nameAlgorytm

Spis treści

1. Wstęp

Coraz częściej urządzenia internetu rzeczy stają się głównymi urządzeniami komputerowymi coraz większej liczby użytkowników (cite). Często gromadzą one wrażliwe dane i dostęp do takich urządzeń przez niewłaściwe osoby grozi nieodwracalnymi stratami dla ich właściciela. Nowe przyrządy wyposażone w odpowiednie sensory pozwalają na uwierzytelnienie dostępu już nie tylko za pomocą hasła ale również przez weryfikacje biometryczną. Zabezpieczenia biometryczne mogą się opierać na rozpoznawaniu linii papilarnych, głosu, skanowaniu żył, czy też tęczówki lub siatkówki oka. W szczególności popularnym rozwiązaniem jest weryfikacja użytkownika przez biometrie twarzy (jakiś cytat).

Metody weryfikacji twarzy (ją jakieś) wymagają wyspecjalizowanych i dokładnych kamer (need fact check). Z jednej strony montowanie drogich i nowoczesnych kamer na urządzeniach IoT do celów weryfikacji jest nieopłacalne finansowo, a z drugiej z perspektywy użytkownika pożądane jest posiadanie możliwie dokładnego systemu weryfikacji dostępu. Najnowocześniejsze i najbardziej dokładne metody bazują w całości lub przynajmniej części na bazie sieci neuronowych (cite,fact check). Metody te pewnym stopniu niwelują potrzebę posiadania wyspecjalizowanych kamer jednak dokładność nowoczesnych metod jest bardzo uzależniona od jakości i ilość danych, które posłużyły do wytrenowania sieci neuronowej.

Sensory, w które wyposażone są te urządzania (na przykład aparat, mikrofon, itp), w połączeniu z faktem, że są używane codziennie, gromadzą niebywałą ilość, zazwyczaj prywatnych, danych. Modele wyuczone na takich danych dają znakomitą poprawę ich użyteczności jednak ze względu na wrażliwy charakter danych wiąże się z ryzykiem i wysoką odpowiedzialnością ich przechowywania w scentralizowanej lokalizacji albo nawet całkowitym brakiem dostępu do tych danych.

Federated Learning pozwala na bezpieczne dla użytkownika wykorzystanie jego prywatnych danych (zdjęć) w celu dotrenowania sieci neuronowych i w tym poprawy ich jakości. W tej pracy zostanie zbadana metoda ta metoda uczenia sieci neuronowych w implementacji systemu rozpoznawania twarzy systemu na urządzania IoT.

Praca została podzielona na rozdziały. W rozdziale XXX została przedstawiona ogólny zarys implementowanego systemu. Opisujemy czym charakteryzują się urządzania IoT się, na czym polega zadanie weryfikacji użytkownika i pokazujemy, że zastosowanie podejścia Federated Learningu do tego zadania jest odpowiednie.

Następnie w rozdziale XXX w szczegółach zostaje opisany problem weryfikacji użytkownika na podstawie cech biometrycznych jego twarzy. Omawiane zostają dwa współczesne podejścia wykorzystujące głębokie sieci neuronowe, ich wady i zalety względem wykorzystania w FL. Prezentujemy dokładniej wybrane przez nas podejście wraz z naszą implementacją i otrzymanymi wynikami.

Rozdział XXX został poświęcony na omówienie Federated Learningu. Opisujemy

cechy środowiska, w którym zastosowanie tej metody treningu sieci daje największy zysk, prezentujemy projekt całego systemu zaczynając od protokołu komunikacji, założeń co do urządzeń końcowych oraz serwera. Omawiamy w algorytm Federated Averaging, jego implementacje oraz walidacje implementacji na syntetycznym zbiorze danych MNIST oraz CIFAR10. Ostatecznie prezentujemy zastosowanie FL do dotrenowania ekstraktora cech w rozproszonym zbiorze danych.

Na końcu w rozdziale XXX zostało zawarte podsumowanie tej pracy wraz z propozycją jej dalszego rozwoju.

Główne kontrybucje tej pracy to 1) Implementacja i weryfikacja algorytmu FL dla zadań klasyfikacji obrazów oraz weryfikacji twarzy. 2) ???

2. Rozproszone uczenie na urządzeniach IoT

Praca została podzielona na rozdziały. W rozdziale XXX została przedstawiona ogólny zarys implementowanego systemu. Opisujemy czym charakteryzują się urządzania IoT się, na czym polega zadanie weryfikacji użytkownika i pokazujemy, że zastosowanie podejścia Federated Learningu do tego zadania jest odpowiednie.

3. System weryfikacji użytkownika za pomocą biometrii twarzy

3.1. Biometria twarzy

twarz nadaje się do weryfikacji; przykłady systemów weryfikacji?

3.2. Procedura weryfikacji przy wykorzystaniu sieci neuronowych

Weryfikacja twarzy jest zadaniem przyrównania twarzy kandydata to innej, i weryfikacja czy nastąpiło ich dopasowanie. Jest to mapowanie jeden-do-jednego: należy sprawdzić czy jest to ta sama osoba.

Mając na wejściu naszego systemu dwa zdjęcia x_i oraz x_j wynik weryfikacji będzie wyznaczany następująco:

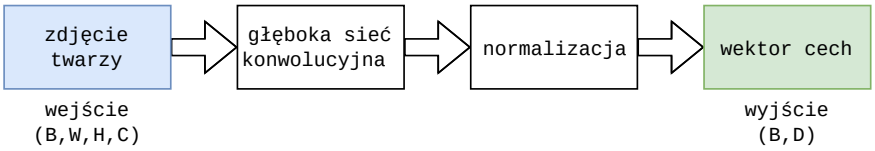
$$\text{weryfikacja jest} \begin{cases} \text{pozytywna}, & \text{jeśli } d(f(x_i), f(x_j) < \alpha \\ \text{negatywna}, & \text{w.p.p} \end{cases} \tag{1}$$

gdzie $f(x)$ jest wektorem cech obrazu x, opisanym w sekcji 3.4, α jest marginesem, $d(f_1, f_2)$ jest pewną funkcją dystansu liczoną pomiędzy wektorami f_1, f_2.

3.3. Wstępne przetwarzanie obrazu

3.4. Neuronowy ekstraktor cech

We współczesnych systemach weryfikacji wykorzystuje się głębokie sieci konwolucyjne. W szczegółach zostaną omówione używana przez nas architektura w sekcji XXX. Pomijając szczegóły modelu i traktując go jako czarną skrzynkę ogólna idea ekstraktora została pokazana na Rysunku 1. Głównym założeniem jest stworzenie systemu end-to-end, którego rezultatem działania będzie embedding $f(x)$, wyznaczony z obrazu wejściowego x przez rzutowanie go do pewnej przestrzeni cech $\mathbb{R}^d$, w taki sposób, że pewna funkcja odległości wyznaczona dla wszystkich zdjęć twarzy jest mała dla twarzy należących do tych samych osób i duża dla różnych twarzy.



Rysunek 1. Struktura ekstraktora cech. Ekstraktor składa się z wejścia, które w ogólnym przypadku może być paczką B przetworzonych wstępnie obrazów twarzy o wymiarach $W \times H \times C$, głębokiej sieci konwolucyjnej i następującej po niej warstwie normalizacji. W rezultacie na wyjściu otrzymujemy B wektorów cech o wymiarach D.

W literaturze można znaleźć dwie rodziny algorytmów, jedna wzorująca się na klasycznym podejściu stosowanym podczas klasyfikacji obrazów i druga bazująca na optymalizacji multi-class classification hinge loss (po pl?).

Classification loss Pokazać że jest kilka rodzajów takich funkcji 1) Centre loss 2) Cosine loss 3) Arc loss

Tripletloss jest o wiele lepszy dla zastosowań federated learningu procedura trenowania

$$\left\| f(x_i) - f(x_j) \right\|_q^p < \alpha \tag{2}$$

3.5. Implementacja systemu weryfikacji twarzy

Zbiory danych Są jakieś zbiory daych 1) VggFace2 2) MS1M 3) MegaFace 4) LWF

Sprawdzić wpływ datasetu początkowego na wyniki ewaluacji początkowego modelu globalego

ms1m do pre trengowania ponieważ posiada duża różnorodność twarzy oraz ogólną duża liczbe przykładów trenujących. VggFace2 zostonie z koleji wykorzystany do koncowego dotreniowania modelu - ze względu na dużą liczę zdjec przypadajaca na jedna osobę posiada dużą różnorodność wewnątrzklasową co powinno zwięszyć finałową wfektywaność podelu - większa odporność na rotację twarzy względem obiektywu, zmienne wartunki świetlne itp.

Ze względu na popularność dwóch ostatnich zbiorów w ewaluacji systemów rozpoznających twarze zostaną one właśnie wykorzystane do ewaluacji, MegaFace ma tę dodatkową zaletę, dużej liczby osób, a dwa pierwsze tylko do treningu.

3.5.1. Metody weryikacji twarzy

Wyjściem z modelu jest wektor(embedding), który pozwala na odróżnienie jednej twarzy od drugiej za pomocą porównanie embedingPapier googla twierdzi ze udało im sie uzyskać dobry score jednak nie rzadne inne prace nie raportują sukcesywngeo otrzymania podobnego wyniku. Może to wynikać z 1) braku zbliżonego wielkością zbioru danych

użytych do uzyskania wyniku raportowangeo przez googla 2) brakiem podobnych zasobów obliczeniowychu jednej twarzy do embedingu drugiej twarzy. Coś o tym, że są tak jakby dwie rodziny algorytmów. Jedna bazująca na klasycznym podjeściu stosowanym podczas klasyfikacji obrazów i druga bazująca na optymalizacji multi-class classiication hindge loss(jak to do uja wafla przetłumaczyć?).

Papier googla twierdzi ze udało im sie uzyskać dobry score jePapier googla twierdzi ze udało im sie uzyskać dobry score jednak nie rzadne inne prace nie raportują sukcesywngeo otrzymania podobnego wyniku. Może to wynikać z 1) braku zbliżonego wielkością zbioru danych użytych do uzyskania wyniku raportowangeo przez googla 2) brakiem podobnych zasobów obliczeniowychdnak nie rzadne inne prace nie raportują sukcesywngeo otrzymania podobnego wyniku. Może to wynikać z 1) braku zbliżonego wielkością zbioru danych użytych do uzyskania wyniku raportowangeo przez googla 2) brakiem podobnych zasobów obliczeniowych

Tripletloss jest o wiele lepszy dla zastosowań federated learningu procedura trenowania

Classification loss Pokazać że jest kilka rodzajów takich lossów 1) Centre loss 2) Cosine loss 3) Arc loss

Implementacja Papier googla twierdzi ze udało im sie uzyskać dobry score jednak zadne inne prace nie raportują sukcesywngeo otrzymania podobnego wyniku. Może to wynikać z 1) braku zbliżonego wielkością zbioru danych użytych do uzyskania wyniku raportowangeo przez googla 2) brakiem podobnych zasobów obliczeniowych

Została podjęta próba implementacji wytrenowania modelu stosując w.w.y metodę wykorzystując zbiór danych VggFace2.

W celach pokazania, że implementacja jest poprawna porównujemy następujące modele

Porównanie: dwa poejścia: dwa datasety, modele niekoniecznie moje ale testowane na własnej ewaluacji

triplet(google report), wytrenowanych na danych prywatnych triplet(own), centre(external source) wytrenowanych na VggFace2 triplet(own), centre(external source) wytrenowanych na MS1m -> wyjdzie, że triplet loss jest o wiele mniej skuteczna

see this: https://arxiv.org/pdf/1901.08616.pdf https://arxiv.org/pdf/1709.02940.pdf

3.5.2. Rozporszona weryfikacja twarzy

porównanie:

centre loss ms1m

globalny model arcface uczony na ms1m, testowany na lwf i megaface globalny model arcface uczony na ms1m, dotrenowany tripletem na VggFace2, testowany

globalny model arcface dotrenowanie na lwf ale negatywne przykłady samplujemy z generatora globalny model arcface dotrenowanie na megaface ale negatywne przykłady samplujemy z generatora

4. Federated Learning

W tym rozdziale przedstawiony zastany projekt systemu, który korzystając z podejścia Federated Learning (FL) umożliwi na trening ekstraktora cech twarzy w rozproszonym środowisku urządzeń IoT.

Federated Learning Federated Learning (FL) jest podejściem zastosowania uczenia maszynowego w rozproszonym środowisku pozwalające na trening modeli on dużym zbiorze danym zdecentralizowanych prywatnych danych znajdujących się na urządzeniach końcowych użytkowników, a w szczególności urządzeniach Internetu Rzeczy. FL realizuje ideę "przyniesienie kodu do danych, zamiast danych do kodu"i adresuje fundamentalne problemu prywatności, własności i lokalności danych. Federated learning został opisany w (cite). Problemy odpowiednie do zastosowania federated learningu moją następujące właściwości:

- Trening na rzeczywistych danych gromadzonych na urządzaniach mobilnych dają znaczą przewagę nad treningiem na ogólnie dostępnych danych proxy dostępnych w centrach danych.
- Te dane są prywatne albo są zbyt duże do przetrzymywania ich w centrach danych
- Dla zadań nadzorowanych, etykiety danych powstają samoistnie z interakcji użytkownika z urządzeniem.

Cechy środowiska systemu Algorytmy optymalizacji mogące być zastosowane do optymalizacji na urządzaniach IoT mają kilka cech wyróżniających je od znanych już algorytmów rozproszonej optymalizacji:

- **Non-IID** Dane trenujące on danym urządzaniu są zazwyczaj zależne od konkretnego użytkownika i dlatego lokalny zbiór danych zebrany na dowolnym urządzeniu nie będzie reprezentatywny w stosunku do dystrybucji całej populacji
- **Niezbalansowany** Podobnie, niektórzy użytkownicy będą o wiele częściej korzystali z aplikacji aparatu niż inni, co będzie prowadziło do różnic w wielkości zebranych lokalnych zbiorów danych trenujących.
- **Masywnie rozproszony** Spodziewa się, że liczba finalnych użytkowników biorąca udział w optymalizacji będzie większa niż średnia liczba przykładów trenujących przypadająca na jednego klienta.
- **Ograniczona komunikacja** Urządzania IoT są pomimo założenia, że mają dostęp do internetu mogą być ograniczone wolnym albo kosztownym łączem sieciowym.

W tej pracy główna uwaga zostanie poświęcona na doprowadzenie systemu do działania w patologicznym przypadku środowisku danych Non-IID oraz ograniczonej i zawodnej komunikacji.

4.1. Projekt systemu

Implementowany system umożliwia trening głębokich sieci neuronowych on danych przetrzymywanych na bezpośrednio urządzaniu IoT. Dane te nigdy nie opuszczają samego urządzania. Wagi modelu są agregowane i łączone na serwerze znajdującym się w chmurze za pomocą algorytmu Federated Averaging konstruując nowy model globalny, który zostaje przesłany z powrotem do urządzeń końcowych do inferencji. System ten został opisany pierwotnie w (cytat) i z sukcesem zaaplikowany w implementacji inteligentnej klawiatury smartphone. (cite blogaska googla).

Przedstawienie architektury systemu zaczynamy od przedstawienia protokołu według, którego przebiega cały przepływ danych. Opisujemy to w następnej sekcji.

4.1.1. Protokół

Uczestnikami protokołu są urządzania Internetu Rzeczy oraz serwer, który jest usługą chmurową. Urządzania anonsują serwerowi swoją gotowość do uruchomienia zadania. Zadanie jest specyficzne dla populacji urządzeń i polega na lokalnym uruchomieniu obliczeń, takich jak trening z zadanymi przez serwer parametrami albo ewaluacja wytrenowanego modelu na lokalnych dla urządzenia danych.

Protokół dzieli komunikacje na rundy, z której każda zaczyna się od selekcji. Z potencjalnie tysięcy gotowych urządzeń w danym oknie czasowym, serwer wybiera ich podzbiór, który dostanie zaproszenia do wzięcia udziału obliczeniach. Liczebność tego podzbioru jest parametrem algorytmu opisywanego w kolejnym rozdziale

Serwer mówi wybranym urządzeniom jakiego typu obliczenia będą wykonywane. Wraz z tą informacją przesłany graf obliczeniowy modelu, zserializowane parametry globalnego modelu oraz pozostałe informacje niezbędne do uruchomienia obliczeń w danej rundzie. Następnie każdy z uczestników wykonuje lokalnie obliczenia bazując na globalnym stanie oraz swoim lokalnym zbiorze danych i przesyła wynik obliczeń z powrotem na serwer. W szczególności wynikiem, w przypadku rundy treningowej, będą wytrenowane parametry modelu lokalnego. Serwer wciela zebrane aktualizacje w swój stan globalny co kończy pojedyńczą rundę i proces ten się powtarza.

Opisywany protokół pozwala urządzeniom końcowym na poprawianie globalnego, pojedyńczego modelu pomiędzy rundami, z których każda składa się z trzech faz co zostało pokazane na rysunku (rysunek?).

Selekcja Cyklicznie, urządzenia, które spełniają wymagane kryteria (Patrz sekcja XXX) meldują serwerowi swoją gotowość. Serwer wybiera podzbiór z dostępnych mu urządzeń. W naszej implementacji wybrano prostą, losową selekcje z rozkładem jednostajnym N urządzeń z tych, które ogłosiły swoją gotowość.

Konfiguracja Serwer jest skonfigurowany na podstawie wybranego mechanizmu selekcji urządzeń oraz agregacji modeli. Urządzenia końcowe są samo-konfigurowane według

przesłanej przez serwer informacji o typie obliczeń, grafu obliczeniowego oraz stanu globalnego.

Raportowanie Serwer czeka, aż partycypujące urządzenia zdadzą raport z wynikiem przeprowadzonych obliczeń. Jeśli runda była rundą treningową to wraz z otrzymaniem wszystkich zaktualizowanych modeli, serwer agreguje je z użyciem algorytmu Federated Averaging i informuje raportujące urządzenia kiedy mogą ponownie zgłosić swoją gotowość. Jeśli wystarczająca liczba urządzeń zaraportuje wyniki serwerowi w pewnym oknie czasowym, runda zostanie uznana za zakończoną z powodzeniem i zagregowany model zastąpi aktualny model globalny. W przeciwnym przypadku zebrane wyniki z tej rundy zostają porzucone. Protokół jest w pewnym stopniu odporny na to, że partycypujące urządzenia z pewnych powodów nie odpowiedzą na przesłaną konfiguracje albo nie zaraportują wyników.

Fazy selekcji i raportowania są dospecyfikowane przez zestaw parametrów. Podczas fazy selekcji serwer bierze pod uwagę pożądaną liczbę uczestników rundy, czasy time-outów oraz minimalną liczbę potrzebnych uczestników do rozpoczęcia rundy. Faza selekcji trwa dopóty dopóki nie zostanie wybrana docelowa liczba urządzeń albo nie skończy się czas przeznaczony na faze selekcji. W drugim przypadku runda zostanie rozpoczęta jeśli została zebrana minimalna liczba urządzeń, w przeciwnym przypadku runda zostaje porzucona. Faza raportowania parametryzowana jest przez minimalną liczbę urządzeń, które muszą zaraportować wynik.

4.1.2. Urządzenie IoT

4.1.3. Serwer

4.2. Algorytm optymalizacji

Algorytm 1 opisany został zaimplementowany w języku Python. Do implementacji modeli neuronowych i algorytmów uczących został wykorzystany framework PyTorch [1]. Poprawność implementacji została sprawdzona na zadaniu klasyfikacji obrazów wykorzystując prostą sieć konwolucyjną oraz popularny zbiór danych CIFAR10.

Sieć konwolucyjna Jako obiekt treningu omawianego algorytmu zastała użyta niewielka sieć neuronowa zawierająca dwie warstwy konwolucyjną z filtrami o szerokości 5x5 (pierwsza z 32 kanałami, druga z 64, po każdej dodatkowa warstwa 2x2 max pooling), po których następuje dwu-warstwowy perceptron i na końcu warstwa przekształcenia liniowego, co daje w sumie 10^6 miliona parametrów. Model został podsumowany w tabeli

CIFAR10 CIFAR10 jest popularnym syntetycznym zbiorem danych. Zbiór danych składa się z 60 000 kolorowych obrazów podzielonych na 10 klas, z 6000 obrazami przypadającymi na jedną klasę. Zawarte są w nim obrazy o szerokości i wysokości 32 pikseli. Standordowo

Algorytm 1 `FederatedAveraging`. The K clients are indexed by k; B is the local minibatch size, E is the number of local epochs, and η is the learning rate.

Server executes:
initialize w_0
for each round $t = 1, 2, \dots$ **do**
  $m \leftarrow \max(C \cdot K, 1)$
  $S_t \leftarrow$ (random set of m clients)
  for each client $k \in S_t$ **in parallel do**
    $w_{t+1}^k \leftarrow \text{ClientUpdate}(k, w_t)$
  $w_{t+1} \leftarrow \sum_{k=1}^{K} \frac{n_k}{n} w_{t+1}^k$

ClientUpdate (k, w): // *Run on client k*
$\mathcal{B} \leftarrow$ (split $\mathcal{P}_k$ into batches of size B)
for each local epoch i from 1 to E **do**
  for batch $b \in \mathcal{B}$ **do**
    $w \leftarrow w - \eta \nabla \ell(w; b)$
return w to server

zbiór dzieli się na dwa zbalansowane klasowo podzbiory: testowy i treningowy zawierających odpowiednio 10000 i 50000 etykietowanych przykładów. Na rysunku 2 znajduje się 10 losowo wybranych obrazów, dla każdej z 10 klas.

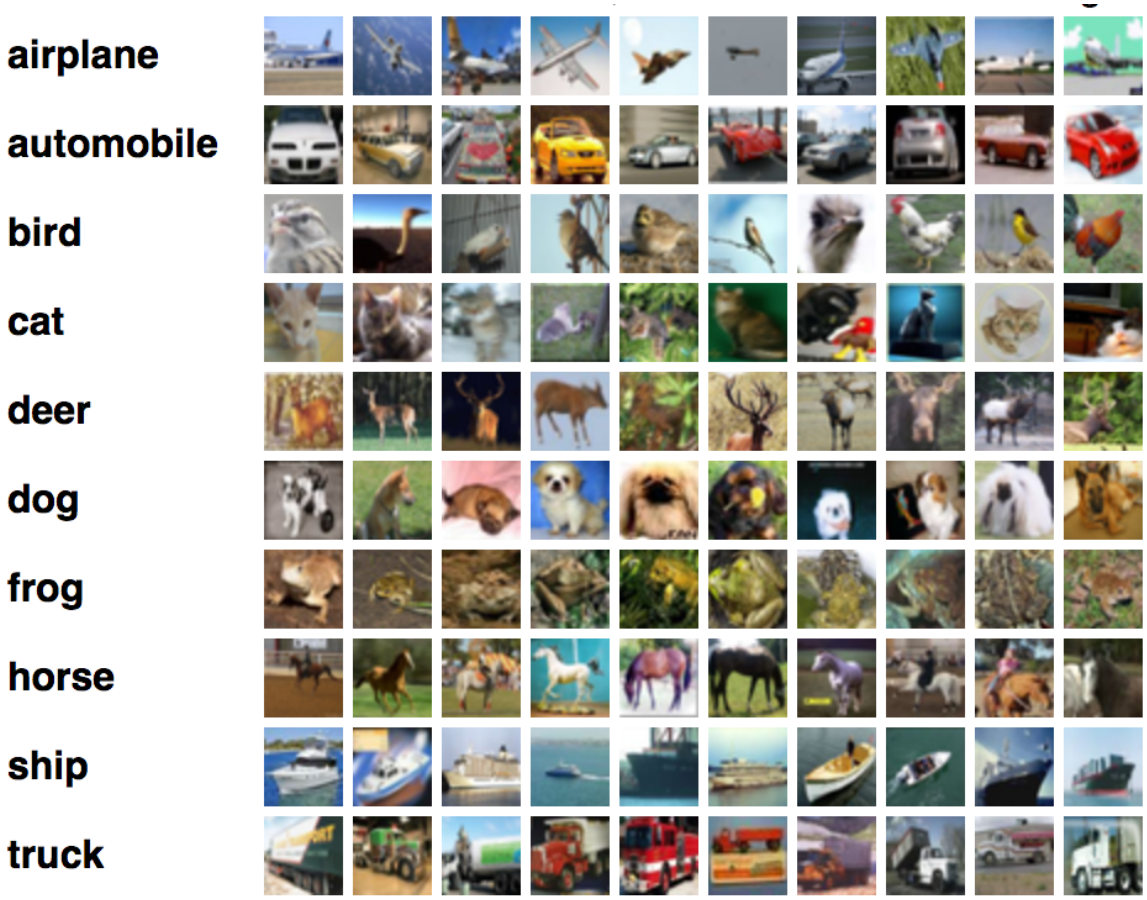
Protokół treningowy Do sprawdzenia poprawności implementacji została zaimplementowana procedura treningowa wzorowana na [2]. Zbiór treningowy został podzielony pomiędzy 100 użytkowników tak żeby każdy zawierał po 500 przykładów trenujących. Z powodu braku naturalnego podziału danych na tak dużą liczbę klientów rozważany jest tutaj nieco mniej wymagający przypadek, w którym dane każdego użytkowania są zbalansowane oraz równomiernie rozdystrybuowane.

Naszym celem była maksymalizacja dokładności z jaką model klasyfikował obrazy pochodzące ze zbioru testowego.Badanie jakości końcowego modelu globalnego odbywało się już nie w sposób rozproszony, a na serwerze stosując cały dostępny zbiór testowy, co zostało umożliwione dzięki wprowadzonym uproszczeniom co do rozkładu danych.

Obrazy uległy standardowemu przetworzeniu wstępnemu i augmentacji. Przykłady trenujące zredukowano do wielkości 24x24 pikseli przez losowe obcięcie krawędzi, obrazy uległy losowemu horyzontalnemu odbiciu lustrzanemu oraz standardowej normalizacji.

Zaimplementowany algorytm został porównany do standardowego algorytmu SGD (cytat).

Ewaluacja



Rysunek 2. 10 przykładowych obrazów dla każdej z 10 klas zbioru CIFAR10

5. Podsumowanie

Bibliografia

[1] A. Paszke, S. Gross, S. Chintala, G. Chanan, E. Yang, Z. DeVito, Z. Lin, A. Desmaison, L. Antiga i A. Lerer, **?**Automatic Differentiation in PyTorch**?**, w *NeurIPS Autodiff Workshop*, 2017.

[2] H. B. McMahan, E. Moore, D. Ramage, S. Hampson i B. A. y Arcas, *Communication-Efficient Learning of Deep Networks from Decentralized Data*, 2016. arXiv: 1602.05629 [cs.LG].

Wykaz symboli i skrótów

EiTI – Wydział Elektroniki i Technik Informacyjnych
PW – Politechnika Warszawska