The State of the Art in Enhancing Trust in Machine Learning Models with the Use of Visualizations
A. Chatzimparmpas, R. Martins, I. Jusufi, K. Kucher, Fabrice Rossi, A. Kerren

To cite this version:

HAL Id: hal-03909758
https://hal.science/hal-03909758
Submitted on 21 Dec 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License
The State of the Art in Enhancing Trust in Machine Learning Models with the Use of Visualizations

A. Chatzimparmpas\textsuperscript{1}, R. M. Martins\textsuperscript{1}, I. Jusufi\textsuperscript{1}, K. Kucher\textsuperscript{1}, F. Rossi\textsuperscript{2}, and A. Kerren\textsuperscript{1}

\textsuperscript{1}Department of Computer Science and Media Technology, Linnaeus University, Sweden
\textsuperscript{2}Ceremade, Université Paris Dauphine, PSL University, France

Abstract

Machine learning (ML) models are nowadays used in complex applications in various domains, such as medicine, bioinformatics, and other sciences. Due to their black box nature, however, it may sometimes be hard to understand and trust the results they provide. This has increased the demand for reliable visualization tools related to enhancing trust in ML models, which has become a prominent topic of research in the visualization community over the past decades. To provide an overview and present the frontiers of current research on the topic, we present a State-of-the-Art Report (STAR) on enhancing trust in ML models with the use of interactive visualization. We define and describe the background of the topic, introduce a categorization for visualization techniques that aim to accomplish this goal, and discuss insights and opportunities for future research directions. Among our contributions is a categorization of trust against different facets of interactive ML, expanded and improved from previous research. Our results are investigated from different analytical perspectives: (a) providing a statistical overview, (b) summarizing key findings, (c) performing topic analyses, and (d) exploring the data sets used in the individual papers, all with the support of an interactive web-based survey browser. We intend this survey to be beneficial for visualization researchers whose interests involve making ML models more trustworthy, as well as researchers and practitioners from other disciplines in their search for effective visualization techniques suitable for solving their tasks with confidence and conveying meaning to their data.

Keywords: trustworthy machine learning, visualization, interpretable machine learning, explainable machine learning

ACM CCS:
• Information systems → Trust;
• Human-centered computing → Visual analytics;
• Human-centered computing → Information visualization;
• Human-centered computing → Visualization systems and tools;
• Machine learning → Supervised learning;
• Machine learning → Unsupervised learning;
• Machine learning → Semi-supervised learning;
• Machine learning → Reinforcement learning

1. Introduction

Trust in machine learning (ML) models is one of the greatest challenges in real-life applications of ML [TAC\textsuperscript{*}20]. ML models are now commonplace in many research and application domains, and they are frequently used in scenarios of complex and critical decision-making [NGDM\textsuperscript{*}19, PWJ06, TKK18]. Medicine, for example, is one of the fields where the use of ML might offer potential improvements and solutions to many difficult problems [KKS\textsuperscript{*}19, SGSG19, SKK\textsuperscript{*}19]. A significant challenge that remains, however, is how trustworthy are the ML models that are being used in these disciplines. Rudin and Ustun [RU18], for example, emphasize the importance of trust for ML models in healthcare and criminal justice, since they play a significant role in making decisions regarding human lives. It is not uncommon to observe that domain experts may not rely on ML models if they do not understand how they work [JSO19].

The impact of this problem can already be observed in recent works, such as the program “Explainable AI (XAI)” founded by DARPA (Defense Advanced Research Projects Agency) [Dar20] and described by Krause et al. [KDS\textsuperscript{*}17]. This initiative is only one of the various projects that suggest further research into the field of XAI, which—to a certain extent—addresses challenges related to trust. The XAI program in its two main motivational points mentions specifically that “producing more explainable models, while maintaining a high level of learning performance” and “enabling human users to understand, appropriately trust, and effectively manage the emerging generation of AI” are both key actions for the future development in numerous domains that use ML. Understanding and trusting ML models is also arguably mandatory under the General Data Protection Regulation (GDPR) [EC16] as part of the “right to be informed” principle: data controllers must provide meaningful information about the logic involved in automated decisions [Art18]. Individuals have also the right not to be subject
to a decision based solely on automated processing; enabling subjects of ML algorithms to trust their decision is probably the easiest way to reduce the objection to such automated decisions.

In reaction to these aforementioned challenges, multiple new solutions have recently been proposed both in academia and in industry. Google’s Explainable Artificial Intelligence (AI) Cloud [Goo20], for example, assists in the development of interpretable and explainable ML models and supports their deployment with increased confidence. Another example is the Descriptive Machine Learning EXPlanations (DALEX) [Dal20] package, which offers various functionalities that help users understand how complex models work. Some works propose to enable domain experts to collaborate with each other to tackle this problem together [CJH19, FBG19]. In this context, information visualization (InfoVis) techniques have been shown to be effective in making analysts more comfortable with ML solutions. Krause et al. [KPB14], for example, present a case study of domain experts using their tool to explore predictive models in electronic health records. Also, in visual analytics (VA), the first stages to partially address those challenges have already been reached, for instance by discussing how global [RSG16a] or local [MPG∗14] interpretability can assist in the interpretation and explanation of ML [GBY∗18, Wol19], and how to interactively combine visualizations with ML in order to better trust the underlying models [SSK∗16].

We build our state-of-the-art report (STAR) upon the results of existing visualization research, which has emphasized the need for improved trust in areas, such as VA in general, dimensionality reduction (DR), and data mining. Sacha et al. [SSK∗16] aimed to clarify the role of uncertainty awareness in VA and its impact on human trust. They suggested that the analyst needs to trust the outcomes in order to achieve progress in the field. Sedlmair et al. [SBIM12] found important gaps between the needs of DR users and the functionalities provided by available methods. Such limitations reduce the trust that users can put in visual inferences made using scatterplots built from DR techniques. Bertini and Lalanne [BL09] concluded, from a survey, that visualization can improve model interpretation and trust-building in ML. An interesting paper by Ribeiro et al. [RSG16b] shows that the interest on using visualization to handle issues of trust is also present in the ML field. The authors describe a method that explains the predictions of any classifier via textual or visual cues, providing a qualitative understanding of the relationship between the instance’s components. Despite all the currently proposed solutions, many unanswered questions and challenges still remain, e.g., (1) If the analysts are not aware of the inherent uncertainties and trust issues that exist in an ML system, how to ensure that they do not form wrong assumptions? (2) Are there any guarantees that they will not be deceived by false (or unclear) results? (3) What problems of trustworthiness arise in each of the phases of a typical ML pipeline?

In this STAR, we present a general mapping of the currently available literature on using visualization to enhance trust in ML models. The mapping consists of details about which visualization techniques are used, what their reported effectiveness levels are, which domains and application areas they apply to, a conceptual understanding of what trust means in relation to ML models, and what important challenges are still open for research. Note that the terms trust and trustworthiness are used interchangeably throughout the report. The main scientific contributions of this STAR are:

- an empirically informed definition of what trust in ML models means;
- a fine-grained categorization of trust against different facets of interactive ML, extracted from 200 papers from the past 12 years;
- an investigation of existing trends and correlations between categories based on temporal, topic, and correlation analyses;
- the deployment of an interactive online browser (see below) to assist researchers in exploring the literature of the area; and
- further recommendations for future research in visualization for increasing the trustworthiness of ML models.

To improve our categorization, identify exciting patterns, and promote data investigation by the readers of this report, we have deployed an interactive online survey browser available at

https://trustmlvis.lnu.se

We expect that our results will support new research possibilities for different groups of professionals:

- beginners/non-experts who want to get acquainted with the field quickly and gain trust in their ML models;
- domain experts/practitioners of any discipline who want to find the appropriate visualization techniques to enhance trust in ML models;
- model developers and ML experts who investigate techniques to boost their confidence and trust in ML algorithms and models; and
- early-stage and senior visualization researchers who intend to develop new tools and are in search of motivation and ideas from previous work.

The rest of this report is organized as follows (see Figure 1). In Section 2, we introduce background information that we used in order to comprehend the concept of trustworthiness of ML models. We also describe our adopted definition of the meaning of trust in ML models. In Section 3, we discuss existing visualization surveys that are relevant to our work. Afterwards, Section 4 provides details with regard to our methodology, i.e., the searched venues and the paper collection process. The overview in Section 5 includes initial statistical information. In Section 6, we present our categorization and describe the most representative examples. In Section 7, we report the results of a topic analysis performed on these papers to find new and interesting topics and trends derived from them, and further findings from data-driven analysis. Our interactive survey browser and research opportunities are discussed in Section 8. Finally, Section 9 concludes the STAR. Additionally, a set of supplementary materials (referred to as S1 to S8) is also available, including the documents used to guide our categorization methodology, as well as the data that could not be part of this report due to space restrictions.

2. Background: Levels of Trustworthiness of Machine Learning Models

First, we present some earlier definitions of trust that are subsequently adapted to the context of our research. We also discuss
The issues of definition and operationalization of trust have been discussed in multiple research disciplines, including psychology [EK09] and management [MDS95]. Such definitions typically focus on trust in the context of expectations and interactions between individuals and organizations. The existing work in human-computer interaction (HCI) extends this perspective. For example, Shneiderman [Shn00] provides guidelines for software development that should facilitate the establishment of trust between people and organizations. To ensure trustworthiness of software systems, he recommends the involvement of independent oversight structures [Shn20]. Fogg and Tseng [FT99] state that “trust indicates a positive belief about the perceived reliability of, dependability of, and confidence in a person, object, or process”; in their work, trust is also related (and compared) to the concept of credibility. Rather than focusing on interpersonal trust, the existing work has also addressed trust in automation [HJBU13], which is more relevant to our research problem. Lee and See provide the following definition, widely used by the researchers in this context [LS04]: trust is “the attitude that an agent will help achieve an individual’s goals in a situation characterized by uncertainty and vulnerability”. This definition has been further extended by Hoff and Bashir [HB15], who propose a model of trust in automation with factors categorized into multiple dimensions and layers. Further adaptation of such multi-dimensional approach has been demonstrated, for example, by Yu et al. [YBC18], Lyons et al. [LHF18] adopt a model consisting of a non-orthogonal set of factors in their analysis of trust factors for ML systems. In this STAR, we rely on the rather general definition of trust by Lee and See [LS04] and further expand it into a more detailed, multi-level model presented below. Additionally, we make use of the definitions and factors of trust described in the existing work within the ML process; building upon these definitions and results, we group the identified factors of trust into five trust levels (TLs). These levels are a part of our overall methodology, discussed in Section 6.

Definitions of trust. The issues of definition and operationalization of trust have been discussed in multiple research disciplines, including psychology [EK09] and management [MDS95]. Such definitions typically focus on trust in the context of expectations and interactions between individuals and organizations. The existing work in human-computer interaction (HCI) extends this perspective. For example, Shneiderman [Shn00] provides guidelines for software development that should facilitate the establishment of trust between people and organizations. To ensure trustworthiness of software systems, he recommends the involvement of independent oversight structures [Shn20]. Fogg and Tseng [FT99] state that “trust indicates a positive belief about the perceived reliability of, dependability of, and confidence in a person, object, or process”; in their work, trust is also related (and compared) to the concept of credibility. Rather than focusing on interpersonal trust, the existing work has also addressed trust in automation [HJBU13], which is more relevant to our research problem. Lee and See provide the following definition, widely used by the researchers in this context [LS04]: trust is “the attitude that an agent will help achieve an individual’s goals in a situation characterized by uncertainty and vulnerability”. This definition has been further extended by Hoff and Bashir [HB15], who propose a model of trust in automation with factors categorized into multiple dimensions and layers. Further adaptation of such multi-dimensional approach has been demonstrated, for example, by Yu et al. [YBC18], Lyons et al. [LHF18] adopt a model consisting of a non-orthogonal set of factors in their analysis of trust factors for ML systems. In this STAR, we rely on the rather general definition of trust by Lee and See [LS04] and further expand it into a more detailed, multi-level model presented below. Additionally, we make use of the definitions and factors of trust described in the existing work within InfoVis and VA and incorporate them in our model. For example, Chuang et al. [CRMH12] define trust as “the actual and perceived accuracy of an analyst’s inferences”. Although important,
this definition touches only on a single perspective of trust: the
one related to the users’ expectations. The authors also mention
that usually, during evaluations of the design choices performed on
new visualization systems and tools, the modelling of choices and
relationships between views is often omitted. This practice intro-
duces limitations regarding the improvement of trust for the system
as a whole, as opposed to the trustworthiness of each view indi-
vidually.

In the uncertainty typology detailed by MacEachren et al. [MRO12],
trust is decomposed into three high-level types: (i) accuracy, de-

Table 1: Summary of the answers to the two open-ended questions
on the participants’ expectations and suggestions, which were pro-
vided at the end of the online questionnaire. The answers are sorted
based on the number of occurrences # and then alphabetically.

<table>
<thead>
<tr>
<th>Summary of open answers</th>
<th>#</th>
</tr>
</thead>
<tbody>
<tr>
<td>Everything (i.e., all together)</td>
<td>5</td>
</tr>
<tr>
<td>Data importance (i.e., impact of data in the output)</td>
<td>4</td>
</tr>
<tr>
<td>Feature importance</td>
<td>4</td>
</tr>
<tr>
<td>Evaluation</td>
<td>3</td>
</tr>
<tr>
<td>Impact of hyper-parameters</td>
<td>3</td>
</tr>
<tr>
<td>Pre-processing</td>
<td>3</td>
</tr>
<tr>
<td>Evolution of metrics during training</td>
<td>2</td>
</tr>
<tr>
<td>Investigation of outliers</td>
<td>2</td>
</tr>
<tr>
<td>Model accuracy and results in general</td>
<td>2</td>
</tr>
<tr>
<td>Raw data</td>
<td>2</td>
</tr>
<tr>
<td>Class separation</td>
<td>1</td>
</tr>
<tr>
<td>Decision boundaries</td>
<td>1</td>
</tr>
<tr>
<td>Learned features</td>
<td>1</td>
</tr>
<tr>
<td>Uncertainty</td>
<td>1</td>
</tr>
</tbody>
</table>

Online questionnaire. The next step of our work can be
dict to domain problem characterization [Mun09]. In order to
elicit the expectations and suggestions from ML practitioners
with regard to our problem, we distributed an online questionnaire
titled “How Would Visualization Help Enhancing Trust in Machine
Learning Models?” (see supplementary material S1). We received
answers from 27 participants, all with at least a Bachelor’s de-
gree, and most with a Master’s (40.7%) or a Doctorate degree
(51.9%). Almost all of them had their education in Computer Sci-
ence or related fields. Some participants have only used ML in a
few projects (around 33.3%), but most are either ML practition-
ers (22.2%) or developers/researchers in the field (44.4%). Their
experiences with different types of ML algorithms/models are di-
verse, with rather balanced numbers between supervised (85.2%)
and unsupervised (70.4%) learning. Within these two categories,
classification (95.7%) and clustering (89.5%) are the most popular,
respectively. The questionnaire itself begins with a description of a
hypothetical scenario where a real-world data set was used (Pima
Indians Diabetes, obtained from the UCI ML repository [DG17]).
Each of the 15 questions presents a possible use of visualization re-
lated to trust in ML, and participants are asked to score them from 1
(strong disagreement) to 5 (strong agreement). Questions are also
accompanied by short descriptions of some characteristics of the
proposed scenario, in order to help participants in answering them.

According to the results, the bulk of the answers in most of the
questions is concentrated around the scores of 4 and 5. This is evi-
dence that the overall attitude of the participants towards visuali-
zation for enhancing trust in ML is largely positive. Factors such as
visualizing details of the source of the data (Q1), data quality issues
(Q3), performance comparison of different ML algorithms (Q4),
hyper-parameter tuning (Q5), exploration of “what-if” scenarios
(Q11), and investigation of fairness (Q12) obtained the majority of
votes on score 5. Other factors which showed very positive—
but less overwhelming—opinions were the visualization of details
about the data collection process (Q2), data control and steering
during the training process (Q6 and Q9), feature importance (Q7),
visualizing the decisions of the model (Q8 and Q10), enabling col-
laboration (Q13), and the choice of tools for specific models (Q14).
In these cases the majority of the scores were 4, but with some
variance towards 3 and 5. The only question that deviated from
this trend was the last one (Q15), where we proposed that a sin-
gle well-designed performance metric would be enough to judge
the quality of an ML model, and no further actions (such as visu-
alization) would be necessary. In this case, most of the scores were
concentrated on either 1 or 2, showing clear disagreement.

The questionnaire ends with two open-ended questions, where
participants were free to give their ideas and opinions on which
steps of the ML process (or properties of the models and the data)
together would like to visualize to increase the trust in the ML models
they use. Many participants indicated their desire to visualize the
ML process as much as possible, in all phases where it might apply
(5 answers). Additionally, out of all the specific concepts and ideas
that emerged, the most popular were the visualization of feature
importance (4 answers), the impact of different characteristics of
the data instances (4 answers), investigation of hyper-parameters (3
answers), visualizing the pre-processing steps (3 answers), and the
evaluation of the model (3 answers). Table 1 summarizes all these
answers along with the number of occurrences. These answers were
mostly aligned with our prior hypotheses, but also enabled us to
gain new insights on what was missing from our categorization of
trust factors (see below). For instance, the source reliability cate-
gory was influenced by one participant who described her/his work
with Parkinson’s disease data and the reliability problems involved
with it: “For instance, I have been working with clinical studies
with Parkinson’s disease patients wearing sensors in their wrists.
For us researchers, it was difficult to see how the data was collected
e.g. patients could do a certain daily activity (e.g. cutting grass)
but in our model we accounted that as tremor.” Another important point
that was brought up is that visualization-based steering of the ML
training process might push the user to “fish” for desired results
and invalidate the statistical significance of the model.

Trust levels (TLs) and categories. In this STAR, we cover the
subject of enhancing trust in ML models with the use of visualiza-
tions. As such, we do not cover solutions proposed to address those
questions solely at the algorithmic level, even if they are consid-
ered with growing interest by ML researchers (as exemplified by
the two plenary invited talks [How18, Spi18] on the subject given
in 2018 at NeurIPS, one of the major ML venues). Based on the
existing work discussing the issues of trust, the suggestions from ML experts (see above), and internal discussions, we consider that the problem of enhancing trust in ML models has a multi-level nature. It can be divided into five **TLs** related to trustworthiness of the following: the raw data (→TL1), the processed data (→TL2), the learning method (i.e., the algorithms) (→TL3), the concrete model(s) for a particular task (→TL4), and the evaluation and the subjective users' expectations (→TL5). These levels of trust are aligned with the usual data analysis processes of a typical ML pipeline, such as (1) collecting the raw data; (2) allowing the user to label, pre-process, and query/filter the data; (3) interpreting, exploring, and explaining algorithms in a transparent fashion; (4) refining and steering concrete model(s); and (5) evaluating the results collaboratively. With the term algorithm, we define an ML method (e.g., logistic regression or random forest); in contrast to a model which is the result of an algorithm and is trained with specific parameters.

We use the term level to refer to the increasingly abstract nature of concepts as well as to emphasize the sequential aspect of the ML pipeline. Indeed, the lack of trustworthiness in each stage of the pipeline cumulatively introduces instability in the predictions of a model. Thus, trust issues (i.e., categories) that are relevant to two or more of our TLs are assigned to the lowest TL possible. This is similar to concerns about issues cascading from earlier to later
levels within the nested model for visualization design and validation [Mun09], for instance. Figure 2 displays the connection between a typical ML pipeline (slightly adapted from the work of Sun et al. [SLT17]) and the visualization techniques that enhance trust in ML models in various phases. In the bottom layer of Figure 2, we depict (in red) the ML pipeline comprising the distinct areas where users are able to interact with (and choose from) a large pool of alternatives or combinations of options. The layer above depicts the visualization (in purple). The upper layer consists of the different target groups that we address, the generation of knowledge, and the usability of this knowledge in solving problems stemming from real-life applications. Finally, the multiple categories of trust associated with each of these levels are presented in green in Figure 2 and discussed in detail below.

- **Raw data (TL1).** The lowest trust level gathers categories attached to the data collection itself. They belong to the complex task of preparing the data for further analysis, commonly referred to as data wrangling [KHP^11]. Arguably, source reliability is the very first category that should be visualized in a system. It should detect and handle the cases that do not meet the quality expectations or that show unusual behavior. For instance, detecting that some labels are unreliable could guide the user in selecting ML algorithms that are resistant to label noise [FV14]. However, perceiving source reliability is not an easy task, as it involves visualization questions, such as “how to visualize the data source involved in data collection?” and also the very statistical questions of measuring reliability. As a proxy for this measure, one can visualize information, for instance, “was a particular university involved in data collection, was a domain expert such as a doctor present during the health data collection, and were the sensors reliable and error-free?” Hence, source reliability is strongly related to ensuring a transparent collection process, the second category of this level. This includes visualizing the data collection process, what systems were used to collect the data, and how, why, and how objectively that was done.

Issues about reliability of the data and of the collection process can jeopardize, from the very start, the ML process and diminish the TLs set by users. If those issues remain undetected, they can spoil the later phases, according to the classic “garbage in, garbage out” principle. For instance in the case of unreliable labels [FV14], reported error rates are also unreliable. This is becoming more relevant with the growing attention given to adversarial machine learning, an ML research field which focuses on adversarial inputs designed to break ML algorithms or models [GMP18,LL10].

- **Data labeling & feature engineering (TL2).** The next group of categories has its focus beyond the raw data and into feature engineering and labeling of the data. This is also partially related to data wrangling. Trust issues at this level focus on particular instances, while the category described previously, considers data globally. For this level of trust, understanding/explanation is a very relevant category. It concerns the possible sources of subgroup-specific bias in the decision of an ML model. For instance, if a subgroup of the population has characteristics that are significantly different from the ones of the population as a whole, then the decisions for members of this subgroup could be unfair compared to the decisions for members of other subgroups. Visualization methods can be used to explore interesting subgroups and to pinpoint potential issues.

**Comparison (of structures)** [KCK17] implies the usage of visualization techniques in order to compare different structures in the data. As an example, experts in the biology domain would like to compare different structures visually, and furthermore, improve these representations with various encodings such as color.

**Guidance/recommendations** [CGM19] is a good continuation of the previous concept: trust can be improved by using visualization tools that (1) recommend new labels in the unlabeled data scenarios, for example, in semi-supervised learning and (2) guide the user to manage the data by adding, removing, and/or merging data features and instances.

Finally, for this level of trust, outlier detection, i.e., searching and investigating extreme values that deviate from other observations of a data set, can be alleviated by visualization systems (this is a major issue in ML [CBK09]). Detecting and manipulating in a meaningful way an observation that diverges from an overall pattern on a sample is a useful way to positively influence the results and boost overall trust in the process. Notice that this category focuses on particular instances, while the source reliability category described previously, considers data globally.

- **Learning method/algorithms (TL3).** This group of categories concerns the ML algorithms themselves, as the third step of the ML pipeline. Each category corresponds to a particular way of enabling a better control, in broad sense, over ML algorithms.

**Familiarity** is how visualization can support users in order to help them getting familiar with a certain learning method. There is a possibility that users are biased towards using an ML algorithm they know instead of the others that might actually be more appropriate. Improvement of familiarity by using visualization could help to both limit this type of bias and to enhance the users’ trust in algorithms they do not know well. Interpretability and explainability are among the most common and widespread categories—being found in most of the papers that we identified. We further subdivide both into the following categories:

- understand the reasons behind ML models’ behavior and why they deviate from each other (understanding/explanation);
- diagnose causes of unsuccessful convergence or failure to reach a satisfactory performance during the training phase (debugging/diagnosis);
- guide experts (and novices) to boost the performance, transparency, and quality of ML models (refinement/steering); and
- compare different algorithms (comparison).

It should be noted that the issue of interpretability and explainability has been receiving a growing attention in the ML commu-
nity. Algorithms are modified in order to produce models that are easier to interpret. However, those models are frequently claimed to be more interpretable based on general rules of thumb, such as “rule-based systems are easier to understand than purely numerical approaches” or “models using fewer features than others are easier to understand”. Only the most recent papers tend to include user-based studies [AGW18, CSWJ18]. Unfortunately, they only explore quite simple visualization techniques such as static scatterplots.

Knowledgeability translates to the question: if users are not aware of an ML algorithm, then how are they supposed to use it? Possible solutions to provide assistance to users in such situations include visualizations designed to compare different models or to provide details about each algorithm. However, the lack of visualization literacy limits the possibilities for exploration of an ML algorithm and negatively all the categories of this phase [KRBF14, BBG19]. Model-agnostic (more general) visualization techniques that consider multiple algorithms can also support this challenge.

Last but not least, the category of fairness covers the analysis of subgroup-specific effects in ML prediction, e.g., whether predictions are equally accurate for various subgroups; for instance, females versus males, or if there are discrepancies that give a group an advantage or a disadvantage compared to other groups. This topic has recently received a lot of attention in the ML community. It has been shown in particular that the most natural fairness and performance criteria are generally incompatible [KMR17]. Thus, ML algorithms must make some compromises between those criteria which justify the strong need for visually monitoring/analyzing such trade-offs.

**Concrete model(s) (TL4).** This final step of the ML pipeline consists of turning its inputs, mainly a set of ML learning methods/algorithms, into a concrete model or a combination of models [SKKC19]. Trust issues related to this step concern mostly performance related aspects, both in a static interpretation but also in a dynamic/interactive way.

Experience is a primary crucial factor, since promoting personalized visualizations based on the experiences of a user alter and might determine the selection. As an example, an expert in ML, a novice user, and a specific domain expert have different needs, and “what are their experiences and how can the visualization adapt to that?” is an important question.

In situ comparison can be described as comparing different snapshots and/or internal structures of the same concrete model in order to enhance trust.

Performance is another very common way to monitor the results of a model visually. Performance can objectively compare a model with another. However, this is usually insufficient for a complete understanding of the trade-off between different models.

What-if hypotheses appear when users search for impacts based on their interactions. A potential question is: “What is the consequence if we change one parameter and keep the rest stable for a specific model, or select some points to explore further?”

Model bias and model variance are well-known concepts originating from statistics with regard to the bias-variance trade-off. The bias is a systematic error created by the wrong hypotheses in a model. High bias can cause a model to avoid seeing the relevant associations between features and target outputs, thus underfitting. The variance is a manifestation of the model’s sensitivity or the lack thereof to the data, more precisely to the training set. It could also be the result of parameterizations or perturbations. High variance can result in a model which bears inside random noise in the training data, rather than the intended outputs, hence overfitting.

**Evaluation/user expectation (TL5).** The last group of categories is subsequent to visualization tools and techniques that oversee the ML pipeline, leading to knowledge generation in the overall workflow. Evaluation of models and meeting user expectations [CRMH12] is a key component for people to trust or not ML model(s) for a task.

Agreement of colleagues is supported by visualizations with provenance [OAB*17, RESC16] and collaborative visualizations which facilitate, for instance, ten experts from diverse domains to agree that a model performed well. This purpose could be served by provenance features and specific glyphs or snapshots, along with web-based online tools and platforms. When using visualizations, the choices of the visual metaphor and the visual variable (e.g., color instead of size) are important but can supplement the process negatively with visualization bias. This kind of bias was described, for example, by Lespinats and Aupetit [LA11]. However, this issue is being addressed by multiple ongoing research efforts in various subfields of visualization which are outside of the scope of this survey [MHSW19, XPGF19]. Thus, we have not included this perspective in our categorization.

A measure against visualization bias that we consider instead is the visualization evaluation [Mun09] that many authors of visualization papers perform. Quantitative or qualitative methods are used in the InfoVis and other communities to evaluate new visualization techniques. Both count as visualization evaluations, even receiving feedback from ML experts and/or domain experts before, during, or after the development of a visualization system.

Moreover, results/metrics validation is the most common method utilized by developers of visualization tools to indicate if a model can be trusted and has reached user expectations. However, we believe that it is not sufficient on its own.

Finally, user bias is a rarely addressed category which tries to understand the cognitive biases of users who have the power to steer an automated process. Questions such as where, when, and why a user has to interact with a model are still an open challenge. A paper from Nalcaci et al. [NGB*19], for example, works with distinction bias and confirmation bias in visualization systems that are related to user bias when viewing visualizations. Also, a recent survey from Dimara et al. [DFP*20] tries to connect the possibly-biased judgment and decision making of humans with specific visualization tasks.

3. Related Surveys

The challenge of enhancing trust in ML models has not yet received the same level of attention in systematic surveys as other topics, for example, the understanding and interpretation of DR or deep learn-
ing (DL). To the best of our knowledge, this is the only survey that deals with InfoVis and VA techniques for enhancing the trustworthiness of ML models. In order to confirm that, we carefully examined the online browser of the survey of surveys (SoS) paper from McNabb and Laramee [ML17], which contains 86 survey papers from main InfoVis venues. We have also investigated 18 additional survey papers in our own recent SoS paper [CMJK20]. Our analysis indicated that many of these surveys are about interpretable ML models, especially regarding current popular subjects such as interpretative and interactive ML (IML), predictive VA (PVA), DL, and clustering and DR. None of these papers, however, has an explicit focus on categorizing and/or analyzing techniques related specifically to the subject of trust in ML models. Related issues, such as accuracy, quality, errors, stress levels, or uncertainty in ML models, are touched upon by some of them, but in our work these issues are discussed in more detail. Particularly, uncertainty in the data and the visualization itself is a part of our TLs in the uncertainty awareness and the visualization bias categories. One of the main differences in our work is the focus on the transformation from uncertainty to trust, which should happen progressively in all phases of an ML pipeline. Some previous works offer brief literature reviews and propose frameworks for human-centered IML with visualization [SSZ∗16, SSZ∗17], the problem of integrating ML into VA [ERT∗17], trust in VA [SSK∗16], or comparison of DR techniques from an ML point of view [VDMPvdH09]. Although interesting, those papers fall outside the scope of the trust in ML models subject. One of the motivations for this STAR came from our analysis of the future work sections of these surveys—10 out of the 18 surveys highlight the subject of enhancing trust in the context of ML models, making this challenge one of the most emergent and essential to solve. This body of work also forms the basis for our methodological part of the literature research, presented in Section 4.

3.1. Interpretable and Interactive Machine Learning

The work concerning the interpretability of ML models in the visualization community started to emerge around 15 years ago. This opportunity was captured by Liu et al. [LWLZ17] who conducted a survey that summarizes several ML visualization tools focusing on three categories (understanding, diagnosis, and refinement). This is different compared to our perspective and goal to categorize only those papers that tackle the problem of enhancing trust in ML models. The recent publication by Du et al. [DLH20] groups techniques for interpretable ML into intrinsic and post-hoc, which can be additionally divided into global and local interpretability. The authors also suggest that these two types of interpretability bring several advantages, for example, that users trust an algorithm and a model’s prediction. However, they do not analyze in details the different aspects of enhancing trust in ML models as we performed in this STAR. Overall, these surveys (and the categories from Liu et al. [LWLZ17], together with comparison) target the interpretability and explainability at the level of ML algorithms, which are themes under the umbrella of VIS4ML (visualization for ML) and comprise only a small subset of our proposed categorization.

Moreover, the topic of IML aided by visualizations has been discussed in many papers recently, as it was summarized in the surveys by Amershi et al [ACKK14] and Dudley and Kristensson [DK18]. The former focused on the role of humans in IML and how much users should interfere and interact with ML. They also suggested at which stages this interaction could happen and categorized their papers accordingly. Steering, refining, and adjusting the model with domain knowledge are not trivial tasks and can introduce cumulative biases into the process. Due to this, in this STAR our analysis focuses on the biases that a user might introduce into a typical ML pipeline. Furthermore, visualizations may introduce different biases to the entire process, as discussed in the previous Section 2. In such situations, the visualization design should be directed towards conveying, or occasionally removing, any of these biases initially and not simply making it easier for users to interact with ML models.

3.2. Predictive Visual Analytics

Lu et al. [LGH∗17] adopted the pipeline of PVA, which consists of four basic blocks: (i) data pre-processing, (ii) feature selection and generation, (iii) model training, and (iv) model selection and validation. These are complemented by two additional blocks that enable interaction with the pipeline: (v) visualization and (vi) adjustment loop. The authors also outline several examples of quantitative comparisons of techniques and methods before and after the use of PVA. However, no analysis has been performed about trust issues that are incrementally added in each step of the pipeline. Another survey written by Lu et al. [LCM∗17] follows a similar approach by classifying papers utilizing the same PVA pipeline, but with two new classes: (a) prediction and (b) interaction. For instance, regression, classification, clustering, and others are the primary subcategories of the prediction task; and explore, encode, connect, filter, and others, are subcategories of interaction. This work inspired us to introduce the interaction technique subcategory of our basic category, called visualization. One unique addition, though, is the verbalize category, which describes how visualization and use of words can assist each other by making the visual representation more understandable to users and vice versa. Concluding, none of these survey papers so far provide future opportunities touching the subject of how visualization can boost ML models’ trustworthiness.

3.3. Deep Learning

Grün et al. [GRNT16] briefly explain how the papers they collected are separated to their taxonomy for feature visualization methods. The authors defined three discrete categories as follows: (i) input modification methods, (ii) deconvolutional methods, and (iii) input reconstruction methods. Undoubtedly, learned features of convolutional neural networks (CNNs) are a first step to provide trust to users for the models. But still, this step belongs to the interpretability and explainability of a specific algorithm, i.e., very specialized and targeted to CNNs. In our work, we cover not only CNNs but every ML model with a focus on the data, learning algorithms, concrete models, users, and thus not only on the model. The two main contributions of Seifert et al. [SAB∗17] are the analysis of insights that can be retrieved from deep neural network (DNN) models with the use of visualizations and the discussion about the visualization techniques that are appropriate for each type of insight. In their paper, they surveyed visualization papers and distributed them into...
five categories: (1) the visualization goals, (2) the visualization methods, (3) the computer vision tasks, (4) the network architecture types, and (5) the data sets that are used. This paper is the only one that contains analyses for the data sets used in each visualization tool, which worked as a motivation for us to include a data set analysis in our survey. However, their main contributions do not touch the problem of trustworthiness, but more the correlation of visualizations and patterns extraction (or insights gaining) for DNNs. A summarization of the field of interpreting DL models was performed by Samek et al. [SWM18], putting into the center the increasing awareness of how interpretable and explainable ML models should be in real life. The main goal of their survey is to foster awareness of how useful it is to have interpretable and explainable ML models. General interpretability and explainability play a role in increasing trustworthiness, but not a major one. The different stages of the ML pipeline should be taken into account as from early stages, bias and deviation can occur and grow when processing through the pipeline. Zhang and Zhou [ZZ18] study their papers starting from the visualization of CNN representations between network layers, over the diagnosis of CNN representations, and finally examining issues of disentanglement of “the mixture of patterns” of CNNs. They neither provide a distinct methodology of categorization for their survey, nor insights on the problem of trust as opposed to our survey.

Another batch of papers on DL assembles into Garcia et al.’s [GtDS*18] survey in which visualization tools addressing the interpretability of models and explainability of features are described. The authors focus on various types of neural networks (NNs), such as CNNs and recurrent neural networks (RNNs), by incorporating a mathematical viewing angle for explanations. They emphasize the value of VA for the better understanding of NNs and classify their papers into three categories: (a) network architecture understanding, (b) visualization to support training analysis, and (c) feature understanding. In a similar sense, (i) model understanding, (ii) debugging, and (iii) refinement/steering are three directions that Choo and Liu [CL18] consider. Model understanding aims to communicate the rationale behind model predictions and spreads light to the internal operations of DL models. In cases when the DL models underperform or are unable to converge, debugging is applied to resolve such issues. Finally, model refinement/steering refers to methods that enable the interactive involvement of usually experienced experts who build and improve DL models. Compared to our survey, only half of the learning methods are considered. Thus, their reader support is limited when it comes to show how their algorithms actually work on several occasions. Yu and Shi [YS18] examined visualization tools that support the user to accomplish four high-level goals: (1) teaching concepts, (2) assessment of the architecture, (3) debugging and improving models, and (4) visual exploration of CNNs, RNNs, and other models. They describe four different groups of people in their paper: (a) beginners, (b) practitioners, (c) developers, and (d) experts, distributed accordingly to the four aforementioned classes. These groups are also considered in our work. Nonetheless, teaching concepts and assessing the architectures of DNNs are particular concepts that do not enhance trust explicitly. This is why we focus on multiple other categories, such as models’ trade-off of bias and variance or in situ comparisons of structures of the model, in general and not exclusively for DL models. Hohman et al. [HKPC19] surveyed VA tools that explore DL models by investigating papers into six categories answering the aspects of “who”, “why”, “what”, “when”, “where”, and “how” of the collected papers. Their main focus is on interpretability, explainability, and debugging models. The authors conclude that just a few tools visualize the training process, but solely consider the ML results. Our ML processing phase category is motivated by this gap in the literature, i.e., we investigate this challenge in our paper to gain new insights about the correlation of trust and visualization in pre-processing, in-processing, and post-processing of the overall ML processing phases. Finally, as many explainable DL visualization tools incorporate clustering and DR techniques to visualize DL internals, the results of these methods should be validated on how trustworthy they are.

3.4. Clustering and Dimensionality Reduction

Sacha et al. [SZS*17] propose, in their survey, a detailed categorization with seven guiding scenarios for interactive DR: (i) data selection and emphasis, (ii) annotation and labeling, (iii) data manipulation, (iv) feature selection and emphasis, (v) DR parameter tuning, (vi) defining constraints, and (vii) DR type selection. During the annotation and labeling phase, for example, hierarchical clustering could assist in defining constraints which are then usable by DR algorithms. Nonato and Aupetit [NA19] separate the visualization tools for DR according to the categories linear and nonlinear, single-versus multi-level, steerability, stability, and others. Due to the complexity of our own categorization and our unique goals, we chose to use only their first category (linear versus nonlinear), as is common in previous work [VDMPVdh09]. Nonato and Aupetit also describe different quality metrics that can be used to ensure trust in the results of DR. However, as the results of our online questionnaire suggested (cf. Section 2), comparing those quality metrics alone is probably not sufficient. To conclude, the main goal of these two surveys is not related to ML in general, and the latter one only discusses trust in terms of aggregated quality metrics. This is a very restricted approach when compared to our concept of trust, which should be ensured at various levels, such as data, learning method, concrete model(s), visualizations themselves, and covering users expectations.

4. Methodology of the Literature Search

In the following, we present the methodology used to identify and systematically structure the papers of our STAR. Our work is inspired by the same methodology guidelines from Lu et al. [LGH*17], Garcia et al. [GtDS*18], and Sacha et al. [SZS*17] presented in Section 3. In an initial pilot phase (cf. [Sny19]), we extracted appropriate keywords from ten relevant papers [VKSP15, WCJCC16], including those that deal with the problems of interpretable/explainable ML (which are closely related to trust in ML). The keywords were divided into two lists with the goal to cover both trust and ML. For trust, the used keywords were, in alphabetical order: “accuracy”, “assess”, “bias”, “black box”, “confidence”, “diagnose”, “distort”, “error”, “explain”, “explore”, “feedback”, “guide”, “interact”, “noise”, “quality”, “robustness”, “stress”, “trust” “uncertainty”, “validate”, “verify”, and their.

© 2020 The Author(s)
Computer Graphics Forum © 2020 The Eurographics Association and John Wiley & Sons Ltd.
derivatives. For ML, the searched keywords were: “artificial intelligence”, “classification”, “clustering”, “deep learning”, “dimensionality reduction”, “machine learning”, “neural network”, “projections”, and all the types of ML (e.g., “supervised learning”).

The keywords from the two lists were combined into pairs, such that each keyword from the first list was paired with each keyword from the second. These paired keywords were used for seeking papers relevant to the focus of this survey in different venues (cf. Section 4.1). A validation process was used in order to scan for new papers and admit questionable cases, as described in Section 4.2. Papers that were borderline cases and eventually excluded are discussed in Section 4.3.

4.1. Search and Repeatability

To gather our collection of papers, we manually searched for papers published in the last 12 years (from January 2008 until January 2020). We started our search from InfoVis journals, conferences, and workshops, and later extended it to well-known ML venues (the complete list can be found at the end of this subsection). Moreover, when seeking papers in ML-related venues (e.g., the International Conference on Machine Learning, ICML), we included two additional keywords: “visual” and “visualization”.

Within the visualization domain, we checked the following resources for publications:


Conferences: IEEE Visual Analytics in Science and Technology (VAST), IEEE Visualization Conference (VIS) short papers track, Eurographics Visualization (EuroVis), IEEE Pacific Visualization (PacificVis), ACM Conference on Human Factors in Computing Systems (CHI), and ACM Intelligent User Interfaces (UII).

Workshops: Visualization for AI Explainability (VISxAI), EuroVis Workshop on Trustworthy Visualization (TrustVis), International EuroVis Workshop on Visual Analytics (EuroVA), Machine Learning Methods in Visualisation for Big Data (MLVis), Visualization for Predictive Analytics (VPA), Visual Analytics for Deep Learning (VADL), IEEE Large Scale Data Analysis and Visualization (LDAV), and Visualization in Data Science (VDS).

Within the ML domain, we checked the following venues:

Conferences: ICML, Knowledge Discovery and Data Mining (KDD), and European Symposium on Artificial Neural Networks, Computational Intelligence, and Machine Learning (ESANN).

Workshops: ICML Workshop on Visualization for Deep Learning (DL), ICML Workshop on Human Interpretability in ML (WHI), KDD Workshop on Interactive Data Exploration & Analytics (IDEA), NIPS Workshop on Interpreting, Explaining and Visualizing Deep Learning.

The search was performed in online libraries, such as IEEE Xplore, ACM Digital Library, and Eurographics Digital Library. As an example of the number of results we got, both IEEE Transactions on Visualization and Computer Graphics (TVCG) and IEEE Visual Analytics in Science and Technology (VAST) together resulted in around 750 publications. Due to the use of a couple of broad keyword combinations in order to cover our main subject effectively, some of the papers collected were not very relevant. They were sorted out in the next phase of our methodology.

4.2. Validation

For the sake of completeness, we quickly browsed through each individual paper’s related work section and tried to identify more relevant papers (a process known as snowballing [Woh14]). With this procedure, we found more papers belonging to other venues, such as the Neurocomputing Journal, IEEE Transactions on Big Data, ACM Transactions on Intelligent Systems and Technology (ACM TIST), the European Conference on Computer Vision (ECCV), Computational Visual Media (CVM), and the Workshop on Human-In-the-Loop Data Analytics (HILDA), co-located with the ACM SIGMOD/PODS conference. In more detail, this validation phase was performed in four steps:

1. we removed unrelated papers by reading the titles, abstracts, and investigating the visualizations;
2. we split the papers into two categories: approved and uncertain;
3. uncertain papers were reviewed by at least two authors, and if the reviewers agreed, they were moved to the approved papers;
4. for the remaining papers (i.e., where the two reviewers disagreed), a third reviewer stepped in and decided if the paper should be moved to the approved category or discarded permanently.

The calculated amount of disagreement, i.e., the number of conflicts in the 70 uncertain cases, was less than 20% (approximately 1 out of 5 papers). This process led to 200 papers that made it into the survey.

4.3. Borderline Cases

We have restricted our search to papers with visualization techniques that explicitly focus on supporting trust in ML models, and not on related perspectives (e.g., assisting the exploration and labeling process of input data with visual means). Therefore, papers such as those by Bernard et al. [BH18, BSA18], Gang et al. [GR10], and Kucher et al. [KPS17], although undoubtedly interesting, are out of the scope of our survey, since their research contributions are exclusively based on labeling data. Other partially-related papers [AAS19, AW12, BHG14, FBT10, SBTK08, ZSC18] are also not included because they focus on using clustering solely to explore the data, without addressing inherent problems of the method. For similar reasons, the paper by Wenskovitch et al. [WC18], that tries to connect and aggregate benefits from clustering and DR methods, was excluded. Moreover, papers on high-dimensional data clustering or exploratory data analysis are not included (e.g., Behrisch et al. [BKSS14], Lehmann et al. [LKZ15], Nam et al. [NM07], and Wu et al. [WC15]). Finally, there are related works that provide important contributions to the visualization community, but do not study trust explicitly, and thus were not included:
improving the computational performance of algorithms (e.g., t-SNE) [PHL*16, PLvdM*17], frameworks and conceptual designs for closing the loop [SKBG*18], investigating cognitive biases with respect to users [CCR*19], and enabling collaboration with the use of annotations [CBY10].

5. General Overview of the Relations Between the Papers

This section begins with a meta-analysis of the spatiotemporal aspects of our collection of papers. The analysis shows, on the one hand, that there is an increasing trend in trust-related subjects; on the other hand, it also highlights the struggles of collaborations between visualization researchers and ML experts. Additionally, we generated a co-authorship network to observe the connections of the authors from all the papers. By exploring the network and its missing links, we hope to bring researchers closer to form new collaborations towards research in the trustworthiness of ML models.

Time and venues. Our collection of papers comprises 200 entries from a broad range of journals, conferences, and workshops. The analysis of the temporal distribution (see Figure 3) shows a stable growth in interest in the topic since 2009, with a sharp increase in 2018 and 2019 (and promising numbers also for 2020). The numbers for the publication venues identified can be seen in Table 2. Visualization researchers seem to be very interested in working with solutions to this problem and try to extend their work in ML venues with the creation of new workshops. There is a large number of workshops on the topic, co-located with ML venues, which indicates that researchers are interested in reaching out of their respective areas in order to collaborate. However, the small number of publications outside of visualization venues could possibly show a struggle of visualization researchers to find and collaborate with ML experts. It might also indicate that ML experts are not fully aware of the possibilities that the visualization field provides.

Co-authorship analysis. We analyzed the co-authorship network of the authors of our collection of papers using Gephi [BHU09], as presented in Figure 4. The goal was to identify a potential lack of collaboration within the visualization and ML communities. Enhancing collaboration between specific groups may lead to improvements in the subject of boosting trust in ML models with visualizations. The more connections an author has, the bigger is the size of the resulting node, i.e., the in-degree values of the graph nodes are represented by node size in the drawing. We colored the top eight clusters with the highest overall in-degree for all the nodes of each cluster. Finally, we filtered the node labels (authors first names and surnames) by setting a limit to the in-degree value in order to reduce clutter. By looking at the resulting co-authorship network (see Figure 4 and S2), we can observe a huge cluster in violet (1). In this cluster, Huamin Qu, Remco Chang, Daniel A. Keim, Cagatay Turkay, and Nan Cao seem to be the most prominent authors, with many connections. If we consider different subclusters in this massive cluster, Nan Cao is the bridge between some of the subclusters. Another cluster on the left (with light green color (2)) is related to the big industries (such as Google and Microsoft) with Fernanda B. Viégas, Martin Wattenberg, and Steven M. Drucker as the most eye-catching names. Interestingly, this industry cluster is very well separated from the remaining academic clusters. Potentially, the connection of this industry cluster with the remaining clusters could have an impact on the research output produced by the visualization community. There are many smaller clusters of collaborating people, for example, the cluster with David S. Ebert and Wei Chen (3), Klaus Mueller (4), Han-Wei Shen (5), Alexandru C. Telea (6), Valerio Pascucci (7), and others (e.g., (8)) obviously serving as main coordinators.

6. In-Depth Categorization of Trust Against Facets of Interactive Machine Learning

In this section, we discuss the process and results of our categorization efforts. We introduce a multifaceted categorization system with the aim to provide insights to the reader about various aspects of the data and ML algorithms used in the underlying literature. The main sources of input for the categorization were the previous work from the surveys discussed in Section 3, the iterative process of selecting papers (and excluding the borderline cases) described in Section 4, and the feedback received from the online questionnaire (Section 2). The top two levels of the proposed hierarchy of categories can be seen below, with 8 overarching aspects (6.1 to
Figure 4: Co-authorship network visualization with the eight largest connected components (1–8) highlighted in different colors. The node size represents the in-degree centrality of each author. The labels are filtered based on the in-degree value in order to reduce clutter.

6.8), partitioned into 18 category groups (6.1.1 to 6.6.3, plus TL1 to TL5), resulting in a total of 119 individual categories.

- 6.1. Data
  - 6.1.1. Domain (10 categories)
  - 6.1.2. Target Variable (5 categories)
- 6.2. Machine Learning
  - 6.2.1. ML Methods (16 categories)
- 6.2.2. ML Types (10 categories)
- 6.3. ML Processing Phase (3 categories)
- 6.4. Treatment Method (2 categories)
- 6.5. Visualization
  - 6.5.1. Dimensionality (2 categories)
  - 6.5.2. Visual Aspects (2 categories)
  - 6.5.3. Visual Granularity (2 categories)
  - 6.5.4. Visual Representation (19 categories)
• 6.6. Evaluation
  – 6.6.1. User Study (2 categories)
  – 6.6.2. User Feedback (2 categories)
  – 6.6.3. Not Evaluated (1 category)
• 6.7. Trust Levels (TL) 1–5
  – TL1: Raw Data (2 categories)
  – TL2: Processed Data (5 categories)
  – TL3: Learning Method (7 categories)
  – TL4: Concrete Model (6 categories)
  – TL5: Evaluation/User Expectation (4 categories)
• 6.8. Target Group (4 categories)

The complete overview of all categories is shown in Table 3 (also in S3 as a mind map). The aspect and category group names are preceded by the subsection numbers where they are introduced and discussed. This is to avoid confusion and to reduce the cognitive load of the reader.

Designing the categorization. Compared to previous surveys, we created new categories to better cover the 200 papers we included in our STAR. In the following list, we present the basic purpose for each aspect, along with the core similarities and differences when compared to the related surveys from Section 3.

• 6.1. Data tries to create a link between the input data/application and the enhancement of trust in ML models. The first category group we identified in this aspect is the data domain. We took the inspiration from our previous publication [KPK18], but the categories are significantly different to fit the current subject. In the case of the target variable, we conceived the idea of separating the independent variable of each data set.

• 6.2. Machine Learning is an inherent component in boosting the trustworthiness of ML models. We used several sources for defining parts of the ML methods category group. Different neural networks methods, such as CNNs, RNNs, DCNs, and DNNs, were contained in other works [SAB17, YS18]. Also, as mentioned in Section 3, linear and non-linear DR is an existing categorization from [NA19], but ensemble learning and the remaining DL categories are new to our STAR. ML types, such as classification, regression, and clustering, can be seen in the work [LGH17], but we improved this short categorization by using the complete supervised, unsupervised, semi-supervised, and reinforcement learning distinction.

• 6.3. ML Processing Phase connects the ML and the visualization aspects and shows when VA techniques are deployed to improve the trustworthiness of the ML models. During and after training categories can be found in the work of Hohman et al. [HKPC19], which in our case are adjusted to the newly introduced pre-processing, in-processing, and post-processing phases.

• 6.4. Treatment Method deals with differences between model-agnostic or model-specific approaches. Observing such distinctions might indicate where the community should later focus on to better boost the trust in ML models. Model-agnostic vs. model-specific methods used in VA systems are first described in our work, although Dudley and Kristensson [DK18] hinted about model agnosticism.

• 6.5. Visualization is another inherent component of how increasing trust in ML models can be achieved. Visualization details, such as dimensionality, can also be found in the work of Kucher et al. [KK15]. However, we added visual aspects and granularity. Visual representation was also inspired by Kucher et al. [KK15] and many of the other related surveys. The verbalize category is a novel addition to pre-existing work, which is part of the 6.5.5. Interaction Technique group described in the work of Lu et al. [LCM17]. Finally, for this aspect, the work of Kucher et al. [KPK18] covers all the visual variables used by us except for opacity.

• 6.6. Evaluation of visualization can reduce the visualization bias, thus boosting even further the application of VA systems for ML. We are among the first who included this new aspect to highlight the importance of evaluations in visualization systems, tools, and techniques.

• 6.7. Trust Levels (TL) 1–5, introduced in Section 2, is the most novel category group. Only TL3, which contains the interpretability/explainability group of categories, is described in previous works [LWLZ17, CL18]. Despite that, comparison is a fresh addition to this group.

• 6.8. Target Group is equally important to the problem of enhancement of the trustworthiness in ML models as the input (i.e., the data) and the actual visualization. This aspect is inspired mainly by Yu and Shi’s paper [YS18].

Overall, this extensive categorization aims to completely unveil the relationship between trust and the remaining categories, as can be seen later in Figure 6 and Section 7.

Filling in the categorization. To ensure consistency during the process of assigning the 200 papers to our categories in a first cycle, we created a code of practice (see S4) as a base structure. This base structure provides guidance to evaluate the individual papers in the same way without misalignment between the authors of this STAR. We also cleared and double-checked the resulting data for any issues that could come up with the annotated data in a second cycle. In particular, we looked for the following issues: (1) outliers, (2) typos, (3) discrepancies, and (4) inconsistencies between different evaluators by inspecting and removing any obscure and misclassified data cases. The fact that a large subset of the papers (75%) were classified by the same author also maximizes the consistency of their final categorization. Each classified paper belongs to zero, one or more categories for every aspect depending on the information the paper contains. Due to the page limits and readability concerns, we cannot discuss all 200 papers in this section. Instead, we only focus on the most prominent and (in our opinion) most important ones. All 200 papers are referenced in Table 4 and are part of the bibliography. The complete survey data set, including the individual categorization for each paper, is provided in our online survey browser (see Fig. 8) and in S5.

6.1. Data

Many visualization techniques have been tested with specific data sets coming from different domains. However, just a few of them specifically work for one type of data set, for instance, the systems proposed by Bremm et al. [BvLBS11] and Wang et al. [WGZ19]. In this subsection, we present the most frequent data domains we
Table 3: The categorization used in our survey. The total number of corresponding visualization techniques per category is shown in every row, along with heatmap-style icons.

<table>
<thead>
<tr>
<th>6.1. Domain</th>
<th>6.3. ML Processing Phase</th>
<th>6.5.6. Visual Variable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Biology</td>
<td>Pre-processing / Input</td>
<td>Color</td>
</tr>
<tr>
<td>Business</td>
<td>In-processing / Model</td>
<td>Opacity</td>
</tr>
<tr>
<td>Computer Vision</td>
<td>Post-processing / Output</td>
<td>Position / Orientation</td>
</tr>
<tr>
<td>Computers</td>
<td></td>
<td>Shape</td>
</tr>
<tr>
<td>Health</td>
<td></td>
<td>Size</td>
</tr>
<tr>
<td>Humanities</td>
<td></td>
<td>Texture</td>
</tr>
<tr>
<td>Nutrition</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Simulation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Social / Socioeconomic</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Binary (categorical)</td>
<td>Model-agnostic / Black Box</td>
<td>Standard</td>
</tr>
<tr>
<td>Multi-class (categorical)</td>
<td>Model-specific / White Box</td>
<td>Comparative</td>
</tr>
<tr>
<td>Multi-label (categorical)</td>
<td></td>
<td>Before / During Development</td>
</tr>
<tr>
<td>Continuous (regression problems)</td>
<td></td>
<td>After Development</td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td>Not Evaluated</td>
</tr>
<tr>
<td>6.1.2. ML Methods</td>
<td>6.5.1. Dimensionality</td>
<td>6.7. Trust Levels (TL) 1–5</td>
</tr>
<tr>
<td>Convolutional Neural Network (CNN)</td>
<td>2D</td>
<td>Source Reliability</td>
</tr>
<tr>
<td>Deep Convolutional Network (DCN)</td>
<td>3D</td>
<td>Transparent Collection Process</td>
</tr>
<tr>
<td>Deep Feed Forward (DFF)</td>
<td></td>
<td>Uncertainty Awareness</td>
</tr>
<tr>
<td>Deep Neural Network (DNN)</td>
<td></td>
<td>Equality / Data Bias</td>
</tr>
<tr>
<td>Deep Q-Network (DQN)</td>
<td></td>
<td>Comparison (of Structures)</td>
</tr>
<tr>
<td>Generative Adversarial Network (GAN)</td>
<td></td>
<td>Guidance / Recommendations</td>
</tr>
<tr>
<td>Long Short-Term Memory (LSTM)</td>
<td></td>
<td>Outlier Detection</td>
</tr>
<tr>
<td>Recurrent Neural Network (RNN)</td>
<td></td>
<td>Familiarity</td>
</tr>
<tr>
<td>Variational Auto-Encoder (VAE)</td>
<td></td>
<td>Understanding / Explanation</td>
</tr>
<tr>
<td>Other (DL methods)</td>
<td></td>
<td>Debugging / Diagnosis</td>
</tr>
<tr>
<td>Linear (DR)</td>
<td></td>
<td>Refinement / Steering</td>
</tr>
<tr>
<td>Non-linear (DR)</td>
<td></td>
<td>Comparison</td>
</tr>
<tr>
<td>Bagging (ensemble learning)</td>
<td></td>
<td>Knowledgeability</td>
</tr>
<tr>
<td>Boosting (ensemble learning)</td>
<td></td>
<td>Fairness</td>
</tr>
<tr>
<td>Stacking (ensemble learning)</td>
<td></td>
<td>Experience</td>
</tr>
<tr>
<td>Other (generic)</td>
<td></td>
<td>In Situ Comparison</td>
</tr>
<tr>
<td>6.2. ML Types</td>
<td>6.5.2. Visual Aspects</td>
<td>6.8. Target Group</td>
</tr>
<tr>
<td>Classification (supervised)</td>
<td>Computed</td>
<td>Beginners</td>
</tr>
<tr>
<td>Regression (supervised)</td>
<td>Mapped</td>
<td>Practitioners / Domain Experts</td>
</tr>
<tr>
<td>Other (supervised)</td>
<td>Instance-based / Individual</td>
<td>Developers</td>
</tr>
<tr>
<td>Association (unsupervised)</td>
<td></td>
<td>Model Experts</td>
</tr>
<tr>
<td>Clustering (unsupervised)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dimensionality Reduction (unsupervised)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Classification (semi-supervised)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clustering (semi-supervised)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Classification (reinforcement)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Control (reinforcement)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.5. Interaction Technique</td>
<td>Bar Charts</td>
<td>6.8.1. Trust Levels (TL) 1–5</td>
</tr>
<tr>
<td>Select</td>
<td>82</td>
<td>Standard</td>
</tr>
<tr>
<td>Explore / Browse</td>
<td>11</td>
<td>Comparative</td>
</tr>
<tr>
<td>Reconfigure</td>
<td>50</td>
<td>Before / During Development</td>
</tr>
<tr>
<td>Encode</td>
<td>63</td>
<td>After Development</td>
</tr>
<tr>
<td>Filter / Query</td>
<td>19</td>
<td>Not Evaluated</td>
</tr>
<tr>
<td>Abstract / Elaborate</td>
<td>19</td>
<td></td>
</tr>
<tr>
<td>Connect</td>
<td>46</td>
<td></td>
</tr>
<tr>
<td>Guide / Shepherd</td>
<td>56</td>
<td></td>
</tr>
<tr>
<td>Verbalize</td>
<td>66</td>
<td></td>
</tr>
<tr>
<td>6.7. Trust Levels (TL) 1–5</td>
<td>Node-link Diagrams</td>
<td>6.9. Experience</td>
</tr>
<tr>
<td>Not Evaluated</td>
<td>47</td>
<td>Understanding / Explanation</td>
</tr>
<tr>
<td>After Development</td>
<td>6</td>
<td>Debugging / Diagnosis</td>
</tr>
<tr>
<td>Not Evaluated</td>
<td>5</td>
<td>Refinement / Steering</td>
</tr>
<tr>
<td>After Development</td>
<td>4</td>
<td>Comparison</td>
</tr>
<tr>
<td>Not Evaluated</td>
<td>3</td>
<td>Knowledgeability</td>
</tr>
<tr>
<td>After Development</td>
<td>1</td>
<td>Fairness</td>
</tr>
<tr>
<td>Not Evaluated</td>
<td>2</td>
<td>Experience</td>
</tr>
<tr>
<td>After Development</td>
<td>1</td>
<td>In Situ Comparison</td>
</tr>
<tr>
<td>Not Evaluated</td>
<td>1</td>
<td>Performance</td>
</tr>
<tr>
<td>After Development</td>
<td>1</td>
<td>What-if Hypotheses</td>
</tr>
<tr>
<td>Not Evaluated</td>
<td>1</td>
<td>Model Bias</td>
</tr>
<tr>
<td>After Development</td>
<td>1</td>
<td>Model Variance</td>
</tr>
<tr>
<td>Not Evaluated</td>
<td>1</td>
<td>Agreement of Colleagues</td>
</tr>
<tr>
<td>After Development</td>
<td>1</td>
<td>Visualization Evaluation</td>
</tr>
<tr>
<td>Not Evaluated</td>
<td>1</td>
<td>Metrics Validation / Results</td>
</tr>
<tr>
<td>After Development</td>
<td>1</td>
<td>User Bias</td>
</tr>
</tbody>
</table>

Legend: □ 0 papers □ 100 papers □ 200 papers

... spotted and the nature of the target variable that should be predicted by ML classifiers.

6.1.1. Domain

DeepVID, by Wang et al. [WGZ’19], is an example that focuses only on images (i.e., the overall field of computer vision). It shows how ML models for image classification can be interpreted and debugged with the use of simpler models (e.g., a linear model) in DNNs. Since DNNs usually work well with image data, exploring and diagnosing the training process of a DNN is an initial step towards boosting trust in them. With regard to humanities data, Sherkat et al. [SNM18] propose a system that empowers users...
incorporating their feedback to define several diverse algorithms for clustering. The supported interactions enable users to adjust (or even create) new key terms, which are then used to supervise the algorithms and cluster the different documents. Involving humanities experts in user studies to evaluate the effectiveness of VA systems can further increase trust. An example of operating with health data is INFUSE [KPB14], which helps analysts to select features and retrieve extra information based on a selection from a collection of algorithms, cross-validations folds, and different ML models. The visual representations assist domain experts (i.e., doctors) in manipulating their medical records more precisely and improve the accuracy of the results. In this case, the visualization tool seems to be generalizable to other domains. In medicine, receiving recommendations during the data processing phase is necessary to ensure that no further biases are introduced in the input phase of an ML model. This guidance is better achievable by feature exploration and feature selection with the use of visualization. Bremm et al. [BvLBS11] focus on biological data sets. In their paper, the authors utilize scatterplot- and grid-based visualizations to facilitate selection and later comparison of data descriptors for unlabeled biology-related data. Except for the comparison of data and structures, any uncertainties stemming from the data should be highlighted for the biologists to focus on them. As a consequence, this extraction of patterns through visualization can increase their trust in ML. A number of papers focus on various other data domains, such as the works of Gleicher [Gle13], Sips et al. [SNLH09], and Tatu et al. [TMF∗12].

6.1.2. Target Variable

In ML, the target (or response) variable is the characteristic known during the learning phase that has to be predicted for new data by the learned model. In classification problems, it can take a binary value for two-class problems, a single label for multi-class problems, or even a set of labels for multi-label problems. In regression problems, it is generally a continuous variable. On the one hand, Krause et al. [KDS∗17] propose a workflow to help practitioners to examine, diagnose, and explain the decisions made by a binary classifier. In their approach, instance-level explanations are obtained based on local feature significance measures that explain single instances. With these findings as a basis, they develop visualizations that lead the users to important areas of investigation. Extensions of this approach could evaluate the reliability of the incoming data by comparing different areas and timeframes of the data. On the other hand, a multi-class data set has been used in ActiVis [KAKC18]. This visualization tool integrates coordinated multiple views, such as a graph that provides an overview of the model architecture, and a neuron activation view for exploring DNN models with user-defined subsets of instances. To wrap up the decisions made based on the provided views, agreement of colleagues could further enhance the trust in these complex DNNs. Many approaches exist for regression problems, such as those described in the publications of Fernstad et al. [FSJ13] and Hohman et al. [HSD19]. For instance, Piringer et al. [PBK10] describe a validation framework for regression models that enable users to compare models and analyze regions with poor predictive performances. The optimization of the so-called trade-off of bias and variance is also crucial for regression problems.

Papers categorized as others on the target variable group concern ML settings in which no target variable is available. These are mostly related to DR and clustering problems. The method designed by Zhou et al. [ZLH∗16], for example, combines both aspects to enable users to design new dimensions from data projections of subspaces, with the goal of maintaining important cluster information. The newly adapted dimensions are included in the analysis together with the original ones, to help users in forming target-oriented subspaces that explain—as much as possible—cluster structures.

6.2. Machine Learning

This subsection covers various ML methods that were divided into three main classes: DL, DR, and ensemble learning. We also discuss different ML types that we considered in our categorization: supervised learning, unsupervised learning, semi-supervised learning, and reinforcement learning.

6.2.1. Machine Learning Methods

In the area of DL, we observed two categories that are in the focus of most DL-related papers: CNNs and RNNs. CNNComparator [ZHP∗17] addresses the challenges of comparing CNNs and enables users to freeze the tool for different epochs of a trained CNN model (by using so-called snapshots). An epoch is completed when a data set is processed one time forward and backward through an NN. Thus, CNNComparator provides insights into the architectural design, and as a consequence, it enables better training of CNN models. For RNNs, RNNbow [CPM∗18] visualizes the gradient flow while backpropagation occurs in the training of RNNs. By visualizing the gradient, this tool offers insights into how exactly the network is learning. Both papers explicitly enhance trust in different DL models by either comparing CNNs or explaining RNNs to the users via visualization. In the DR subclass, linear techniques surpass non-linear ones in volume (the former was found in 57 papers vs. 51 for the latter). One example here is the iPCA tool [JZF∗09]. It augments the principal component analysis (PCA) algorithm with an interactive visualization system that supports the investigation of relationships between the data and the computed eigenspace. Overall, the tool employs views for exploring the data, the projections, the PCA’s eigenvectors, and the correlations between them. Eventually, prominent uncertainties become aware to users by examining all these relations. In another example, AxiSketcher [KKW∗17] enables users to impose their domain knowledge on a visualization by allowing interaction using a direct-manipulation technique over a t-SNE projection (non-linear DR technique). Users can sketch lines over specific data points, and the system composes new axes that represent a non-linear and weighted mixture of multidimensional attributes. Thus, the comparison of clusters enables users to identify problematic cases (in terms of trust) in a projection. For ensemble learning, bagging is the most common category. iForest [ZWLC19] is a visualization tool that accommodates users with an aggregated view showing and summarizing the decision paths in random forests, which finally reveals the working mechanism of the ML model. Visualizing and understanding the decision paths of random forest algorithms, as well as how their performance was reached, serves as a foundation for assessing the trust in bagging ensemble learning. Other,
more general examples can be found in the works by Schneider et al. [SJS*18] and Sehgal et al. [SRG*18].

6.2.2. Machine Learning Types

According to our analysis, supervised learning and classification problems are extensively addressed by the visualization community. For instance, a visualization system that works with choosing the best classifiers is EnsembleMatrix [TLKT09]. It allows users to directly interact with the visualizations in order to explore and build combinations of models. Comparison of ML models and validation metrics are key factors in increasing trust in them. HyperMoVal [PBK10], already discussed in Section 6.1.2, focuses on regression problems and provides several functionalities: comparing the ground truth against predicted results, analyzing areas with a poor fit, evaluating the physical plausibility of models, and comparing various classifiers. When users address regression problems, the comparison of alternative ML models and steering each of them can also improve the trustworthiness of the models. In unsupervised learning, a clustering example is the visualization technique developed by Turkay et al. [TPRH11], which visualizes the structural quality of several temporal clusters at a certain point in time or over time. DimStiller [IMI*10] is a system (belonging to the DR subclass) that assists the user in converting the input dimensions in a number of analytical steps into data tables that can be transformed into each other with the help of so-called operators. Users can manipulate those operators for parameter tuning and for guidance to discover patterns in the local neighborhood of the data space. Both DR and clustering visualization tools often utilize comparison of structures and emphasize patterns observable in projections. Some rare cases are related to semi-supervised learning, such as MacInnes et al. [MSW10] and Bernard et al. [BZL*18]. Reinforcement learning is covered by the work of Saldanha et al. [SPBA19], for instance.

6.3. Machine Learning Processing Phase

VASSL [KKZE20] is a system that works with the pre-processing/input phase and enhances the performance and scalability of the manual labeling process by providing multiple coordinated views and utilizing DR, sentiment analysis, and topic modeling. The system allows users to select and further investigate batches of accounts, which supports the discovery of spambot cases that may not be detected when checked independently. For the in-processing/model phase, Liu et al. [LSL*17] designed a tool that helps to better understand, diagnose, and steer deep CNNs. They represent a deep CNN as a directed acyclic graph, and based on this representation, a hybrid visualization has been developed to disclose multiple aspects of each neuron and the intercommunications between them. The largest category with regard to the number of available visualizations is post-processing/output for visualizing the final results, such as MultiClusterTree [VL09]. In their tool, the authors propose a 2D radial layout that supports an inherent understanding of the distribution arrangement of a multidimensional multivariate data set. Unique clusters can be explored interactively by using parallel coordinates when being selected in a cluster tree representation. The overall cluster distribution can be explored, and better understanding of the relations between clusters and the initial attributes is supported as well. As expected, the input phase is highly related to TL2, the in-processing phase to understanding and steering categories of TL3, and the final phase to metrics validation (TL5). Finally, Gil et al. [GHG*19] and Sacha et al. with VIS4ML [SKKC19] are two workflow papers that provide an overview of all these phases.

6.4. Treatment Method

Model-agnostic techniques are twice as common as model-specific techniques. With the former, we mean—in most of the cases—visualization methods that treat ML models as black boxes. The latter is usually connected to techniques specifically developed to open these black boxes, and thus make the ML models to be regarded as white boxes. An example of a model-agnostic visualization tool is ATMSear [WMJ*19] with which users are able to steer the search space of AutoML and explain the results. A multi-granular visualization empowers users to observe the AutoML process, examine the explored ML models, and refine the search space in realtime. In the white box case, the visualization tool EasySVM [MCM*17] facilitates users in tuning parameters, managing the training data, and extracting rules as a component of the support vector machine (SVM) training process. The goal of model-specific techniques is to explain the inner workings of a particular ML model. However, some tools combine both specific models and model-agnostic algorithms, such as Chae et al. [CGR*17], Roesch and Günther [RG19], Pezzotti et al. [PHV*18], and others [CWGW19, KKB19, MCMT14].

6.5. Visualization

Various approaches, types, and properties of visualization are used in our 200 surveyed papers, often in combinations. The knowledge of the most common techniques and approaches can guide early-stage researches to choose the most important of them or senior researchers to discover potential gaps in the literature. The selection of the best visualization approaches, types, and properties for a given situation can effectively reduce potential visualization bias. Successfully addressing questions such as “where, when, and why should I use a 2D bar chart to present aggregated information instead of another visual representation?”.

6.5.1. Dimensionality

With regard to dimensionality of the visual display, almost all visualizations (196) are 2D, such as [dBD*12, JJ09, MXC*20, SDMT16]. An exception is the interactive visualization technique by Coimbra et al. [CMN*16] that adapts and improves biplots to show the data attributes in the projected three-dimensional (3D) space. They use interactive bar chart legends to present variables that are visible from a given angle and also support users to decide on the optimal position to examine a desired set of attributes.

6.5.2. Visual Aspects

The information to be visualized can either be directly mapped from the data values themselves or be computed (algorithmically...
derived). ModelTracker [ACD*15] extracts information contained in conventional summary statistics and charts while letting users examine errors and diagnose ML models. Hence, it contains computed instead of mapped instances. Arendt et al. [ASW*19] visualize the classifier’s feedback after each iteration with their IML interface. To address scalability issues of the visualization, this interface communicates with the user by a small set of system-proposed instances for each class.

6.5.3. Visual Granularity

Görtler et al. [GSS*20] represent aggregated information in their visualizations. They use a technique that performs DR on data that is subject to uncertainty by using a generalization of standard PCA. Their technique helps to discover high-dimensional characteristics of probability distributions and also supports sensitivity analysis on the uncertainty in the data. Zeiler and Fergus [ZF14] introduce a visualization technique that contributes to insight generation for the general operation of the classifier in an instance-based manner, i.e., for individual data cases. Nevertheless, most visualization systems and techniques involve both the exploration of aggregated information and individual cases, e.g., presented by Choo et al. [CLKP10] and the visualization tool BaobabView [vv11].

6.5.4. Visual Representation

Liu et al. [LXL*18] combine multiple coordinated views to provide a thorough overview of a tree boosting model and enable the effective debugging of a failed training process. One of their views utilizes bar charts in order to rank the most valuable features that affect the model’s performance. Ji et al. [JSR*19] propose visual exploration of a neural document embedding with the goal to gain insights into the underlying embedding space and encourage this utilization in standard infrared (IR) spectroscopy applications. In their paper, they use a scatterplot visualization, i.e., a projection. LSAView [CDS09] is a system for interactive, latent semantic analysis (LSA) models. Multiple views, linked matrix-graph views, and data views in the form of lists are used to choose parameters and see the effects of them. Other papers apply different visual representations, some rare cases are waterfall charts, violin charts, Voronoi diagrams, and bipartite graphs [Aup07, HSD19, KKZE20, LA11, LGG*18, WGSY19, WGY18, ZTR16].

6.5.5. Interaction Technique

Gehrmann et al. [GSK*20] argue that both the visual interface and model architecture of DL systems need to consider the interaction design. They propose a collaborative semantic inference for the constructive cooperation between humans and algorithms. Semantic interactions permit a user both to understand and regulate parts of a model’s reasoning process. All these interactions enable the selection of particular sentences and then further exploration of the content with suggestions stemming from the system side. Abstract/elaborate is another interaction technique found in, e.g., Borland et al. [BWZ*20] and can be interpreted as different granularities that the visualization allows users to explore the data. Sevastjanova et al. [SBE*18] argue that a combination of visualization and verbalization methods is advantageous for generating wide and versatile insights into the structure and decision-making processes of ML models. For more details about the remaining interaction techniques (e.g., [CD18a, CBB*19, CLKP10, PSMD14, PLHL19, ZWC*18]), we refer to the survey of Lu et al. [LGH*17].

6.5.6. Visual Variable

Ahmed et al. [AYMW11] use a qualitative color scheme in order to encode cluster groupings in all views of their visualization tool for steering mixed-dimensional KD-KMeans clustering. Color is used in almost every paper we examined [CSG*18, EASKC18, KS12, ML14, PSF17, XCH*16]. DeepCompare [MMD*19] uses opacity and size, which are the two second-most occurring visual variables. Their tool visualizes the results of DL models, provides insights into the model behavior and the assessment of trade-offs between two such models. In more detail, the activation value of an NN is encoded as size, while opacity is used to remove the highlighting when specific cases are selected.

6.6. Evaluation

In this subsection, we explore how visualizations are evaluated in our community and how many of them had been actually evaluated. Surprisingly, around half of the visualizations were never evaluated. The evaluation of visualizations is a fundamental component to validate the usability of visualization tools and systems.

6.6.1. User Study

RuleMatrix [MQB19] is one of the approaches that follows a standard procedure for performing an evaluation in the InfoVis community. That is, various participants had to solve a series of tasks by using the tool during which the accuracy and timing was monitored to gain insight into the usability of the proposed solution. The paper presents an interactive visualization technique to assist novice users of ML to understand, examine, and verify the performance of predictive models. FairSight [AL20] is another tool designed to accomplish different concepts of fairness in ranking decisions. To achieve that, FairSight distinguishes the required actions (understanding, computing, and others) that can possibly lead to fairer decision making. It was compared against the What-If Tool [WPB*20] and found to perform better and result in more benefits than the latter approach.

6.6.2. User Feedback

Cashman et al. [CHH*19] worked with exploratory model analysis, which is defined as the process of finding and picking relevant models that can be used to create predictions on a data source. During development, they improved their tool and received user feedback. Hazarika et al. [HLW*20] used networks as surrogate models for visual analysis, and after the development of their system and techniques, a domain expert gave them feedback in order to further improve the VA system at the end of the development process. Ultimately, from the further analysis of the statistics, we conclude that in five cases both domain and ML experts used visualization tools and evaluated them. In 32 cases, e.g., [CS14, KCK*19, LLL*19, MvW11, XYC*18], only domain experts were asked; and in 19 cases only ML experts participated, such as in [LSC*18, NHP*18].
6.6.3. Not Evaluated

As described earlier, approximately half of the papers did not include any type of evaluation. However, we discovered one visualization tool [KTC+19] that was evaluated later in a new publication [KC19].

6.7. Trust Levels

The most novel components of the categorization presented in this section are the different levels of trust we identified in the 200 individual papers. In Section 2, we divided the enhancement of trust in ML models with the help of visualizations into five levels (raw and processed data, learning method, concrete model, and user expectation).

6.7.1. Raw Data (TL1)

Source reliability often comes together with transparent collection processes as in AnchorViz [CSV+18], an interactive visualization that facilitates erroneous regions detection through semantic data exploration. By pinning anchors on top of the visualization, users create a topology to lie upon data instances based on their relation to those nearby anchors. Examination of discrepancies between semantically related data points is another functionality of the tool. This data exploration helps to observe source reliability and if any strange effects occurred when the collection process happened. However, as can be seen from the data in Table 3, these two categories are covered rarely by visualization tools.

6.7.2. Processed Data (TL2)

Uncertainty awareness and investigation is an established subject of research in the visualization community with techniques such as the one presented by Berger et al. [BPFG11]. The authors developed techniques that guide the user to potentially interesting parameter areas and visualize the intrinsic uncertainty of predictions in 2D scatterplots and parallel coordinates. FairVis [CEH+19] is a recent paper that addresses a new problem which seems to become a trend. Data bias and equality is a major issue and should be—as much as possible—removed from our ML models. FairVis facilitates users to review the fairness of ML models in interesting, explored subgroups. iVisClustering [LKC+12] is one of the many visualization tools that allow the comparison of different structures (clusters in this case) and guide/recommend the users by proposing new clusters based on previous actions. With the help of such visualizations, users can interactively refine clustering results in various ways. Also, iVisClustering can fade away noisy data and re-cluster the data accordingly to demonstrate a meaning representation. Zhao et al. [ZCW+19] developed a tool that enables users to recognize, explain, and choose outliers discovered by various algorithms. Roughly one third of the papers cover outlier detection related topics (68 out of 200), such as [LWT+15, RFFT17, SKB+18].

6.7.3. Learning Method (TL3)

The work of Olah et al. [OSJ+18] tries to familiarize users with different DL algorithms. They test robust interfaces that appear when users appropriately combine them and the rich composition of this combinatorial solution space. In our STAR, interpretability and explainability is separated into four categories: understanding/explanation, debugging/diagnosis, refinement/steering, and comparison. These categories may even occur in pairs or triplets, depending on the visualization system and technique. For instance, Liu et al. [LLS+18] support understanding/explanation of the reasons behind faulty predictions introduced by adversarial attack examples. The basic concept is to analyze groups of critical neurons and their connections of the adversarial attacks and match them with those of the normal cases. DeepTracker [LCJ+18] facilitates the exploration of the intense dynamics of CNN training processes and helps to identify the unique patterns that are “buried” inside the enormous amount of information in a training log (debugging process). Hamid et al. [HDK+19] describe a visual ensemble analysis based on hyper-parameter space and performance visualizations. These visualizations are mutually used with associations’ explorations between topological arrangements and allow the production of enough knowledge in order to support users steering the process. Rieck and Leitte [RL15a] suggest a comparative analysis of DR methods according to what level of preservation of structural features in the high-dimensional space remains in the 2D embeddings. Local and global structural features are assessed in the original space, and specific DR methods are chosen based on those findings. Manifold [ZWM+19] is conceived of a generic framework that does not rely on the internals of particular ML models and only observes the input and the output. With the comparison of various models and learning methods, it allows users to become knowledgeable about their usability. FairSight [AL20] which was discussed earlier along with the What-If Tool [WPB+20] are both two recent examples of how fairness is a trending unexplored subject in the community. The What-If Tool (which was not discussed yet) enables domain experts to assess the performance of models in hypothetical scenarios, analyze the significance of several data features, and visualize model functionality across many ML models and batches of input data. It also engages practitioners in grading systems that are able to show multiple ML fairness validation metrics.

6.7.4. Concrete Model (TL4)

Cashman et al. [CPCS20] researched the rapid exploration of model architectures and parameters. To this end, they developed a VA tool that allows a model developer to discover a DL model immediately via exploration as well as rapid deployment and examination of NN architectures. By visually comparing models, beginners might come to similar conclusions (e.g., that early stages of convolutional layers perform well in feature extraction) as ML experts who take advantage of their experience. In situ comparison, i.e., a comparison of two or more states of the same model, is performed by Gamut [HHC+19], for example. The benefit of Gamut lies in the justification of why and how professional data scientists interpret models and what they look for when comparing their internal components. Our investigation showed that interpretability is not a monolithic concept: data scientists have different reasons to interpret models and tailor explanations for specific audiences, often balancing competing concerns of simplicity and completeness. Moreover, performance is one of the most common techniques to choose from (see Table 3) when having different models. LoVis [ZWRH14] allows the user to progressively
construct and validate models that promote local pattern discovery and summarization based on “complementarity”, “diversity”, and “representativeness” of models. What-if hypotheses are supported by Clustrophile 2 [CD19], which guides users in a clustering-based exploratory analysis. It also adapts incoming user feedback to improve user recommendations, helps the interpretation of clusters, and supports the rationalization of differences between clusterings. Last but not least, papers that deal with issues related to model bias and model variance usually occur together. Mühlbacher and Piringer [MP13] present a framework for building regression models addressing these limitations. Analyzing prediction bias with model residuals is one of the techniques used to limit the local prediction bias of a model, i.e., avoiding the inclination towards underestimation or overestimation. They also visualize the point-wise variance of the predictions by using a pixel-based view.

6.7.5. Evaluation/User Expectation (TL5)

The Agreement of colleagues is related to provenance and the possibility to enable users to collaborate with each other. Wongsuphasawat et al. [WSW18] present a design study of the TensorFlow Graph Visualizer, which is a module of the shareable TensorFlow platform. This tool improves users’ understanding of complicated ML architectures by visualizing data-flow graphs. These flows can be investigated, and at each point in time, provenance can be considered as a way to return back to a previous situation. Visualization evaluation, as mentioned earlier in Sect. 6.6, is activated when the visualization techniques and tools are evaluated or if any type of feedback is provided. Showing metrics validation/results is the most common way of enhancing trust until now. Squares [RAL*17] is a performance visualization for multi-class classification problems. Squares supports estimating standard performance metrics while demonstrating instance-based distribution information essential for supporting domain experts in prioritizing efforts. Furthermore, Fujiwara et al. [FKM20] implemented a VA method that highlights the crucial dimensions of a cluster in a DR result. To obtain the important dimensions, they introduce an improved method of contrastive PCA. The method utilized is called ccPCA (contrast clustering in PCA) and can compute each dimension’s relevant contribution to one versus other clusters. An example that implicitly checks user bias is the explAIner tool by Spinner et al. [SSSEA20]. explAIner is a VA system based on a framework that connects an iterative explainable ML pipeline with 8 global observing and refinement mechanisms, including “quality monitoring”, “provenance tracking”, or “trust building”. Additionally, Jenner et al. [JS*18] propose the metaphorical narrative methodology to translate mental models of the involved modeling and domain experts to machine commands and vice versa. The authors provide a human-machine interface and discuss crucial features, characteristics, and pitfalls of their approach. With regard to user bias, the research community has taken “small steps” with only a few papers tackling this issue. However, explicit reports about this challenge are still rare, unfortunately.

6.8. Target Group

In most cases, the visualization tools cover at least the target group of domain experts/practitioners [EGG*12, FMH16, FCS*20, GNRM08, HNH*12, KPN16]. Then, other target groups such as ML experts [JC17b, KJR*18, SSK10, WLN*17] and developers are in the focus of the authors [KFC16, Mad19, RL15b, YZR*18] (commonly together). Beginners/h novice users [JS019, MXQR19, SRM*15, TLRB18] are rarely considered. To give two examples, Bögl et al. [BAF*14] support with TiMoVA-Predict several types of predictions with a holistic VA approach that focuses on domain experts. Providing different prediction capabilities allows for assessing the predictions during the model selection process via an interactive visual environment. Biologists and doctors, for instance, are interested in being able to compare data structures and receive guidance on where to focus on. Ma et al. [MXLM20] employ a multi-faceted visualization schema intended to aid the analysis of ML experts for the domain of adversarial attacks.

7. Survey Data Analysis

In the previous parts of our report, we explained our overall methodology, provided high-level statistical information on the selected papers, and introduced our categorization together with example papers assigned to the individual categories. Now in this section, we discuss lower-level analytical results based on the collected papers and their metadata. In order to detect interesting connections and important emerging topics among the 200 papers, we applied topic modeling to all of them, following the visual text analysis approach by Kucher et al. [KMK18]. While the topic modeling results might be subject to the algorithm and parameter choice concerns to some extent, they provide information complementary to the results of our manual investigations. Thus, the topic analysis contributes both to the validation and the new insights regarding the categorized publications. In addition, we investigate the relations between categories in general (again following the workflow proposed by Kucher et al. [KPK18]) and explore the different data sets used in the individual papers. All those analyses help us to validate and further explore our categorization by creating new insights that can be used as research opportunities for this subject (cf. Section 8).

7.1. Topic Analysis

Methodology. First, we collected the PDF files of the selected papers and converted them to plain text. After that step, we prepared the text corpus by clearing the full texts from the authorship details and acknowledgments. Next, we processed them with the latent Dirichlet allocation (LDA) algorithm [BJN03, GS04] (a common approach for topic modeling). In order to verify the LDA results—because it might produce diverse results at different executions—we ran the same process several times to get comparable results. The results do not indicate a major deviation from the main topic of each paper previously assigned by the manual categorization process. Finally, our LDA results led to ten topics (limited by the lack of space and our attempt to choose a reasonable number of topics). The top eight terms for each topic are displayed in Table 4 together with the papers belonging to a topic (see S6 for further details). From the terms that occurred, we removed any terms related to the structure of the analyzed texts and not to the actual content, for instance, “figure” and “fig”. Our implementation is based on Python with NLTK [Bir06] for the pre-processing
Table 4: For each of the ten topics, we present the top eight terms that we extracted from the results of the latent Dirichlet allocation (LDA) that has been applied to all papers. The suggested topic titles are shown in italics. Each topic is encoded by one specific color. In each topic, we cite the papers that mostly belong to them.

<table>
<thead>
<tr>
<th>Topic 1</th>
<th>NNs hidden states and models' parameter spaces visualization (in time series applications)</th>
</tr>
</thead>
<tbody>
<tr>
<td>keywords</td>
<td>papers</td>
</tr>
<tr>
<td>model</td>
<td>13 papers</td>
</tr>
<tr>
<td>view</td>
<td>3 papers</td>
</tr>
<tr>
<td>tree</td>
<td>3 papers</td>
</tr>
<tr>
<td>state</td>
<td>13 papers</td>
</tr>
<tr>
<td>hidden</td>
<td>3 papers</td>
</tr>
<tr>
<td>hidden state</td>
<td>13 papers</td>
</tr>
<tr>
<td>time parameter</td>
<td>3 papers</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Topic 2</th>
<th>Network visualizations to investigate the behavior of projections and explore classes (for topic analysis)</th>
</tr>
</thead>
<tbody>
<tr>
<td>keywords</td>
<td>papers</td>
</tr>
<tr>
<td>topic</td>
<td>9 papers</td>
</tr>
<tr>
<td>node</td>
<td>5 papers</td>
</tr>
<tr>
<td>network</td>
<td>5 papers</td>
</tr>
<tr>
<td>projection</td>
<td>5 papers</td>
</tr>
<tr>
<td>behavior</td>
<td>5 papers</td>
</tr>
<tr>
<td>class</td>
<td>5 papers</td>
</tr>
<tr>
<td>edge</td>
<td>5 papers</td>
</tr>
<tr>
<td>tree</td>
<td>5 papers</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Topic 3</th>
<th>NNs models' hyper-parameters and reward visualization during training for image applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>keywords</td>
<td>papers</td>
</tr>
<tr>
<td>image</td>
<td>7 papers</td>
</tr>
<tr>
<td>model training</td>
<td>7 papers</td>
</tr>
<tr>
<td>input network</td>
<td>7 papers</td>
</tr>
<tr>
<td>hyper parameter</td>
<td>7 papers</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Topic 4</th>
<th>Vector space, samples, and distributions visualization in projections and DR</th>
</tr>
</thead>
<tbody>
<tr>
<td>keywords</td>
<td>papers</td>
</tr>
<tr>
<td>projection dimension</td>
<td>4 papers</td>
</tr>
<tr>
<td>view</td>
<td>4 papers</td>
</tr>
<tr>
<td>sample</td>
<td>4 papers</td>
</tr>
<tr>
<td>vector space</td>
<td>4 papers</td>
</tr>
<tr>
<td>point distribution</td>
<td>4 papers</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Topic 5</th>
<th>Models' predictions visualization in clustering (for text applications)</th>
</tr>
</thead>
<tbody>
<tr>
<td>keywords</td>
<td>papers</td>
</tr>
<tr>
<td>model cluster</td>
<td>5 papers</td>
</tr>
<tr>
<td>clustering value</td>
<td>5 papers</td>
</tr>
<tr>
<td>view</td>
<td>5 papers</td>
</tr>
<tr>
<td>prediction document variable</td>
<td>5 papers</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Topic 6</th>
<th>ML models' explanations and visualization systems evaluation</th>
</tr>
</thead>
<tbody>
<tr>
<td>keywords</td>
<td>papers</td>
</tr>
<tr>
<td>model learning system machine</td>
<td>1 papers</td>
</tr>
<tr>
<td>participant explanation instance</td>
<td>1 papers</td>
</tr>
<tr>
<td>machine learning</td>
<td>1 papers</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Topic 7</th>
<th>Subspaces exploration and distances examination in clustering and DR</th>
</tr>
</thead>
<tbody>
<tr>
<td>keywords</td>
<td>papers</td>
</tr>
<tr>
<td>model prediction instance view prototype algorithm</td>
<td>3 papers</td>
</tr>
<tr>
<td>learning design</td>
<td>3 papers</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Topic 8</th>
<th>Models' predictions and design prototyping in ML algorithms</th>
</tr>
</thead>
<tbody>
<tr>
<td>keywords</td>
<td>papers</td>
</tr>
<tr>
<td>point class projection space view instance value outlier</td>
<td>3 papers</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Topic 9</th>
<th>Individual points, projection space, and outliers' exploration</th>
</tr>
</thead>
<tbody>
<tr>
<td>keywords</td>
<td>papers</td>
</tr>
<tr>
<td>layer network neuron model training activation class image</td>
<td>3 papers</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Topic 10</th>
<th>NNs neurons' activations visualization during training for image applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>keywords</td>
<td>papers</td>
</tr>
<tr>
<td>layer network neuron model training activation class image</td>
<td>3 papers</td>
</tr>
</tbody>
</table>

of stop words and Gensim [RJS10] for the topic modeling part. The names of the topics were manually assigned by us after several discussion cycles considering both the top terms and the contents of the papers in each topic. The results are then visualized with the assistance from the interactive visualization tool described by Kucher et al. [KMK18], see Figure 5. This visualization is based on a DR projection which may not be the most reliable approach. However, the ground truth labels taken from the LDA results match in almost all the cases with the clusters formed by the embedding.

**Topics.** In the following description list, we shortly summarize the ten topics (see Table 4) we identified:

- **Topic 1 – hidden states & parameter spaces.** According to our analysis, the common factor between the majority of the 13 papers in this topic is their focus on time series data [BAF+14, BAF+15] and RNNs [SBP19] (in Strobelt et al. [SGPR18]: long short-term memory networks). It seems that the exploration of the hidden states of such networks preserves lost information that could enhance trust [MCZ+17] with appropriate expert intervention. Another subtopic here is the ML models’ parameter spaces exploration [TCE+19], which enables users to find the best parameters based on a series of optimizations for certain goals. In this context, Mühlbacher et al. [MLMP18] present an approach that visualizes the effects of these parameters. As stated by these previous works, support for the visual parameter search is still an open research challenge.

- **Topic 2 – investigation of the behavior.** This topic class contains 2 out of 9 papers on topic analysis applications [CAA+19, KKZE20]. A common theme here is network visualization used for explaining Bayesian networks [CWS+17, VKA+18] and decision trees [vv11]. Other subtopics (which lead to research opportunities) are the exploration of behavior with regard to the decomposition of projections, showing the internal parts of ML models (and how classes are formed inside them), and the role of the user; they are all covered by our categorization presented in Section 6.

- **Topic 3 – hyper-parameters & reward.** All five papers in this class (except one [SPBA19] related to reinforcement learning) make use of image data. They form a tight, green cluster in Figure 5 and focus mainly on DL techniques [YCN+15]. It is an open challenge to decide which hyper-parameter value [SSS+18, WGZ+19] is better for a particular NN and specific problem, thus implying novel visualization techniques. For reinforcement learning, instead, more research is needed for studying what behaviors are associated with the two types of reward (high and low) and monitoring how they develop during training.

- **Topic 4 – vector space, samples, & distributions.** In this topic, class three papers [LBT+18, LIJH19, SZL+18] work with vector space embeddings that illustrate similarities of the data. Most of the 15 papers highlight the importance of visualizing instances and samples [KTC+19, SDMT16] that form clusters in projections and explore the distributions [AHH+14, CCZ+16, CD18b] of points in DR techniques.
Finding ways to improve these visualizations is still an open challenge in the InfoVis community.

**Topic 5 – models’ predictions.** Models’ predictions and results visualization with the use of quality and validation metrics [FSJ13, GS14] (depending on the ML type) composes a big, more general topic class with 32 surveyed papers. A subgroup in this class especially refers to clustering challenges [BDSF17, KEV*18] and open research questions such as: “do we have the best clustering that could be achieved and if not, how can we improve it?” (usually related to text applications) [CDS09].

**Topic 6 – models’ explanations & visualization evaluation.** This topic is rather generic (with 39 papers allocated) as it addresses the understanding/explanation of ML models [GHG*19, TKDB17]. For many visualization tools belonging to this topic class, we can observe that user studies (i.e., evaluations) [BAL*15, BEFI17, GSC16, KLTH10, SLT17, ZYB*16] have been performed with participants from different educational levels (novices, practitioners, ML experts, and so on). Following the overall theme of this STAR, a straightforward unsolved problem in this area is to find answers to how exactly we shall progress with the development of visualization tools for boosting the trust in ML models and their results.

**Topic 7 – subspaces exploration & distances examination.** Clustering and DR are both covered together when exploring subspaces [BAPB*16, KDFB16, LMZ*14]. Finding the correct distance function, checking if these distances are preserved after the projection from the high-dimensional space into the 2D space, and matching the users’ cognitive expectations is clearly
not a trivial task. As a result, many papers are published in this area [AEM11, BLBC12, JHB+17, WLS19], making this topic class with 30 papers one of the most prominent in our analysis.

**Topic 8 – models’ predictions & design prototyping.**

Another generic topic class with 18 related papers contains, among others, the subject of ML models’ predictions [SJS+17, XMM+19] that has already been seen in Topic 5. The difference between this class and Topic 5 is the focus of its related papers, which is on the instantiation of visualization prototypes with different design choices that should be carefully considered based on previous InfoVis research. As such, updating the current methods with improved versions can lead to enhanced trust of visualizations and reduce biases [GDM+19, LGG+18, SGB+19].

**Topic 9 – points, projection space, & outliers’ exploration.**

With 68 papers in total, the area of outlier detection is prominent in our categorization, see Table 3. This category is even confirmed through the topic analysis (with 19 papers assigned) as many techniques work with outlier detection [BHR+19, JPN15, RSF+15]. Another hot topic in the visualization community is the visual analysis of relations between points and dimensions within the various projection spaces [Aup07, CMN+16].

**Topic 10 – neurons’ activations.**

When visualizing DL techniques, the existing research has tried to address the activation of neurons in NN and their visual representation [HDK+19, HLW+20, HPRC20]. Different visualization techniques (e.g., 2D saliency/activation maps) have been used to visualize the activations of such neurons in various DL models, especially for image applications [AJY+18]. This topic class consists of 20 papers about visualizing the internal operations of NNs during the training phase. A possible research question in this context is: “what else can be visualized (for instance, gradients [CPM+18]) that gives meaning to humans about the learning process of a NN?”

**Topic embedding.**

The ten-dimensional data space of the topics over all 200 papers has been reduced to two dimensions by using t-SNE [vdMH08], i.e., two papers are positioned close to each other if their topic relationships are alike, see Figure 5(a). The scales in the depicted bar charts are from 0 to 1, with 1 being the highest relevancy value of a topic in Figure 5(b) and of a term in Figure 5(c). The black outlines in the 2D embedding (see Figure 5(a)) were appended manually.

As it can be derived from Figure 5(b), Topics 6 & 7 are the most prominent ones, followed by Topics 5 & 9, 8 & 10, and the others. In more detail, ML models’ explanation and visualization systems evaluation (Topic 6) and subspaces exploration and distances examination in clustering and DR (Topic 7) are two discussed topics that cover approximately 35% of all papers. With regard to Figure 5(c), some interesting top terms are—as expected—“models” (ML), “image data” (computer vision, see even Table 5), “layers” (DL), “clusters”, “topic” (analysis), “subspace”, “projections”, and “dimensions” (DR). By observing the t-SNE projection in Figure 5(a), we can find more interesting insights. For instance, the tightest cluster is color-encoded in green and related to NNs models’ hyper-parameters and reward visualization during training for image applications (Topic 3). Another interesting result is that the misclassification of orange (Topic 2) & pink (Topic 7) points as well as of pink (Topic 7) & red (Topic 4) points in the embedding happens due to three concept terms that are spread in all three topics, namely, the terms “clustering”, “dimension”, and “projections”. Furthermore, as Topic 6 is rather generic (ML models’ explanations), there are some points laid out in-between (i.e., mixed points) with Topics 1 (DL) & 9 (projections). Lastly, Topic 8 (models’ predictions & design prototyping) is also rather general, because the points in the projection are spread through two other topics (5 & 10); and this is probably because NNs are a subclass of ML models and Topic 5 (models’ predictions) is very similar to Topic 8.

Overall, we notice that the automatically generated topics introduce new subcategories (and ideas) that have been discussed in parallel to our categorization and—in consequence—supported even more the categorization of the papers described in the previous section. For instance, Topics 1 and 10 represent VA tools focusing on the visualization of the NNs hidden states and neurons’ activations respectively to facilitate the understanding/explanation of them. In addition, Topic 1 covers examples for the comparison of models based on the visualization of their parameter spaces. Similarly, Topic 2 is related to the in situ comparison of concrete models to investigate different behaviors of the ML models. Topic 3, instead, focuses more on diagnosing/debugging the training process for reinforcement learning, and Topic 4 reflects the comparison of data structures with the use of projections and DR. The remaining topics are explicitly connected to our TL categorization within the corresponding topic list items above. We believe that this mixture of coarse-grained manual categorization with a fine-grained automatic refinement may help guiding potential readers to more insights and analyze the surveyed papers even further.

### 7.2. Correlation and Summarization of Categories

**Correlation between categories.**

We have conducted a correlation analysis for the categories used in our collected survey data set. Individual visualization papers were treated as observations, and categories (cf. Table 3 and S5) were treated as dimensions/variables. Linear correlation analysis was then used to measure the association between pairs of categories. The resulting matrix in Figure 6 contains Pearson’s r coefficient values and reveals specific patterns and intriguing cases of positive (green) and negative (red) correlation between categories. Since the interpretation of the coefficient values seems to differ in the literature [Coh88, Eva96, Tay90], we focus on values of correlations that appear interesting to us despite a potentially strong or weak correlation level. Due to the extensive size of the correlation matrix, we include only a thumbnail of it and refer the reader to S7 for more detail. In Figure 6, we present some strong, medium, and weak correlation cases that caught our attention.

The strongest case of negative correlation in our data set is the not evaluated category vs. user expectation for evaluation (cf. 6.6. and 6.7.5.), which clearly highlights the need for further evaluation of visualization tools and techniques. Further interesting cases mainly include competing categories from the same group. For example, model-agnostic techniques contradict model-specific techniques, because they consider different visualization granularities for a given ML model. 2D and 3D oppose each other as typically
Important Findings  Correlation

- Not evaluated vs. user expectation for vs. evaluation  -90%
- Model-agnostic vs. model-specific  -79%
- Boosting & stacking  +73%
- 2D vs. 3D  -90%
- Source rel & transp. col. process  +90%
- DQN & control (reinforcement learning)  +57%
- DL models  +25% to +32%
- Model bias & model variance  +53%
- In-processing vs. post-processing  +33%
- DL & ensemble learning  +12% to +66%
- Mapped & instance-based  +48%
- Multi-class vs. other (target variable)  -48%
- Multi-class & computer vision  +37%
- Visualization interactions  -19% to +55%
- Developers & ML experts  +32%
- Source rel. & classification & transp. col. process  +28% to +32%
- Developers & ML experts vs. domain experts  -27% to -29%
- Developers & debugging  +27%
- ML experts & in-processing  +28%
- Continuous data & business  +28%
- Beginners & familiarity  +24%
- RNA & humanities  +23%
- Developers & comparison of models  +23%
- Domain experts & in-processing  -23%
- ML experts & matrix  +21%
- Domain experts & select  +20%
- Domain experts & tables / lists  +19%
- Linear DR & biology  +19%
- Domain experts & debugging  -19%
- Beginners & select  -17%
- ML experts & knowledgeability  +18%
- Beginners & ML experts & understanding  -14% to -17%

(a) Correlation matrix overview  (b) Table for showing important correlation findings

Figure 6: The matrix of correlation values for categories (see Table 3) calculated from our survey data set. In subfigure (a), we show the correlations for the categorization in a thumbnail version of the correlation matrix. The entire correlation matrix for further exploration can be found in S7. (b) To help the reader to see potentially interesting findings, we list the cases in decreasing order of their correlation strengths (independent of negative or positive correlation). In both subfigures, we use red color for negative correlation and green for positive. Cases highlighted in bold refer to groups of categories in general (e.g., visualization interactions).

only one of them exists in a visualization approach. Moreover, techniques that focus on data exploration, explanation, and manipulation related to the in-processing phases of an ML pipeline are very different compared to systems that monitor the results in the post-processing phase of an ML model. The strong negative correlation between multi-class and other target variables might point to an effect that comes from our own categorization procedure: when papers could not be mapped to a concrete target variable (multi-class, for instance), then the other category has been assigned, e.g., to show the irrelevance of the target variable for a visualization technique. The category domain experts is negatively correlated to managing models during the in-processing ML phase, which makes sense as they do often not know much about how models work. Similarly, developers and ML experts together are weakly but negatively correlated with domain experts confirming the previous acquisition. Other insights are that beginners are not usually using selection as interaction technique and domain experts do not work with diagnosing/debugging ML models as they do not have the experience and/or knowledge following the previous inference.

Cases with positive correlation start in Figure 6(b) with stacking which is highly correlated with boosting ensemble learning as the former sometimes includes the latter technique. All DL techniques among each other have on average a medium positive correlation, which shows that they have much more in common compared to other ML methods, for example, DR. The same is true for the group of visualization interactions to a slightly less extend. When source reliability is taken into account and researched by scientists, then the transparent collection process is usually examined together. Deep Q-networks (DQNs) are positively correlated to and seem to be normally used together with reinforcement learning methods, particularly with the subtype control. Furthermore, when model bias challenges are addressed by visualization, then model variance is another category that is addressed simultaneously. Ensemble learning along with DL are positively correlated, as the former includes the latter in many cases (a fact already mentioned before). Mapped instances lead to instance-based visualizations, in general. With regard to domains, continuous target variables and business are positively correlated (potentially due to trend predictions); as well as computer vision and multi-class data in an even stronger fashion. The latter correlation is also supported by our data set analysis (see Table 5). Finally, visualization interactions are positively correlated among each other, with the exception of verbalization which is negatively correlated with the remaining categories in this group. This possibly means that verbalization is not frequently used by the VA system developers. For more details, we refer the reader to Figure 6(b) and supplementary material S7.

Popular approaches. The statistics in Table 3 support our expectations of the most common aspects of existing visualization techniques for enhancing the trustworthy of ML models. For our first aspect (6.1. Data), computer vision, humanities, health, and biology seem the most prominent domains in the surveyed papers. Multi-class classification is the most common target variable in our discussed techniques. Furthermore (6.2. ML), linear and then non-linear DR techniques are commonly used, followed by bagging (ensemble learning) and CNNs from the DL class. The vast majority of the papers address supervised learning and specifically classification problems, and in second position DR and clustering which belong to unsupervised learning. (6.3. and 6.4.) Post-processing and model-agnostic visualization techniques cover around 75% of all papers. (6.5.) With regard to visual aspects and granularity, almost all techniques used have at least a component which is computed and not mapped/derived from the data directly, and aggregated information is slightly more common than instance-based/individual exploration of instances.

The absolute majority of the visualizations rely only on 2D representations, and color is the visual channel most commonly used for encoding information in the corresponding visualization systems, tools, and techniques. The rather large number of techniques using opacity to hide points/instances and size/area to encode data attributes can be explained by the extensive usage of scatterplots. Other popular visualizations are bar charts, custom glyphs and specialized icons, histograms, and finally, line charts. More traditional visual representations, such as tables, lists, and matrices, are working in pairs with instance-based exploration techniques, which are far less complicated than the previously mentioned visualizations. On the interaction side, selection, exploration, and abstraction/elaboration are the three most prominent categories found in many papers, followed by other interaction techniques, such as connecting all the different views, filtering out or search-
Figure 7: Sparkline representation of relative category popularity over time during 2007–2020. Each bar represents the support for a specific category (cf. Table 3) in relation to the total count of techniques in the same year in our data set.
ing for specific instances, and encoding. (6.6.) Around half of the visualization techniques that we analyzed have not been evaluated.

The trust levels (6.7.) show that more works tackle source reliability problems rather than the transparent collection process challenge (as seen in TL1). For the second level (TL2), researchers focus on the comparison of structures and outlier detection. In the third level (TL3), understanding, steering, comparing, and debugging ML methods are quite popular. These aforementioned categories can be considered under the umbrella of interpretable/explainable ML methods. For TL4, performance, in situ comparison, and what-if hypotheses are other very often occurring categories connected with the selection process of an individual ML model. Ultimately in TL5, metrics validation and results observation at the final stage of the processing phase is the most frequent category with 130 papers. Last but not least for TL6, the visualization systems and techniques have as a main target group, usually practitioners/domain experts, followed by ML experts with large distance. The analysis above sheds light into the reasons why a few approaches seem to be more popular than others. The ML side uses mostly performance, metrics validation, and results to monitor and boost trust in the ML models. In contrast, the visualization side focuses more on traditional visual representations and/or multivariate, scalable visualizations that the experts are more willing to use.

Temporal trends. While the analyses presented above focus on the overall statistics, we have also analyzed the temporal trends for individual categories based on the collected data. Figure 7 provides a sparkleline-style representation of the information about each category’s support (i.e., the count of corresponding techniques) over time. The values are normalized by the total count of techniques for each respective year between 2007 and 2020 (for example, 3 out of 9 papers from 2010 used computer vision data to demonstrate the usability of their tools). The resulting representation in Figure 7 allows us to confirm, for instance, that the ML processing phase visualized consistently most often is post-processing rather than in-processing or pre-processing. Combination of such temporal trends with the overall statistics also allows us to identify and further discuss the usage of currently underrepresented categories.

Underrepresented categories. Multi-label data and computer-related data (from software or hardware) are two underrepresented categories that show no trend for a potential increase according to Figure 7. For ML methods, approaches such as stacking ensemble learning, deep convolutional networks (DCNs), and DQNs are also not covered in detail. Nevertheless, there is a very small increasing trend for them observable in Figure 7. Explicit techniques addressing problems that come with stacking ensemble learning were not found in any paper, thus indicating a new research opportunity.

For ML types, the subcategory of solving classification problems while using reinforcement learning is almost never visualized and actually never addressed explicitly by the visualization community. Other underrepresented categories here are reinforcement learning and control, and association for unsupervised learning.

For the visual representation, the treemaps and icicle plots categories are virtually not supported by the data. Further techniques that belong to the last category within visual representation (“other”) and are fairly underrepresented are waterfall charts, bipartite visualizations, and lastly area charts (as also mentioned in Section 6). For the interaction techniques, the category of visualization emerged in 2010 and has not attracted much support in the publications; even though recently in 2018, Sevastjanova et al. [SBE+18] argued about the importance of its existence. Moreover, texture is the least usual way to represent the data visually in comparison to the others. Comparative evaluations are the rarest way of evaluating visualizations, which is rather logical because not every technique has an obvious opposing one.

The real challenges start when we check the trust levels aspect because many techniques are underrepresented, which means there are several research opportunities in the area. Transparent collection processes, source reliability, and equality/data bias are usually not covered by papers. Other problems, such as how visualization can assist with the familiarity a user has for a learning method, should also be in the research agenda of our community. Fairness (and previously mentioned equality for the data) of the learning methods seem to be in the spotlight according to the temporal statistics (see Figure 7). Finally, developers (i.e., model builders) and beginners are the two most underrepresented target groups in the papers we analyzed. Knowledgeability about learning methods and details available to different types of users is not well supported. As a result, customization and reconfiguration of visualizations that take into account the experience of users in order to choose a specific ML model are not researched to the required extent. Furthermore, a few techniques enable agreement of colleagues and study about the consequences of using provenance in visualization tools in order to cover our discussed subject. User bias is ignored in almost all of the visual systems.

All of the underrepresented categories discussed above might be candidates for open challenges, as can be seen in Section 8.2. From an ML perspective, the most real-world challenges are about either classification or regression problems. Consequently, other ML types are not researched to the same level. From the visualization perspective, a large amount of time and effort is necessary to design and perform a “proper” visualization evaluation [LTBS+18]. Moreover, as long as the visualization tools do not focus on beginners, familiarity with and knowledgeability of the algorithms are left aside by visualization researchers.

7.3. Data Set Analysis

Methodology. For the data set analysis, we consider only non-synthetic (i.e., not artificial) data sets which can be accessed online. We also include data sets that can be requested from the paper authors. For the individual data features, we take further into account the labels (i.e., classes), if they are existent. Overall, details about a data set were collected relying on the description provided by the authors of a paper, for example, how they collected and stored the data. In any other case, we omitted the data sets. All data sets are sorted first according to the number of occurrences in the 200 papers, and then by year to show the most recent first.

Results. The result of this process can be observed in Table 5. In the listed 38 cases, the data sets are used in at least two papers, and the remaining 106 entries are used once only (cf. S8). In total, we managed to identify 144 non-synthetic data sets in our
Table 5: Overview of data sets ordered according to their usage. A "#" in the columns indicates the number of papers in this survey using a particular data set; the data sets are then further grouped based on this number.

<table>
<thead>
<tr>
<th>Data Set</th>
<th>Year</th>
<th>Domain</th>
<th># Instances</th>
<th># Features</th>
<th>Target Variable</th>
<th># References</th>
</tr>
</thead>
<tbody>
<tr>
<td>MNIST [LBBH98]</td>
<td>1998</td>
<td>Computer Vision</td>
<td>70,000</td>
<td>784 (28x28)</td>
<td>Classification (10 classes)</td>
<td>[AMJ18, BZL<em>18, CHAS18, PKM20, HDK</em>19, JC17b, LSL<em>17, MXM02, PHL</em>19, PH<em>18, RAL</em>17, SLT<em>17, SSSE02, WGYS18, WGZ</em>19, XYC*18, CD18b]</td>
</tr>
<tr>
<td>Iris [And36]</td>
<td>1936</td>
<td>Biology</td>
<td>150</td>
<td>5</td>
<td>Classification (3 classes)</td>
<td>[BZL<em>18, GSS</em>20, CHAS18, JHB<em>17, JZJ</em>09, RL16, SDMT16, SML17, SNLH09, WLN<em>17, WLM18, FCS</em>20]</td>
</tr>
<tr>
<td>Wine Quality (red &amp; white) [CCA’09]</td>
<td>2009</td>
<td>Business &amp; Physicochemical</td>
<td>6,497</td>
<td>12</td>
<td>Classification &amp; Regression</td>
<td>[BLB12C, CMN<em>16, FPKZ16, HH19, JZJ</em>09, RL16, SDMT16, SML17, SNLH09, TLRB18, ZCW*19, SSM15]</td>
</tr>
<tr>
<td>ImageNet [DDS’09]</td>
<td>2009</td>
<td>Computer Vision</td>
<td>Depends (e.g., 1,350,000)</td>
<td></td>
<td>Classification (1,000 classes)</td>
<td>[AMJ18, AMJ18, ASW*19, HPCR20, JC17b, YCD15, ZF14, LC15]</td>
</tr>
<tr>
<td>Food and Nutrition [USD19]</td>
<td>2019</td>
<td>Nutrition</td>
<td>Depends (e.g., 7,637)</td>
<td></td>
<td>Clustering</td>
<td>[PKZ00, KDYB16, KKB<em>17, TMF</em>12, WLN<em>17, WLS19, ZLB</em>16]</td>
</tr>
<tr>
<td>CIFAR-10 [Kr19]</td>
<td>2009</td>
<td>Computer Vision</td>
<td>60,000</td>
<td>1,024 (32x32)</td>
<td>Classification (10 classes)</td>
<td>[CPCS20, HKK<em>17, JC17b, LSC</em>18, LSL<em>17, WS1W</em>18]</td>
</tr>
<tr>
<td>20 News groups [Lan95]</td>
<td>1995</td>
<td>News &amp; Humanities</td>
<td>18,828</td>
<td>2</td>
<td>Classification (20 classes)</td>
<td>[ASW<em>19, KBWS15, KLTH10, LKT</em>12, SLT*17, SNNM16]</td>
</tr>
<tr>
<td>Yelp Open Data Sets [Ye19]</td>
<td>2019</td>
<td>Reviews &amp; Other</td>
<td>Depends (e.g., 6,885,900)</td>
<td></td>
<td>Clustering</td>
<td>[MC22T, MC22C, MQR19, TKD17]</td>
</tr>
<tr>
<td>Google’s Quick Draw [JRK*16]</td>
<td>2016</td>
<td>Computer Vision</td>
<td>50,000,000</td>
<td>784 (28x28)</td>
<td>Classification (345 classes)</td>
<td>[CD18b, CPCS20, WGYS18, WGZ*19]</td>
</tr>
<tr>
<td>Reuters-21578 [RSW02]</td>
<td>2002</td>
<td>News &amp; Humanities</td>
<td>21,578</td>
<td>5</td>
<td>Classification (4 classes)</td>
<td>[LLG*18, KS12, SNM18, SSK10]</td>
</tr>
<tr>
<td>Optical Recognition of Hand. Digits [AK98]</td>
<td>1998</td>
<td>Computer Vision</td>
<td>5,620</td>
<td>64</td>
<td>Classification (10 classes)</td>
<td>[BAPR16, BDF17, KEV*18, LA11]</td>
</tr>
<tr>
<td>Census (Income) [DG17, YR07]</td>
<td>1994</td>
<td>Social</td>
<td>48,842</td>
<td>14</td>
<td>Classification (4 classes)</td>
<td>[MBD<em>11, GNRM08, WPB</em>20, MMLP16]</td>
</tr>
<tr>
<td>Boston Housing Prices [HRH78]</td>
<td>1978</td>
<td>Business</td>
<td>506</td>
<td>13</td>
<td>Regression</td>
<td>[AMJ18, ASW<em>19, HHC</em>19, SNL*99]</td>
</tr>
<tr>
<td>Number Quality of Life Index [NUM13]</td>
<td>2015</td>
<td>Socioeconomic</td>
<td>88</td>
<td>7</td>
<td>Clustering</td>
<td>[KDP17, ZW12, ZWC<em>18, LCW</em>19]</td>
</tr>
<tr>
<td>OECD Better Life Index [Lin14]</td>
<td>2014</td>
<td>Socioeconomic</td>
<td>34</td>
<td>24 (11 main)</td>
<td>Clustering</td>
<td>[CD18b, CD19, SDMT16]</td>
</tr>
<tr>
<td>House Prices [Coc11]</td>
<td>2011</td>
<td>Business</td>
<td>2,919</td>
<td>81</td>
<td>Regression</td>
<td>[DCC19, KP18, SRG*18]</td>
</tr>
<tr>
<td>Caltech-101 [FFP04]</td>
<td>2004</td>
<td>Computer Vision</td>
<td>3,030</td>
<td>Depends (e.g., 60,000)</td>
<td>Classification (101 classes)</td>
<td>[KLTH10, TLK*09, ZF14]</td>
</tr>
<tr>
<td>Core Image Features [DG17]</td>
<td>1999</td>
<td>Computer Vision</td>
<td>68,040</td>
<td>89</td>
<td>Classification (7 classes)</td>
<td>[MCM14, PSPM12, SDMT16]</td>
</tr>
<tr>
<td>Image Segmentation [DG17]</td>
<td>1990</td>
<td>Computer Vision</td>
<td>2,310</td>
<td>20</td>
<td>Classification (7 classes)</td>
<td>[CMN*16, JPN15, v11]</td>
</tr>
<tr>
<td>COMPAS Recidivism Risk Score [COM19]</td>
<td>2019</td>
<td>Justice</td>
<td>Depends</td>
<td></td>
<td>Classification (2 classes, Clustering)</td>
<td>[AMJ18, CEH*19]</td>
</tr>
<tr>
<td>USPS Hand. [USP17]</td>
<td>2017</td>
<td>Computer Vision</td>
<td>9,298</td>
<td>256 (16x16)</td>
<td>Classification (2 classes)</td>
<td>[LWT*15, ZTR16]</td>
</tr>
<tr>
<td>Titanic [Tit10]</td>
<td>2015</td>
<td>Life</td>
<td>712</td>
<td>10</td>
<td>Classification (2 classes)</td>
<td>[HHC*19, ZWL19]</td>
</tr>
<tr>
<td>Parkinson’s Disease [GTS*08, PPM14]</td>
<td>2014</td>
<td>Health</td>
<td>Depends (e.g., 8,652)</td>
<td></td>
<td>Classification (2 classes)</td>
<td>[CD18a, CD19]</td>
</tr>
<tr>
<td>Tennis Major Tournament [DG17]</td>
<td>2014</td>
<td>Sports</td>
<td>127</td>
<td>42</td>
<td>Regression, Clustering</td>
<td>[FKM20, LRL*18]</td>
</tr>
<tr>
<td>ALL [PSPM12]</td>
<td>2012</td>
<td>Publications</td>
<td>2,814</td>
<td>1</td>
<td>Clustering</td>
<td>[CMN*16, PSPM12]</td>
</tr>
<tr>
<td>Software Projects Quality [MSG*10]</td>
<td>2010</td>
<td>Computers</td>
<td>6,773</td>
<td>12</td>
<td>Classification (2 classes)</td>
<td>[CMN<em>16, SPK</em>15]</td>
</tr>
<tr>
<td>Construction Simulation [IPSC08]</td>
<td>2006</td>
<td>Simulation</td>
<td>2,900</td>
<td>10</td>
<td>Classification (2 classes)</td>
<td>[LWP14, LWT*15]</td>
</tr>
<tr>
<td>University Ranking [DG17]</td>
<td>1998</td>
<td>Education &amp; Status</td>
<td>285</td>
<td>18</td>
<td>Classification (2 classes)</td>
<td>[JHP<em>17, KEV</em>18]</td>
</tr>
<tr>
<td>Synthetic Faces [TLS]</td>
<td>2000</td>
<td>Artificial Intelligence</td>
<td>698</td>
<td>4,096 (64x64)</td>
<td>Classification (2 classes)</td>
<td>[RL15a, RL15b]</td>
</tr>
<tr>
<td>Concrete Compressive Strength [Yeh98]</td>
<td>1998</td>
<td>Construction</td>
<td>1,030</td>
<td>9</td>
<td>Regression</td>
<td>[CEH<em>19, SJS</em>18]</td>
</tr>
<tr>
<td>Adult [DG17]</td>
<td>1996</td>
<td>Social</td>
<td>48,842</td>
<td>14</td>
<td>Classification (2 classes)</td>
<td>[CEH<em>19, SJS</em>18]</td>
</tr>
<tr>
<td>German Credit [DG17]</td>
<td>1994</td>
<td>Financial</td>
<td>1,000</td>
<td>20</td>
<td>Classification (2 classes)</td>
<td>[AL20, ZWL19]</td>
</tr>
<tr>
<td>ISOLET [DG17]</td>
<td>1994</td>
<td>Computers</td>
<td>7,797</td>
<td>67</td>
<td>Classification (2 classes)</td>
<td>[Aup07, SIB10]</td>
</tr>
<tr>
<td>Waveform Database Generator [BFDS84]</td>
<td>1984</td>
<td>Telecommunications</td>
<td>5,000</td>
<td>22</td>
<td>Classification (3 classes)</td>
<td>[BAPR16, LMZ14]</td>
</tr>
<tr>
<td>Auto MPG [DG17]</td>
<td>1993</td>
<td>Business</td>
<td>398</td>
<td>9</td>
<td>Regression</td>
<td>[XYC*18, WS18]</td>
</tr>
<tr>
<td>Penn Treebank [MMS93]</td>
<td>1993</td>
<td>Humanities</td>
<td>60,774</td>
<td>36</td>
<td>Classification (2 classes)</td>
<td>[SGP*18, SBP19]</td>
</tr>
<tr>
<td>Breast Cancer Wisconsin [BM92]</td>
<td>1992</td>
<td>Health</td>
<td>699</td>
<td>10</td>
<td>Classification (2 classes)</td>
<td>[MQB19, XMM*19]</td>
</tr>
</tbody>
</table>

Others (i.e., data sets that are used once): 106 additional unique entries, see supplementary material S8

200 surveyed papers. The most frequently occurred data sets are MNIST [LBBH98], Iris [And36], Wine Quality [CCA*09], ImageNet [DDS’09], Food and Nutrition [USD19], CIFAR-10 [Kr19], and 20 News groups [Lan95]. 3 out of these 7 data sets are about computer vision and are usually used in papers that work with DL and NNs. Validating our previous categorization, classification and then clustering problems are the more occurring target variables, and finally regression. The number of instances and features can be found in our table along with the number of classes for some cases (if available). The individual papers that used the data sets are listed in the rightmost column of Table 5; and references to the data set providers are given together with the name of the data sets in the first column.
8. Discussion and Research Opportunities

In this section, we discuss our online survey browser. Afterwards, we move on to research opportunities based on the data-driven analyses presented in Section 7.

8.1. Interactive exploration with a survey browser

Our work on this survey has been complemented by the development of an interactive survey browser [BKW16, KK14, KK15, KPK18, Sch11, TA13] similar to our group’s previous contributions on text and sentiment visualization. TrustMLVis Browser is available as a web application, and its user interface (see Figure 8) comprises (1) a grid of thumbnails representing visualization techniques and (2) an interaction panel supporting category-, time-, and text-based filtering. The user can access the details and bibliographic information about a specific technique by clicking on the corresponding thumbnail. Several dialogs with the overall statistics for the complete data set (cf. Table 3) and the supplementary materials are available via the links at the top of the web page. We encourage the readers of this article to explore the data with the survey browser and to suggest further candidate entries by using the corresponding “Add entry” dialog.

8.2. Research Opportunities

The impact of bias. By looking at our categorization, we can infer that some level of bias might be represented in all our defined trust levels in different forms: (a) data bias (equality), (b) previous familiarity with algorithms, (c) model bias, and (d) user bias. Also, it is known that visualization techniques ordinarily do not scale very well when analyzing massive volumes of data. Furthermore, some of the ML approaches have inherent challenges to face, for example, the curse of dimensionality [Bel03] in case of DR. Thus, considerable levels of selection bias might be unintentionally ignored by the user, for instance, when users have to choose from a selection while not seeing the entire picture and/or the alternatives [GSC16, LA11]. Hence, the research question here is: “what novel solutions can help users to minimize the impact of bias with regard to the data?” A potential answer would be to consider various interaction logs with the VA system. Data generated as part of the analysis process could be considered as well. This data together with the logs could be processed automatically with additional independent ML models and potentially guide users to improvements of the underlying ML models used in the data analysis process. Hence, the ways of combining automatic methods with smart visualizations [Shn20] are still not revealed and should be further evaluated with empirical studies as well as quantitative and qualitative experiments.

Alternatives and combination. Visualization is often used as the medium enabling human-computer interactions (HCI). It usually encourages the development and application of multidisciplinary methods originating from different areas of research. To find an equilibrium state between human and computer controlling the ML process is not a trivial task [Shn20]. Researchers that are intimate with ML models and visualizations are capable of appropriately promoting the joint development of visual explanations for ML models. Furthermore, there is a possibility to employ verbalization (as discussed before) as a complementary tool alongside visualization for explaining ML models. The challenges of developing visualization systems involving such text explanations and finding the right balance between these two approaches are still open [SBE‘18]. Here, we foresee an open research challenge upon how to combine visualizations, verbalization (text explanations), and voice commands (AI assistants) that should together perform overlapping tasks in complex visualization systems and propose task solutions to the users. As can be seen with our categoriza-
tion, analysts usually deal with data manipulation problems which can lead to compromising the trust, for example, (1) comparison of structures, (2) guidance in data selection, (3) outlier detection, (4) comparison of algorithms, and (5) in-situ comparison of concrete model structures. The aforementioned methods might provide a possible remedy for such compromises of trust.

Security vulnerabilities. When research is conducted in ML, there is always a factor that is not often taken into account at first: “how do we secure ML models from unethical attacks?” An instance of this idea is published by Ma et al. [MXLM20], explaining how visualization can assist in avoiding vulnerabilities of adversarial attacks in ML. Specifically, their focus is on how to avoid data poisoning attacks from the models, data instances, features, and local structures perspectives with the use of their VA approach. Nowadays, visualization systems are deployed online for users to access them easily. Such internet-accessibility leads to further problems concerning security vulnerabilities. This is one of the advantages of TensorFlow.js, which utilizes the WebGL-accelerated implementation of JavaScript in web browsers to implement and use ML models on local computers.

Fairness of the decisions. Going beyond interpretability towards more explainability is another open challenge. However, general proposals of frameworks in the visualization community combining ML and visualizations have been already described in recent research papers [MXQR19, SSSEA20]. These global frameworks were divided into smaller parts by other works that compare DL methods, for instance [MMD+19]. Further tools explore local trends instead of global patterns [ZWRH14]. Two further open questions reaching beyond interpretability and explainability are “how fair were all those decisions and what if we have chosen another path?” and “how can fairness be translated between the trust levels?” (cf. the work by Ahn and Lin [AL20]).

Ways of communication and collaboration. Increasing the users’ trust in ML models is not a trivial task. Visualization can assist in this challenge in multiple ways. A good starting point is employing simple techniques, such as querying specific data instances and areas of interest, in a user-friendly way [HHN+12]. However, the issue of improving trustworthiness in ML with visualization is also related to the issue of improving the trust for visualization itself [BRBF14, BBG19]. To achieve the best outcome when evaluating visualization designs, the input data, the goals, and the target group of a visualization should be under the spotlight. On the optimistic side, many papers exist that try to employ simple techniques, such as querying specific data instances and areas of interest, in a user-friendly way, but further research is required in this regard.

Almost unexplored areas. Related to the non-trust level classes (which implicitly influence trust), we believe that all underrepresented categories can pose as new ideas for novel research. For example, visualization researchers have still not provided sufficient support for some specific NNs, such as convolutional deep belief networks (CDBNs), deep residual networks (DRNs), and multi-column DNNs (MCDNNs). Also in ensemble learning, visualization tools that target solely the boosting techniques are quite rare, e.g., gradient boosting and adaptive boosting (AdaBoost) appear not to be covered to the same level as random forests. Another example of such a category is stacking ensemble learning, i.e., constructing a combination (a stack) of different models that should become the input for other meta-model(s). Employing visualization to facilitate the experts in developing and using such stacks in a trustworthy way without resorting to trial and error is also an open research challenge. Additionally, regression problems are also far less covered than classification. In unsupervised learning, association/pattern mining is uncommonly investigated by visual tools. To conclude this paragraph, reinforcement learning approaches are almost ignored with only a few available papers covering this area of how visualization can help to monitor an automatically controlled learning process [SPBA19]. In reinforcement learning, classification tasks, i.e., letting an agent act on the inputs and learn value functions [WvPS11], are not once addressed by visualization.

9. Conclusion

In this survey, we study the state of the art in enhancing trust in machine learning (ML) models with the use of visualizations. We introduced the background necessary for defining trustworthiness of ML models and explained the methodology used to select relevant papers in the literature. Based on the selected 200 peer-reviewed publications that introduce a large variety of visualization techniques to increase trust in ML models and their results, we proposed a fine-grained categorization comprising 8 high-level aspects partitioned into 18 category groups that on their part contain 119 categories in total. In addition, we performed a topic analysis to be able to discover connections and emerging topics among the 200 papers. Further analyses of the categorized data involved category correlations, temporal trends, and data sets used in the respective publications. In order to make our categorization and the assignment of papers into categories accessible for the public, an interactive survey browser—called TrustMLVis Browser—was implemented and made available online. It supports the readers of this STAR in the exploration of the rich information provided in this work, thus facilitating future research in enhancing trustworthiness of ML models with the help of interactive visualizations. Our findings indicate the growing interest for developing visualizations in ML to improve trustworthiness in the context of various data domains, tasks, and multidisciplinary applications. As future work, we intend to continue extending and refining the survey data set, categorization, and corresponding analyses, as well as maintaining the online survey browser.

References


doi:10.1109/ICDAR.1997.620583.25


Chatzimisropas et al. / Enhancing Trust in Machine Learning Models with the Use of Visualizations


[FP04] Fei-Fei L., Fergus R., Perona P.: Learning generative visual models from few training examples: An incremental Bayesian


Chatzimparmpas et al. / Enhancing Trust in Machine Learning Models with the Use of Visualizations

Chatzimparmpas et al. / Enhancing Trust in Machine Learning Models with the Use of Visualizations

Chatzimparmpas et al. / Enhancing Trust in Machine Learning Models with the Use of Visualizations
Chatzimparmpas et al. / Enhancing Trust in Machine Learning Models with the Use of Visualizations


Kemp B., Zwinderman A. H., Tuk B., Kamphuizen H. A. C., Oberje J. J. L.: Analysis of a sleep-dependent neuronal feedforward loop: The slow-wave microcontinuity of the EEG. IEEE Transactions on Biomedical Engineering 49, 9 (Sept. 2000), 1185–1194. doi:10.1109/87.867928. 25


LR02 Li X., Roth D.: Learning question classifiers. In Proceedings of the 19th International Conference on Computational Linguistics-
Chatzimparmpas et al. / Enhancing Trust in Machine Learning Models with the Use of Visualizations

© 2020 The Author(s)
Computer Graphics Forum © 2020 The Eurographics Association and John Wiley & Sons Ltd.


[Spi88] Spiegelhalter D.: Making algorithms trustworthy: What can statistical science contribute to transparency, explanation and validation? Plenary invited talk at NeuRIPS ’18, Dec. 2018. 4


© 2020 The Author(s)
Computer Graphics Forum © 2020 The Eurographics Association and John Wiley & Sons Ltd.
Chatzimparmpas et al. / Enhancing Trust in Machine Learning Models with the Use of Visualizations

Medical Research 25, 3 (June 2016), 1057–1073. doi:10.1177/096282015588241.9


Chatzimparmpas et al. / Enhancing Trust in Machine Learning Models with the Use of Visualizations


