DOI: https://doi.org/10.36910/6775-2524-0560-2024-54-04
УДК 004.032
Пензеник Андрій Андріянович, аспірант
https://orcid.org/0000-0002-2972-2600
Ужгородський національний університет, м. Ужгород, Україна

АВТОМАТИЗОВАНЕ ВИЯВЛЕННЯ ТА ПОПЕРЕДЖЕННЯ ПЕРЕНАВЧАННЯ В НЕЙРОННИХ МЕРЕЖАХ

Пензеник А.А. Автоматизоване виявлення та попередження перенавчання в нейронних мережах. У статті розглядається питання перенавчання нейронних мереж, проблеми, яка набула популярності по мірі зростання складності моделей штучного інтелекту. Оскільки нейронні мережі стають все складнішими та потужнішими, ризик перенавчання, явища, коли модель вивчає шум і специфіку навчальних даних, замість якісного узагальнювання нових даних. Було досліджено тонкощі перенавчання та його згубний вплив на продуктивність моделі, наголошуючи на необхідності складних підходів для виявлення та пом'якшення цієї проблеми. У статті розглядаються різні методивиявлення, починаючи від статистичних вимірювань і закінчуючи вдосконаленими підходами на основі моделі, підкреслюючи їх сильні сторони та обмеження. Зроблено огляд превентивних стратегій, таких як методи регуляризації, відсіву та ансамблеві методи, які спрямовані на покращення узагальнення моделі. Розглядаються останні досягнення в автоматизованому машинному навчанні (AutoML) і оптимізації гіперпараметрів, з оглядом на їхню ефективність у стримуванні надмірного навчання моделі без перешкод для її точності. Було запропоновано ідею використання ін'єкції шуму для придушення перенавчання в різних нейронних мережах і продемонстровано, що: шум може пригнічувати перенавчання у багатошаровому перцептроні (MLP) і довготривалій короткочасній пам'яті (LSTM). Ця робота показує, що шум може бути ефективним рішенням для пригнічення перенавчання в нейронній мережі Гопфілда (HNN), і, що більш важливо, це додатково свідчить про те, що недосконаліть цифрових пристроїв є багатим джерелом рішень дляприскорення розвитку апаратних технологій в епоху штучного інтелекту.
Ключові слова: перенавчання, нейронні мережі, узагальнення моделі, автоматичне виявлення, стратегії запобігання, методи регулярізації, шум, оптимізація.

Penzenyk A. Automated Detection and Prevention of Overfitting in Neural Networks. The article explores the issue of overfitting in neural networks, a problem that has gained popularity with the increasing complexity of artificial intelligence models. As neural networks become more intricate and powerful, the risk of overfitting, where the model learns noise and specifics of the training data instead of qualitatively generalizing new data, becomes a significant concern. The intricacies of overfitting and its detrimental impact on model performance have been investigated, emphasizing the need for sophisticated approaches to detect and mitigate this problem. The article discusses various detection methods, ranging from statistical measurements to advanced model-basedapproaches, highlighting their strengths and limitations. A review of preventive strategies, such as regularization methods, dropout, and ensemble techniques, is also presented, all aimed at improving the model's generalization. Recent advancements in automated machine learning (AutoML) and hyperparameter optimization are explored, considering their effectiveness in restraining model overtraining without hindering its accuracy. The article introduces the idea of using noise injection to suppress overfittingin various neural networks and demonstrates that noise can dampen overfitting in amultilayer perceptron (MLP) and long short-term memory (LSTM). This work shows that noise can be a beneficial solution for mitigating overfitting in a Hopfieldneural network (HNN) and, more importantly, further suggests that the imperfections in semiconductor devices serve as a rich source of solutions for accelerating hardware technologies in the era of artificial intelligence.
Key words: overfitting, neural networks, model generalization, automated detection, prevention strategies, regularization techniques, noise, optimization.

Вступ та постановка проблеми. В умовах сьогодення нейронні мережі представляють собою ключовий прорив в області здобутків у сфері досліджень штучного інтелекту, віддзеркалюючи складну архітектуру людського мозку для обробки інформації та прийняття рішень. Ці обчислювальні моделі складаються з взаємопов'язаних вузлів, або штучних нейронів, організованих у шари, які працюють разом, щоб навчатися з даних івиконувати завдання без явного програмування. Нейронні мережі чудово працюють у різних програмах, демонструючи свою універсальність і ефективність у таких завданнях, як розпізнавання зображень і мови, обробка природної мови та навіть у стратегічних іграх.

Однією з ґрунтовних особливостей нейронних мереж є їх чудова здатність узагальнювати шаблони та зв'язки від навчальних даних до нових, невідомихданих. Ця адаптивність дозволяє їм робити прогнози та класифікації з високимступенем точності, сприяючи їх широкому впровадженню в галузях промисловості. Однак основою проблемою нейронних мереж постає їх перенавчання.

Перенавчання відбувається, коли нейронна мережа стає надто вмілою увивченні деталей і шуму, тобто будь-яких небажаних перешкод або перешкод,які впливають на якість, цілісність або надійність навчальних даних, що призводить до втрати її здатності узагальнювати нові, невидимі дані. Ці виклики підкреслюють делікатний баланс, необхідний у процесі навчання, наголошуючи на необхідності таких методів, як регуляризація та надійніметоди перевірки, щоб знизити ризики,

пов'язані з перенавчанням. Навігаціяв цих тонкощах має вирішальне значення для використання повного потенціалу нейронних мереж, одночасно забезпечуючи їх надійність і застосовність у практичних умовах.

При використанні регуляризації, алгоритми навчання нейронних мережмодифікуються для зменшення помилки узагальнення, але не помилки навчання. Найпоширеніші методи регуляризації включають:

– рання зупинка: автоматичне припинення навчання, коли певнийпоказник продуктивності перестає покращуватися;

– зниження ваги: стимулює мережу використовувати менші вагові коефіцієнти шляхом додавання мінімізуючого параметру до функції втрат;

– випадання: випадкове ігнорування певних вузлів у шарі під часнавчання;

– комбінація моделей: усереднення виходів окремо навчених нейроннихмереж;

– ін'єкція шуму: допуск деяких випадкових флуктуацій в даних черезрозширення.

Аналіз останніх досліджень і публікацій. Наукові діячі сьогодення внесли значний вклад у розробку методологій автоматизованого виявлення та попередження перенавчання в нейронних мережах. Окрім цього був проведений ряд досліджень для вирішення проблеми навчання нейронних мереж.

У роботах А. Л. І. Мукурі та С. Констхольма [1] було виявлено, що перенавчанню можна запобігти шляхом аугментації даних, тобто процесу штучного генерування нових даних з урахуванням існуючих. Для збільшення каталогу даних на прикладі зображень, можна використовувати ряд технік, таких як перехід, масштабування, обертання, додавання шуму, зміна яскравості тощо.

Завдяки Н. Е. Халіфу, М. Хамеду Таха, А. Е. Хассаньєну та І. Селіму [2] було вперше реалізовано метод аугментації навчальних даних, у результаті чого підвищились надійність запропонованої архітектури та стійкість до пам'яті даних. Однак у випадку перенавчання мережі, в ході проведеної роботи вдалося зменшити його наслідки, але не повністю подолати.

В той час в [3] були використані наступні методи регуляризації:

– L1 (lasso regression) та L2 (ridge regression). Дані методи машинного навчання додають мінімізуючий параметр до функції втрат. Регулярізація L1 додає абсолютне значення коефіцієнта як мінімізуючий параметр, генеруючи розріджені рішення та є корисним для вибору функцій. Регулярізація L2 додає квадрат величини коефіцієнта у якості мінімізуючого параметру, даючи не розріджені рішення та є корисним для побудови простіших моделей.

– метод відсіву, який полягає у випадковому ігноруванні певних вузлів під час навчання.

Результати показали, що L1 і L2 не є ефективними методами для запобігання перенавчання, але вони підвищили точність моделі.

Крім вище описаних робіт дослідників, варто зазначити праці наступнихнауковців: Кадхім Захра, Абдулла Хасанен і Гатван Халіл [4], Сабірі Біхі, АсріБухра, і Рануї Марієм [5], Корновскі Гай, Єхудай Гілад і Шамір Охад [6], КвакЕнлун, Ха Чон Гю [7], Цао Юань, Чен Цзисян, Бєлкін Михайло і Гу Цюаньцюань [8], Павлицька Світлана, Освальд Джоел і Зельнер Дж. [9], Чжу Чженьюй і Фанхуей Лю [10], Ду Ян, Шао Вей, Чай Чжен, Ханьчжан Чжао, ДяоЦих Явей, Юань Сіхуей, Ван Цяоцяо, Лі Тао, Чжан Вейдун, Чжан Цзянь і МінТай [11], Бежані Махді та Гаті Махді [12], Фіорентіні Ніколас, Пеллегріні Ділетта та Лоса Массімо [13], Лім Хен Іль [14], Хюсманн Карім, Родрігес Луїс, Лінсен Ларс та Ріссе Бенджамін [15] та інших.

Проте, беручи до уваги вище зазначену наукову документацію, питання, пов'язане з методами автоматизованого виявлення та попередження перенавчання в нейронних мережах, все ще залишається недостатньодослідженим та потребує подальшого опрацювання.

Постановка завдання.

Метою роботи є дослідження автоматизованоговиявлення та попередження перенавчання в нейронних мережах.

Викладення основного матеріалу дослідження. Враховуючи теперішній розвиток нейронних мереж, варто наголосити, що під час навчання та реалізації моделі, на вихід може впливати кілька функцій. Зі збільшенням числа ознак модель ускладнюється.

Надмірно перенавчена модель, як правило, враховує всі характеристики, навіть якщо деякі з них мають дуже обмежений вплив на кінцевий результат. Або ще гірше, деякі з них є шумами, які не реалізуються на виході. Щоб обмежити ці випадки, існує два типи рішень:

– обрати лише корисні та видалити непотрібні функції з моделі;
– звести до мінімуму ваги функцій, які мало впливають на остаточну класифікацію.

Іншими словами, необхідно обмежити дію цих непотрібних функцій. Однак не завжди відомо, які функції є неважливими, тому необхідно намагатися обмежити їх усі, мінімізуючи функцію вартості моделі. Для цього додається «мінімізуючий параметр», який називається регуляризором, до функції вартості, математична складова якого має наступний вигляд:

$$\mathcal{J}(\omega; X, y) = J(\omega; X, y) + \alpha\Omega(\omega) \quad (1)$$

$$\mathcal{J}(\omega;\, X, y) \; -\frac{1}{2\mathrm{m}} \parallel X_W - y \parallel^{2} + \alpha\Omega(\omega) \quad (2)$$

де
$J(\omega; X,y)$ – початкова функція вартості;
ω – вага;
X – навчальний набір;
y – позначене значення (дійсне значення);
m – розмір навчального набору;
α – коефіцієнт регуляризації;
$\alpha\Omega(\omega)$ – термін дії мінімізуючого параметру.

Для того, щоб встановити набір ваг необхідно використати метод «Градієнтного спуску», математично дана дія представляється у вигляді:

$$\omega^{(k+1)} = \omega^{(k)} - \alpha\frac{1}{m}\sum_{i=1}^{m}\left(p\left(x^{(i)}\right) - y^{(i)}\right)x^{(i)} - \lambda\frac{\omega^{(k)}}{m} \quad (3)$$

$$\omega^{(k+1)} = \omega^{(k)} - \left(1\frac{\lambda}{m}\right) - \alpha\frac{1}{m}\sum_{i=1}^{m}\left(p\left(x^{(i)}\right) - y^{(i)}\right)x^{(i)} \quad (4)$$

Враховуючи (2) видно, що, чим більше m, тим менше $\lambda\frac{\omega^{(k)}}{m}$. Тобто, чим більший навчальний набір, тим менший ризик перенавчання та ефекту регуляризації.

Проте, хоча регуляризація і є одним з найефективніших методів перенавчання за умови, що модель має достатньо великий і різноманітний набір даних для навчання, варто наголосити, що, у випадку невеликого набору даних або недостатньої різноманітності, регуляризація може не мати достатньо прикладів для ефективного виявлення та узагальнення шаблонів, що потенційно може призвести до перенавчання. Крім того, регуляризація призначена для пом'якшення впливу шуму та запобігання надто точномупідбору моделі до даних навчання. У наборах даних з мінімальним шумом або повною його відсутністю, максимально структурованим шаблонам регулярізація може не дати значних переваг, оскільки шум руйнує інформацію.

В результаті чого підвищується важкість навчання моделі набору даних, а отже, і важкість перенавчання. Додаючи шум, навчальний набір даних доповнюється (аугментується) додатковою інформацією. Нейронна мережа отримує повідомлення, що тип шуму, який додається, не повинен сильно змінювати її прогноз.

Було проведено симуляційне дослідження і дослідження набору даних рентгенографічного дослідження легенів у програмі САПР. Були змодельовані набори даних із двовимірною винятковою диз'юнкцією (XOR), яка вимагає нелінійної межі прийняття рішень для досягнення значення AUC (площа під ROC-кривою) більше 0,5. Це проблема, тому що теоретично вже було показано, що розпад ваги та шумова ін'єкція працюють однаково в задачах класифікації, які вимагають лінійних меж рішень.

Популяція XOR була побудована за допомогою чотирьох двовимірних розподілів Гауса з рівними коваріаційними матрицями у двовимірному просторі функцій. Два гаусових розподіли були зосереджені в (0, 0) і (x, x), відповідно, і вонипредставляли «нормальний» клас, тоді як інша пара гаусових розподілів була зосереджена в (x, 0) і (0, x), відповідно, і вони представляли «ненормальний» клас. Коваріаційна матриця кожного з чотирьох розподілів Гауса була окреслена як матриця ідентичності 2 на 2, при чому x = 2,0. Контурний графік популяції XOR показано на рисунку 1.

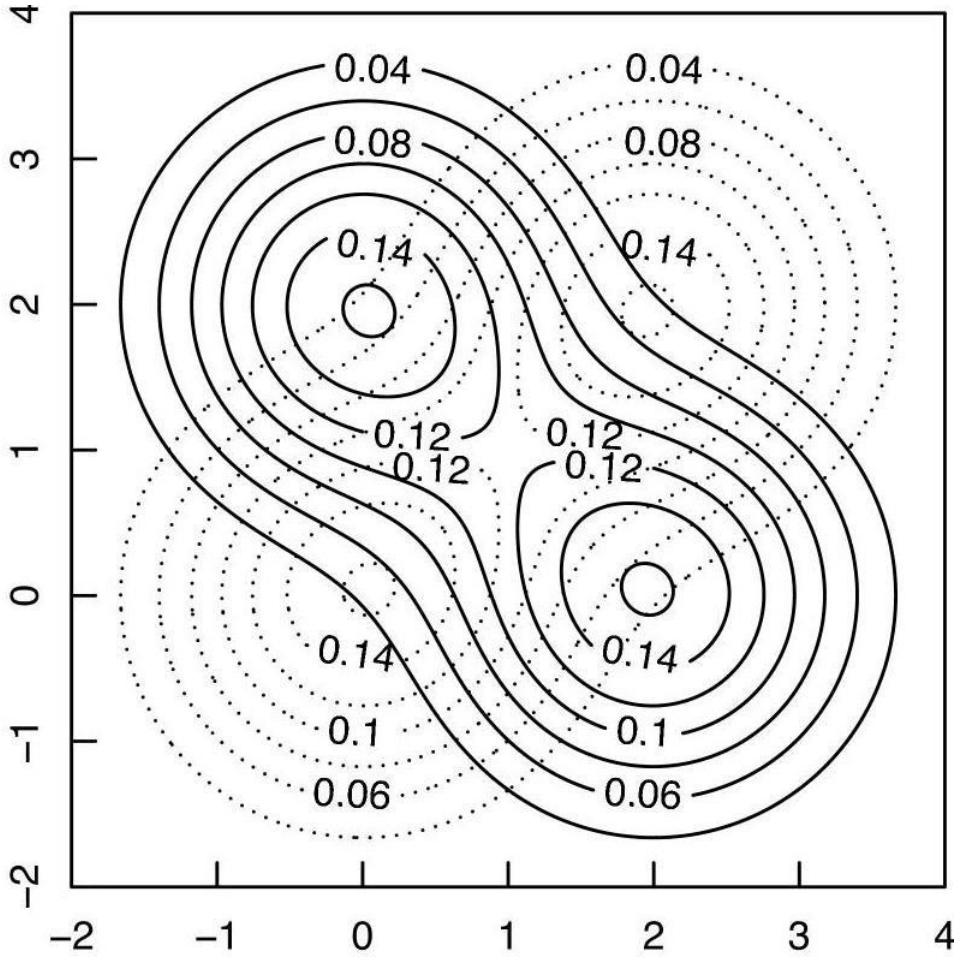

Рис. 1 – Популяція XOR

Нормальні випадки були взяті із щільностіймовірності пунктирною лінією, а аномальні випадки – із щільності ймовірності суцільною лінією.

Були створені навчальні набори даних різного розміру: 50, 100 і 200 загальних випадків, причому половина кожного набору даних є нормальними, а інша половина – ненормальними випадками. Мета полягала в тому, щоб відрізнити злоякісні ураження легенів від запальних. Набір даних містив 157 злоякісних утворень і 969 уражень внаслідок запального процесу (загалом 1126 випадків).

Штучну нейронну мережу (ШНМ) тренували шляхом мінімізації функції перехресної ентропійної помилки за допомогою алгоритму спряженого градієнта. ШНМ у першому татретьому дослідженнях моделювання мали один прихований шар із шістьма прихованими вузлами та були навчені 500 ітераціям. Завдяки дуже великим наборам навчальних даних (500, 1000 і 5000 випадків у 100 повторних експериментах) ця архітектура ШНМ змогла досягти майже ідеальної продуктивності AUC для спостерігача на наборі даних перевірки (0,81, 0,81 і 0,82 відповідно).

В якості ін'єкції було використано метод джиттеру. За допомогою цього методу вектор шуму додається до кожного випадку навчання між ітераціями навчання. Це спричиняє коливання навчальних даних у просторі функцій під час навчання, що ускладнює ШНМ пошук рішення, яке точно відповідає вихідному набору навчальних даних, і таким чином зменшує перенавчання ШНМ. Вектор шуму зазвичай складається з деякої функції щільності ймовірності, відомої як «ядро». Було використано ядро Гауса з нульовим середнім і оновлено вектор шуму незалежно та без наростання передкожною ітерацією навчання.

Оскільки на кожній ітерації навчання ШНМ помічає дещо інший набір даних навчання, спричинений доданим шумом, шумна траєкторія значення AUC ШНМ на різних ітераціях навчання відображає як поступову конвергенцію ШНМ до її кінцевої продуктивності навчання, так і ефект доданого шуму. Результати моделювання з точки зору абсолютних різниць підсумовані втаблиці 1.

Таблиця 1 – Порівняння абсолютної ефективності методів навчанняШНМ у моделювальних дослідженнях

		Без регулярізації	Ін'єкція шуму	Зниження ваги	Рання зупинка
50 навчальнихвипадків	Середня AUC [95% ДІ]	0.723 [0.719, 0.727]	0.756 [0.751, 0.758]	0.742 [0.738, 0.746]	0.740 [0.737, 0.744]
	Стандартне відхиленняAUC [95% ДІ]	0.043 [0.038, 0.048]	0.037 [0.033, 0.041]	0.050 [0.045, 0.055]	0.041 [0.035, 0.046]
50 навчальнихвипадків, комплексні ШНМ	Середня AUC [95%ДІ]	0.694 [0.685, 0.703]	0.758 [0.755, 0.761]	0.745 [0.735, 0.754]	0.748 [0.740, 0.757]
	Стандартне відхиленняAUC [95% ДІ]	0.044 [0.036, 0.052]	0.034 [0.031, 0.038]	0.048 [0.037, 0.060]	0.043 [0.032, 0.053]
100 навчальнихвипадків	Середня AUC [95% ДІ]	0.762 [0.760, 0.765]	0.785 [0.784, 0.787]	0.784 [0.782, 0.786]	0.770 [0.768, 0.772]
	Стандартне відхиленняAUC [95% ДІ]	0.028 [0.026, 0.030]	0.017 [0.016, 0.019]	0.020 [0.019, 0.022]	0.023 [0.021, 0.025]
200 навчальнихвипадків	Середня AUC [95%ДІ]	0.788 [0.785, 0.790]	0.799 [0.797, 0.801]	0.797 [0.795, 0.799]	0.790 [0.788, 0.792]
	Стандартне відхилення AUC [95% ДІ]	0.012 [0.011, 0.014]	0.009 [0.008, 0.010]	0.009 [0.007, 0.011]	0.010 [0.008, 0.011]

За допомогою методу ранньої зупинки навчання ШНМ припиняється дотого, як помилка навчання мінімізується. Як правило, незалежний тестовий набір даних використовується для моніторингу продуктивності ШНМ під часнавчання, на основі якого вибирається відповідна точка для зупинки навчанняШНМ. Однак утримання випадків навчання для тестування не є ефективним використанням даних для невеликих наборів даних навчання.

У симуляційному дослідженні ШНМ, навчені на наборах даних із 50загальними випадками та без регуляризації, мали середнє значення AUC 0,723і стандартне відхилення 0,043. Навчання ШНМ із шумовою ін'єкцією збільшило середнє значення AUC до 0,756 і зменшило стандартне відхилення до 0,037. Навчання ШНМ із зниженням ваги та ранньою зупинкою також покращило середні значення AUC до 0,742 та 0,740 відповідно, але зменшенняваги збільшило стандартне відхилення до 0,050, тоді як рання зупинка не змінила стандартне відхилення. Таким чином, навчання ШНМ із введенням шуму призвело до більшого середнього та меншого стандартного відхилення узначеннях AUC, ніж у альтернативних методах.

Зниження ваги, що є формою регулярізації, яка мінімізує параметри великих ваг (числові значення, пов'язані з вузлами на різних рівнях мережі) в мережі, також було використано у даному дослідженні. Мінімізація параметрів великих ваг здійснюється шляхом додавання до функції втрат параметра/значення, пропорційного сумі квадратів ваг. Цей термін зменшує величину ваг і запобігає їх надто великому зростанню. Модифікована функція похибки має представлення:

$$E_{WD}(\omega) = E(\omega) + \alpha \sum w_i^2,$$

де

$E(\omega)$ – функція крос-ентропійної похибки;

α – параметр, який контролює вагу мінімізації відносно великих значень ваг і використовується для навчання ШНМзі зниженням ваги, який вимагає від користувача вибору значення α.

Комплексні ШНМ мали 20 прихованих вузлів і були навчені 1500 ітераціям, тоді як усі інші ШНМ мали 6 прихованих вузлів і були навчені 500 ітераціям. Результати розраховувалися на 1485-й і 485-й ітерації навчання відповідно.

Висновки. У даній роботі було проведено комплексне дослідження, якезаглиблюється в потенціал включення шуму під час навчання штучних нейронних мереж для медичних рентгенографічних застосувань. Воно засноване на складному моделювальному аналізі в області медичного рентгенографічного дослідження та демонструє, що тренування нейронної мережі за допомогою шуму є потужною стратегією мінімізації проблеми перенавчання. Це дослідження, зокрема, перевершує ефективність звичайних методів ранньої зупинки, а в деяких випадках навіть методи зниження ваги.

Успіх, який спостерігався в дослідженнях підкреслює надійність і адаптивність навчання нейронної мережі за допомогою ін'єкції шумів. Примітно, що результати демонструють значне зменшення випадків перенавчання, позиціонуючи ін'єкцію шуму як передову методологію для підвищення продуктивності ШНМ у програмах медичної візуалізації.

Перспективами подальших досліджень є розробка більш ефективної методології по виявленню та попередженню перенавчання в нейронних мережах.

Список бібліографічного опису

1. Muquri A. L. I., Konstholm S. Data augmentation and related opportunity cost for managing the contemporary data sparsity data augmentation and related opportunity cost for managing the contemporary data sparsity. 2021.
2. Khalifa N. E., Hamed Taha M., Hassanien A. E., Selim I. Deep galaxy V2: Robust deep convolutional neural networks for galaxy morphology classi cations. *Int. Conf. Comput. Sci. Eng. ICCSE 2018* – Proc., 2018. P. 1–6. DOI:10.1109/ICCSE1.2018.8374210.
3. Marin I., Skelin A. K., Grujic T. Empirical evaluation of the effect of optimization and regularization techniques on the generalization performance of deep convolutional neural network. *Appl. Sci.* 2020. vol. 10, №. 21. P. 1–30. DOI:10.3390/app10217817.
4. Kadhim Zahraa, Abdullah Hasanen, Ghathwan Khalil. Automatically Avoiding Overfitting in Deep Neural Networks by Using Hyper-Parameters Optimization Methods. *International Journal of Online and Biomedical Engineering (iJOE)*. 2023. DOI:19. 146-162. 10.3991/ijoe.v19i05.38153.
5. Sabiri Bihi, Asri Bouchra, Rhanoui Maryem. Efficient Deep Neural Network Training Techniques for Overfitting Avoidance. 2023. DOI:10.1007/978-3-031-39386-0_10.
6. Kornowski Guy, Yehudai Gilad, Shamir Ohad. From Tempered to Benign Overfitting in ReLU Neural Networks.

2023.

References

7. Kwak Yeonglong, Huh Jeong-gyu. Random AugmentationTechnique for Mitigating Overfitting in Neural Networks for Financial Time Series Forecasting. *The Korean Data Analysis Socie*ty. 2023. № 25. P. 1653-1669. DOI: 10.37727/jkdas.2023.25.5.1653.
8. Cao Yuan, Chen, Zixiang, Belkin Mikhail, Gu Quanquan. Benign Overfitting in Two-layer Convolutional Neural Networks. 2022.
9. Pavlitskaya Svetlana, Oswald Joël, Zöllner J. Measuring Overfitting in Convolutional Neural Networks using Adversarial Perturbations and Label Noise. 2022. DOI:10.48550/arXiv.2209.13382.
10. Zhu Zhenyu, Fanghui Liu, Chrysos Grigorios, Locatello Francesco, Cevher Volkan. Benign Overfitting in Deep Neural Networks under Lazy Training. 2023.
11. Du Yan, Shao Wei, Chai Zheng, Hanzhang Zhao, Diao Qihui, Gao Yawei, Yuan Xihui, Wang, Qiaoqiao, Li Tao, Zhang Weidong, Zhang Jian, Min Tai.Synaptic 1/f noise injection for overfitting suppression in hardware neural networks. *Neuromorphic Computing and Engineering*. 2022. №2. DOI:10.1088/2634-4386/ac6d05.
12. Bejani Mahdi, Ghatee Mehdi. A systematic review on overfitting control in shallow and deep neural networks. *Artificial Intelligence Review*. 2021. №54. DOI:1-48. 10.1007/s10462-021-09975-1.
13. Fiorentini Nicholas, Pellegrini Diletta, Losa Massimo. Overfitting Prevention in Accident Prediction Models: Bayesian Regularization of Artificial Neural Networks. *Transportation Research Record Journal of the Transportation Research Board*. 2022. P. 26-77. DOI: 10.1177/03611981221111367.
14. Lim Hyun-il. A Study on Dropout Techniques to Reduce Overfitting in Deep Neural Networks. 2021. DOI:10.1007/978-981-15-9309-3_20.
15. Huesmann Karim, Rodriguez Luis, Linsen Lars, Risse Benjamin. The Impact of Activation Sparsity on Overfitting in Convolutional Neural Networks. 2021. DOI:10.1007/978-3-030-68796-0_10.