely on the subspace topology, that consists in the intersection of $A$ with all open sets.

**Proof of Proposition 3**

Following a result stated in Armstrong (2013), since $Z$ is compact and the codomain of $g_M$ is Hausdorff (because Euclidean), then a continuous (by definition) and injective $g_M$ is an embedding. In addition, $g_M$ injective implies $\tilde{g}_M$'s are injective on their respective domains $\mathbf{V}_M$. Moreover, the $\mathbf{V}_M$'s being image of a compact $Z$ by a continuous mapping (by the CGM definition), they are compact, such that the respective $\tilde{g}_M$'s are also embeddings.

**Proof of Proposition 1**

Part 1: Proof of the equivalence between faithful and disentangled. One conditional is trivial: if a transformation is disentangled, it is by definition an endomorphism of $Y_M$ so the counterfactual mapping must be faithful.

For the second conditional, let us assume a faithful $\tilde{Y}_{v_0}^E$ and denote the (unambiguous) map from $V$ to the output

$$Y_M : V \rightarrow Y_M : v \mapsto Y(v).$$

\[\text{Note the mapping } v \mapsto Y(v) \text{ differs from } \tilde{g}_M \text{ because its domain is not restricted to the image set } V_M.\]
We used the method proposed in Berthelot et al. (2017) for CelebA dataset. We used the pre-trained model with the same architecture as was used in the paper. It consists of three blocks of convolutional layers each followed by an upsampling layer. The filter size of convolutional layers is \((3, 3)\) all over the generator. There is also skip connections in the model that is argued to increase the sharpness of images. Consult (Berthelot et al., 2017, Figure 1) for architectural details.

\[ \nabla \mathcal{E} = \nabla \mathcal{E} \circ T' \circ (\tilde{g}_M)^{-1}, \quad \text{where} \quad T': \mathcal{V}^E \times \mathcal{V}^E \rightarrow \mathcal{V}^E \times \mathcal{V}^E. \]

Since \( \nabla \mathcal{E} \) is faithful, it is then an endomorphism of \( \mathcal{V}_M \) (continuity comes from the composition of continuous functions), as required by the definition of disentanglement.

For any \( v \in \mathcal{V} \), consider then the quantity

\[ \nabla \mathcal{E} \circ (\nabla \mathcal{E})(v) = \nabla \mathcal{E} \circ \tilde{g}_M(v), \]

using the above decomposition, we can rewrite it as

\[ \nabla \mathcal{E} \circ (\nabla \mathcal{E})(v) = \nabla \mathcal{E} \circ \tilde{g}_M(v) = \mathcal{V}^E \circ \mathcal{V}^E, \]

where \( T' \) is a transformation that only affects endogenous variables in \( E \), demonstrating that \( \nabla \mathcal{E} \circ (\nabla \mathcal{E})(v) \) is disentangled with respect to \( E \).

**Part 2: Sufficient condition.** This is a direct application of the following Proposition 4 after observing that in our case, the endomorphism \( \nabla \mathcal{E} \) required in this proposition is the constant function with value \( v_0 \).

**Proposition 4.** For embedded CGM \( M \), if a subset \( \mathcal{E} \) of endogenous variables does not share common latent ancestors with the remainder of endogenous variables \( E \), then any endomorphism \( T': \mathcal{V}_M^E \rightarrow \mathcal{V}_M^E \) leads to a transformation

\[ T: y \mapsto g_M \circ T' \circ (g_M)^{-1}(y), \]

with \( T': \mathcal{V}_M^E \times \mathcal{V}_M^E \rightarrow \mathcal{V}_M^E \times \mathcal{V}_M^E, \)

such that \( T \) is disentangled with respect to \( \mathcal{E} \) in \( M \).

**Proof of Proposition 4** The absence of common latent ancestor between \( \mathcal{E} \) and \( E \) ensures that values in both subsets are unambiguously assigned by non-overlapping subsets of latent variables, \( A \) and \( B \) respectively, such that we can write

\[ \left( \mathcal{V}_{|\mathcal{E}}, \mathcal{V}_{|E} \right) = (f_A(z_A), f_B(z_B)). \]

This implies that the image set of this layer fully covers the Cartesian product of the image sets of the two subsets of variables, i.e., \( \mathcal{V}_M = \mathcal{V}_M^E \times \mathcal{V}_M^E \), and guarantees that \( T' \) is an endomorphism of \( \mathcal{V}_M^E \) for any choice of endomorphism \( T \). This further implies \( T \) is well defined and an endomorphism.

**Appendix C: Architecture Details**

**Vanilla \( \beta \)-VAE and DCGAN**

The \( \beta \)-VAE architecture is presented in Supplementary Fig. 7 and is very similar to the DCGAN architecture. Hyperparameters for both structures are specified in Table 1.

**BEGAN CelebA**

We used the method proposed in Berthelot et al. (2017) and the embedding property) that the counterfactual mapping can be decomposed as

\[ \mathcal{V}^E \circ \mathcal{V}^E = \mathcal{V}^E \circ \mathcal{V}^E \rightarrow \mathcal{V}^E \times \mathcal{V}^E. \]

This map differs from \( \tilde{g}_M \) due to its broader domain and codomain, such that it is neither necessarily an injection nor a surjection, but they coincide on the image \( \mathcal{V}_M \). We can first notice (using Definition 7 and the embedding property) that the counterfactual mapping can be decomposed as

\[ \mathcal{V}^E \circ \mathcal{V}^E = \mathcal{V}^E \circ \mathcal{V}^E \rightarrow \mathcal{V}^E \times \mathcal{V}^E. \]

The absence of common latent ancestor between \( \mathcal{E} \) and \( E \) ensures that values in both subsets are unambiguously assigned by non-overlapping subsets of latent variables, \( A \) and \( B \) respectively, such that we can write

\[ \left( \mathcal{V}_{|\mathcal{E}}, \mathcal{V}_{|E} \right) = (f_A(z_A), f_B(z_B)). \]

This implies that the image set of this layer fully covers the Cartesian product of the image sets of the two subsets of variables, i.e., \( \mathcal{V}_M = \mathcal{V}_M^E \times \mathcal{V}_M^E \), and guarantees that \( T' \) is and endomorphism of \( \mathcal{V}_M^E \) for any choice of endomorphism \( T \). This further implies \( T \) is well defined and an endomorphism.

\[ \text{\textsuperscript{*}} \quad A \text{ is an ancestor of } B \text{ whenever there is a directed path } A \rightarrow \ldots \rightarrow B \text{ in the graph.} \]}
BIGGAN-DEEP-256 ARCHITECTURE DETAILS

The pretrained model is taken from Tensorflow-hub (https://tfhub.dev/) we summarize below the main aspects of the architectures. We used the BigGan-deep architecture of Brock et al. (2018) as a pre-trained model on 256x256 ImageNet. We did not retrain the model. The architecture consists of several ResBlocks which are the building block of the generator. Each ResBlock contains BatchNorm-ReLU-Conv Layers followed by upsampling transformations and augmented with skip connections that bring fresh signal from the input to every ResBlock. Consult Brock et al. (2018) for architectural details.

CLASSIFIERS ARCHITECTURE DETAILS

All pretrained models are taken from Tensorflow-hub (https://tfhub.dev/), we summarize below the main aspects of the architectures.

INCEPTION_RESNET_V2

Inception ResNet V2 is a neural network architecture for image classification, originally published by


INCEPTION_V3

Inception V3 is a neural network architecture for image classification, originally published by


NASNET_LARGE

NASNet-A is a family of convolutional neural networks for image classification. The architecture of its convolutional cells (or layers) has been found by Neural Architecture Search (NAS). NAS and NASNet were originally published by


NASNets come in various sizes. This TF-Hub module uses the TF-Slim implementation nasnet_large of NASNet-A for ImageNet that uses 18 Normal Cells, starting with 168 convolutional filters (after the "ImageNet stem"). It has an input size of 331x331 pixels.

RESNET_V2_50

ResNet V2 is a family of network architectures for image classification with a variable number of layers. It builds on the ResNet architecture originally published by


The full preactivation 'V2' variant of ResNet used in this module was introduced by

Kaiming He, Xiangyu Zhang, Shaoqing Ren, Jian Sun: "Identity Mappings in Deep Residual Networks", 2016.

APPENDIX D: ADDITIONAL FILES.

The file influence.py provided at the link https://www.dropbox.com/sh/4qnjictmh4a2soq/AAAa5brzPD1t69Q0c9n2K4u0a?dl=0 contains key elements of the code for counterfactual analysis of generative models.
APPENDIX E: ADDITIONAL RESULTS

INFLUENCE MAP CLUSTERING AND HYBRIDIZATION IN DCGANs

We replicated the above approach for GANs on the CelebA dataset. The result shown in Supplemental Fig. [11] summarize the main differences. First, the use of three clusters seemed again optimal according to the stability of the obtained cluster templates. However, we observed that the eyes and mouth location were associated with the top of the head in one cluster, while the rest of the face and the sides of the image (including hair and background) respectively form the two remaining clusters. In this sense, the GAN clusters are less aligned with high level concepts reflecting the causal structure of these images. However, such clustering still allows a good visual quality of hybrid samples.

APPENDIX F: ADDITIONAL DISCUSSION

EXTENSION AND RELATION TO OTHER FRAMEWORKS

While we defined disentanglement of transformations, this concept has been classically attributed to a representation, or factors of variation. Focusing on a transformation aligns to our aim of providing an agnostic definition, in the sense that it only relies on the generator architecture and a given transformation, but neither on data, nor on properties that are not stated explicitly in the definition. In contrast, disentangled representation is usually understood as intervening on meaningful/interpretable features in the image, which may be subjective, or at least referring to some external knowledge. Alternatively, one might expect that what should be disentangled is a property or a factor of variation (say “hair color”). We argue that we can state a property is disentangled by the generalizing our notion of disentanglement to a family of transformations as follows.

Definition 8 (Disentangled family). A family of transformations (possibly parametric) is disentangled if all members are disentangled with respect to the same $\mathcal{E}$.

Then a property may be disentangled if the class of all transformations changing “only” the value of this specific property is disentangled according to Definition 8. Finally, one might also expect that several transformations (or families of transformations) should be disentangled with respect to each other, e.g. allowing to state that hair color should be disentangled from hair length. This relative disentanglement is easily defined based on our original definition.

Definition 9 (Relative disentanglement). The families of functions $(\mathcal{F}_i)_{i \in 1..N}$ are called jointly disentangled whenever they are disentangled with respect to non-overlapping subsets of variables $(\mathcal{E}_i)_{i \in 1..N}$ within a given layer.7

We argue that the notion introduced in Higgins et al. (2018) can be framed as a special case of Definition 9.

SUPPLEMENTARY FIGURES AND TABLES

<table>
<thead>
<tr>
<th>Architecture</th>
<th>VAE CelebA</th>
<th>GAN CelebA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nb. of deconv. layers/channels of generator</td>
<td>4/(64,64,32,16,3)</td>
<td>4/(128,64,32,16,3)</td>
</tr>
<tr>
<td>Size of activation maps of generator</td>
<td>(8,16,32,64)</td>
<td>(4,8,16,32)</td>
</tr>
<tr>
<td>Latent space</td>
<td>128</td>
<td>150</td>
</tr>
<tr>
<td>Optimization algorithm</td>
<td>Adam ($\beta = 0.5$)</td>
<td>Adam ($\beta = 0.5$)</td>
</tr>
<tr>
<td>Minimized objective</td>
<td>VAE loss (Gaussian posteriors)</td>
<td>GAN loss</td>
</tr>
<tr>
<td>batch size</td>
<td>64</td>
<td>64</td>
</tr>
<tr>
<td>Beta parameter</td>
<td>0.0005</td>
<td>NA</td>
</tr>
</tbody>
</table>

Table 1

7 or within the latent space for extrinsic disentanglement
Figure 6: **Generation of influence maps.** Example of influence maps generated by a VAE on the CelebA dataset (lighter pixel indicate larger variance and thus stronger influence of the perturbations on that pixel).

Table 2: FID analysis of BEGAN hybrids. Distance between different pairs of classes (R: Real data, G: Generated data, Ck: Hybrids by intervention on cluster k). The distances are is computed for balanced number of examples ($10^k$) for each class and normalized by the FID between the real data and the generated data. It can be seen in the table that Hybrids have a small distance to the generated and also to each other. This can be interpreted as closeness of the distribution of Hybrids to that of generated data suggesting that Hybridization produces visually plausible images.

<table>
<thead>
<tr>
<th></th>
<th>G</th>
<th>C0</th>
<th>C1</th>
<th>C2</th>
</tr>
</thead>
<tbody>
<tr>
<td>R</td>
<td>1.022</td>
<td>0.036</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>G</td>
<td>1.143</td>
<td>0.093</td>
<td>0.096</td>
<td>0</td>
</tr>
<tr>
<td>C0</td>
<td>1.158</td>
<td>0.097</td>
<td>0.099</td>
<td>0.045</td>
</tr>
</tbody>
</table>

Figure 7: **VAE architecture.** FC indicates a fully connected layer, $z$ is a 100-dimensional isotropic Gaussian vector, horizontal dimensions indicate the number of channels of each layer. The output image size is $64 \times 64$ (or $32 \times 32$ for cifar10) pixels and these dimensions drop by a factor 2 from layer to layer. (reproduced from [Radford et al., 2015].)
Figure 8: Left: Clustering of influence maps for a VAE trained on the CelebA dataset (see text). Center: samples of the hybridization procedure using as module all channels of the intermediate layer belonging to the cluster of corresponding row. Right: magnitude of causal effects. (top: average influence of modules derived from clustering as a function of the number of clusters; bottom: individual influence of each module as a function of the number of channels they contain, dashed line indicate linear regression).

Figure 9: Label consistency (left) and cosine similarity (right) of the clustering of influence maps for the NMF and k-means algorithm. Errorbars indicate standard deviation across 20 repetitions.
Figure 10: Clustering of influence maps and generation of hybrid samples for a VAE trained on the CelebA dataset (see text).

Figure 11: Clustering of influence maps and generation of hybrid samples for a GAN trained on the CelebA dataset (see text).
Table 3: The classification outcome of several discriminative models for three randomly chosen koala+teddy hybrids (see Figure. [12]). The purpose of this experiment is to investigate the use of the proposed intervention procedure for assessing robustness of classifiers. As can be seen in the following images, the resultant hybrids are roughly a teddy bear in a koala context. An ideal classifier must be sensitive to the object present in the scene not the contextual information. A teddy bear must still be classified as a teddy bear even if it appears on a tree which is the koala environment in most of the koala images in the ImageNet dataset. It can be seen in the following table that nasnet_large is more robust to the change of context compared to other classifiers.

<table>
<thead>
<tr>
<th>Left Image</th>
<th>Model</th>
<th>resnet_v2_50</th>
<th>inception_v3</th>
<th>nasnet_large</th>
<th>inception_resnet_v2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output koala</td>
<td>koala</td>
<td>koala</td>
<td>koala</td>
<td>koala</td>
<td>koala</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Middle Image</th>
<th>Model</th>
<th>resnet_v2_50</th>
<th>inception_v3</th>
<th>nasnet_large</th>
<th>inception_resnet_v2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output koala</td>
<td>koala</td>
<td>koala</td>
<td>koala</td>
<td>teddy</td>
<td>teddy</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Right Image</th>
<th>Model</th>
<th>resnet_v2_50</th>
<th>inception_v3</th>
<th>nasnet_large</th>
<th>inception_resnet_v2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output koala</td>
<td>koala</td>
<td>teddy</td>
<td>teddy</td>
<td>teddy</td>
<td>koala</td>
</tr>
</tbody>
</table>

Figure 12: Three koala+teddy hybrids as the inputs to the classifiers of Table [3].