Белорусский государственный университет
Научно-исследовательский институт
прикладных проблем математики и информатики

# О ПОДХОДАХ К РЕШЕНИЮ ЗАДАЧ КРИПТОЛОГИИ НА ОСНОВЕ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ И МАШИННОГО ОБУЧЕНИЯ

Мальцев Михаил Владимирович
Харин Юрий Семенович
maltsew@bsu.by kharin@bsu.by

2022

# Введение

Машинное обучение (machine learning) – сравнительно молодое направление анализа данных, включающее в себя методы и алгоритмы, которые позволяют автоматически выявлять закономерности в данных и затем использовать обнаруженные закономерности для решения различных задач: прогнозирования, классификации и кластеризации, обнаружения аномалий и т.д.

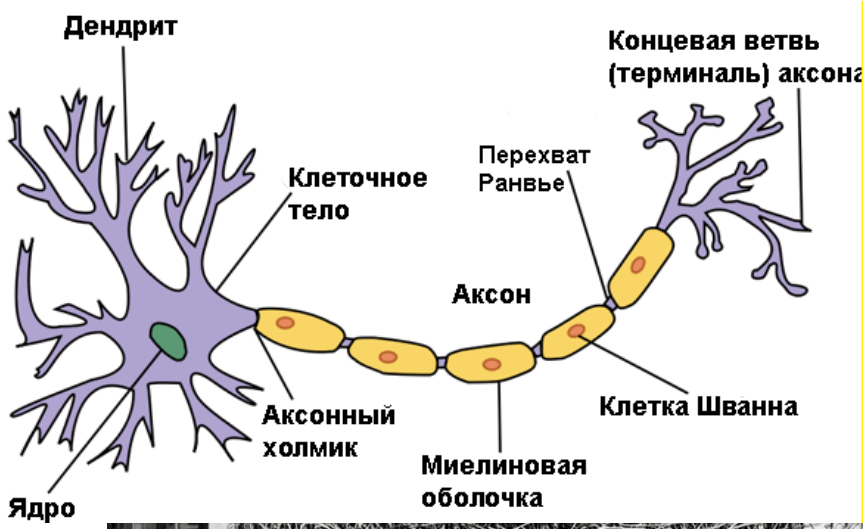
Одним из наиболее перспективных и активно развивающихся методов машинного обучения являются искусственные нейронные сети (ИНС). Применение ИНС позволило значительно улучшить качество распознавания речи и изображений, существенно продвинуться в ряде задач биоинформатики, создать системы искусственного интеллекта, способные на сопоставимом с человеком уровне управлять автомобилем и играть в интеллектуальные игры.

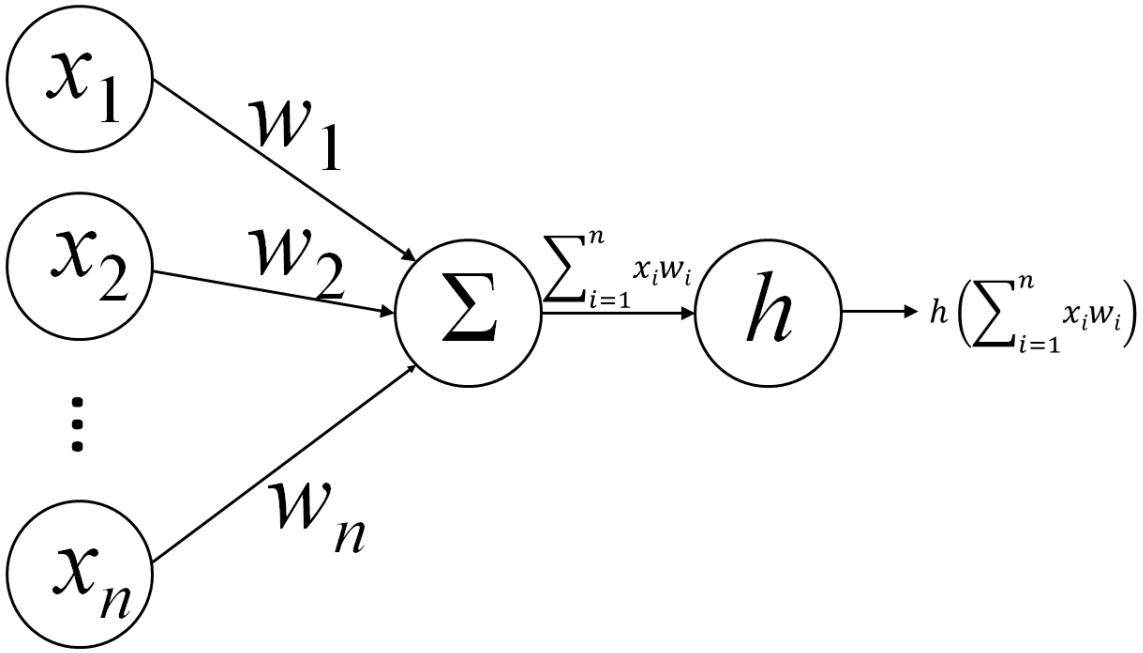
Закономерно, что интерес к ИНС как к эффективному инструменту решения самых разнообразных задач появился и в криптографическом сообществе.

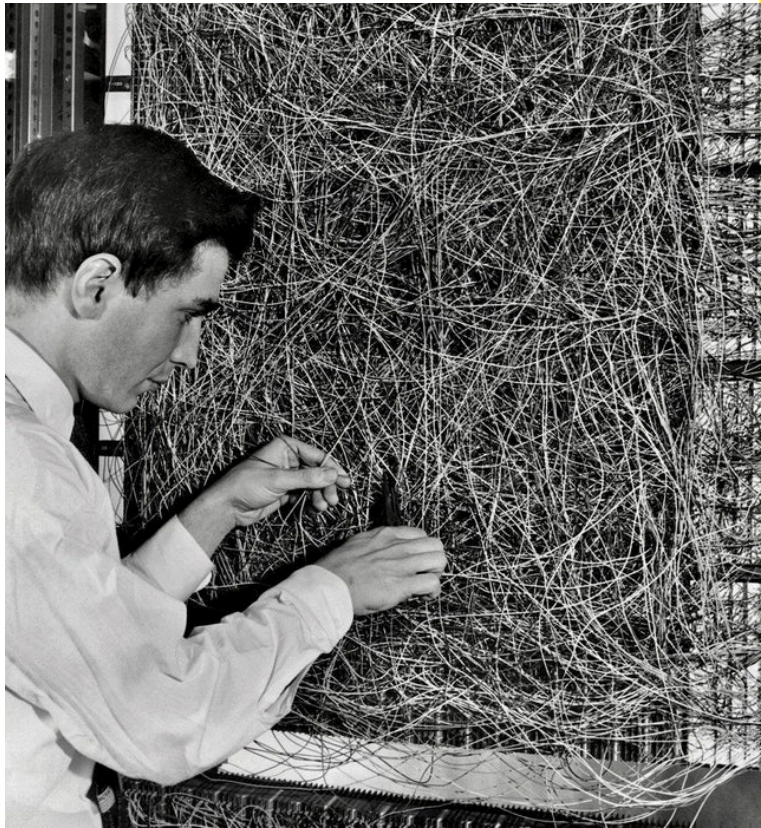
# Задачи машинного обучения

# Искусственные нейронные сети: основные понятия

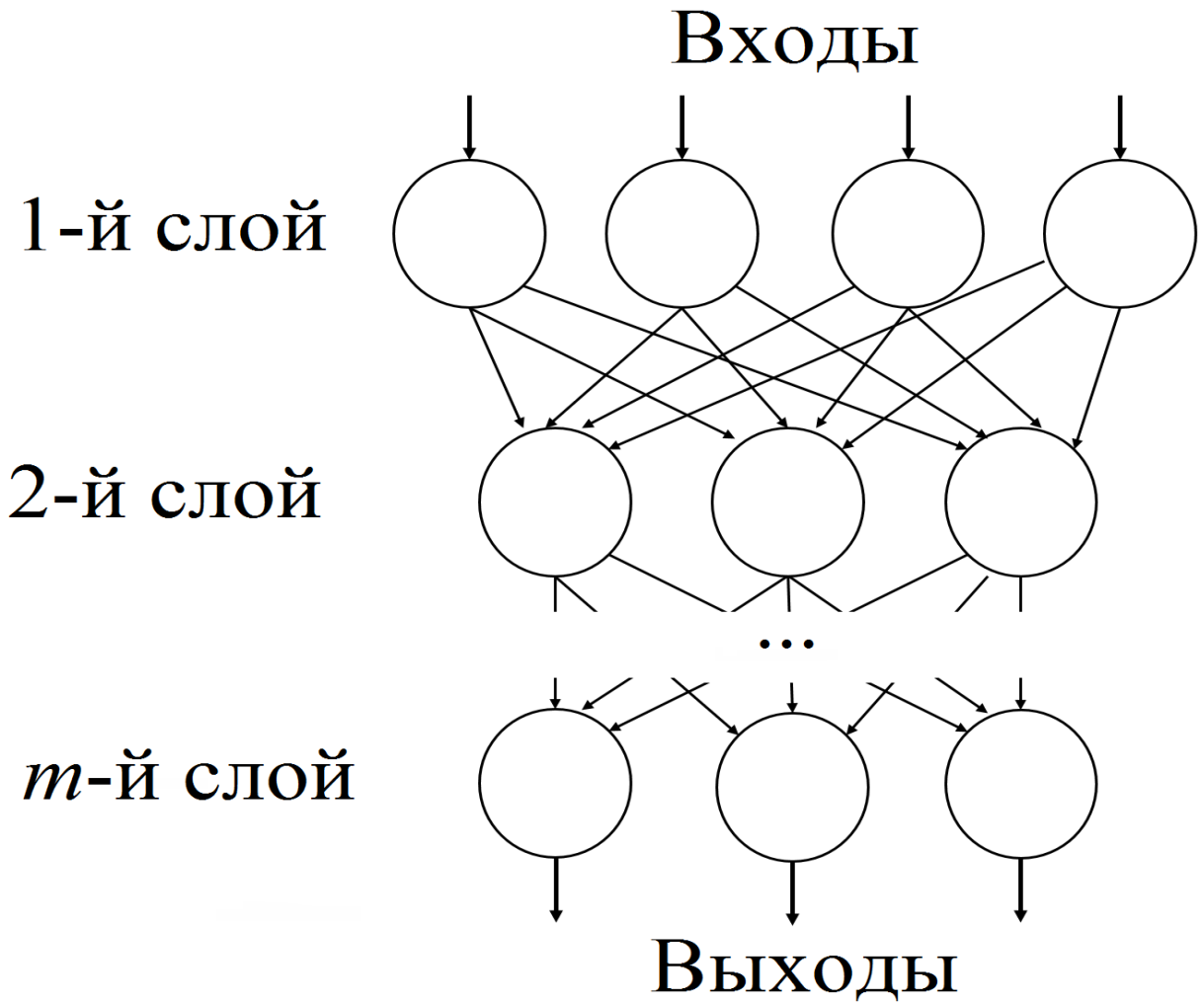
Идея искусственных нейронных сетей состоит в моделировании работы человеческого мозга, состоящего из множества взаимодействующих между собой нервных клеток – нейронов. Моделируя эту структуру, американский ученый Фрэнк Розенблатт в 1950-х годах предложил конструкцию перцептрона.



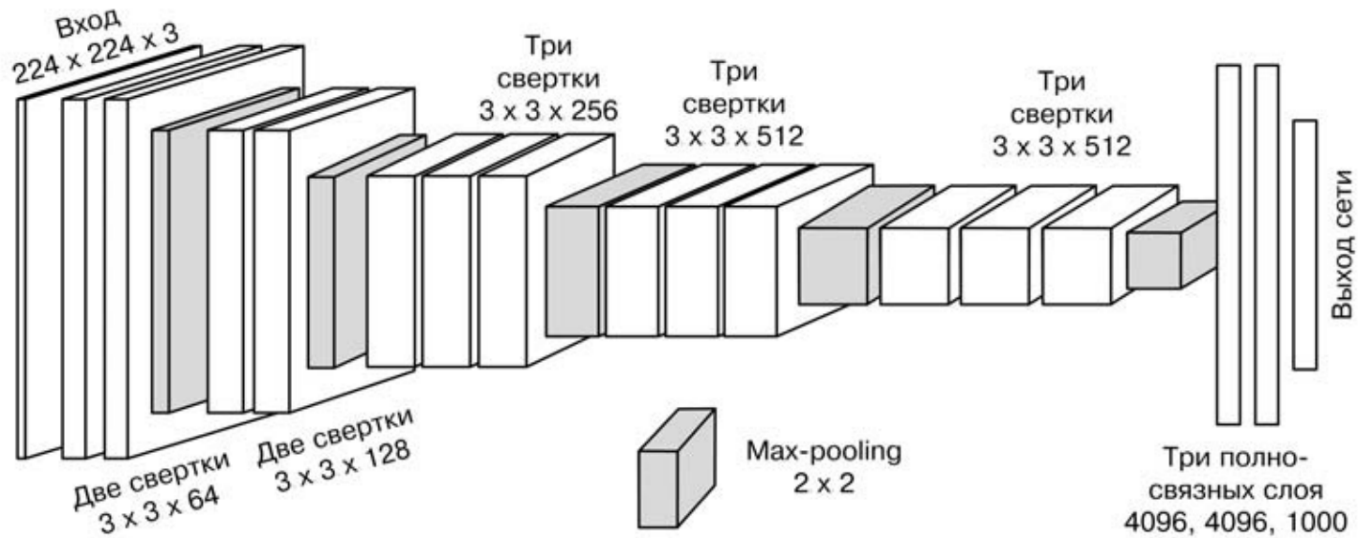



# Искусственные нейронные сети: основные понятия



# Примеры архитектур ИНС

- Сверточные ИНС (convolutional neural network, CNN) состоят из чередующихся слоев двух типов: сверточных (convolution) и субдискретизирующих (pooling). Сверточные ИНС широко применяются для распознавания изображений.
- В рекуррентных ИНС (recurrent neural network, RNN) связи между элементами образуют направленную последовательность, вследствие чего появляется возможность обрабатывать серии событий во времени или последовательные пространственные цепочки. Такие сети используются для распознавания рукописного текста, распознавания речи.
- Генеративно-состязательные ИНС (generative adversarial network, GAN)состоят из двух подсетей: генератора и дискриминатора. Генератор порождает объекты, принадлежащие различным классам, а дискриминатор пытается отличать объекты из разных классов. Применяются такие сети, например, для генерации и улучшения качества изображений.



# Применение машинного обучения в криптологии

Первые идеи применять машинное обучение
в криптологии – 90е гг. XX в.

Ronald L Rivest. Cryptography and machine learning.
In International Conference on the Theory and
Application of Cryptology, 1991

# Нейронные сети в биометрической идентификации и аутентификации

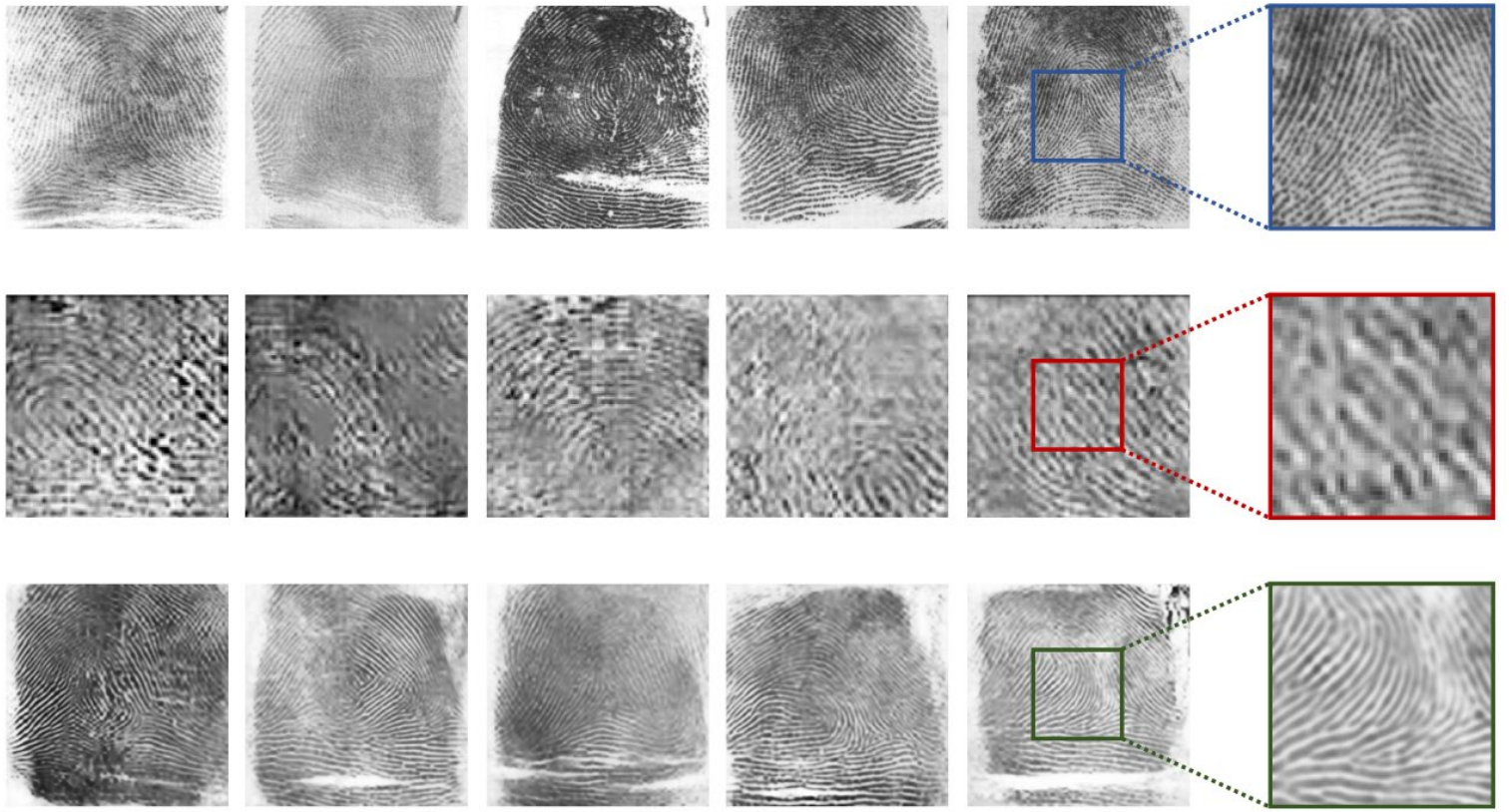
Важной практической задачей, решаемой с помощью искусственных нейронных сетей является классификация. В связи с этим значительное число публикаций посвящено применению нейронных сетей для построения систем идентификации и аутентификации, использующих биометрические характеристики: отпечатки пальцев, изображения лица, радужную оболочку глаза, почерк и др.


Rathgeb, C. A survey on biometric cryptosystems and cancelable biometrics / C. Rathgeb, A. Uhl // EURASIP Journal on Info. Security, № 3, 2011.

Tarek, M. Robust cancellable biometrics scheme based on neural networks / M.Tarek, O.Ouda, T.Hamza // IET Biometrics, № 5. – 2016.

Albakri, A. Convolutional neural network biometric cryptosystem for the protection of the blockchain's private key / A.Albakri, C.Mokbel // Procedia Computer Science, Vol. 160. – 2019.

Riazi,M. Automatic Synthetic Fingerprint Generation / M.Riazi, S. Chavoshian, F.Koushanfar . – 2020. – arXiv:2002.08900.

# Атаки по сторонним каналам (side-channel attacks)

Timo Bartkewitz. Leakage prototype learning for profiled differential side-channel cryptanalysis. IEEE Transactions on Computers, 65(6), 2015.

Richard Gilmore, Neil Hanley, and Maire O'Neill. Neural network based attack on a masked implementation of AES. 2015 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), 2015.

Maghrebi, Houssem & Portigliatti, Thibault & Prouff, Emmanuel. (2016). Breaking Cryptographic Implementations Using Deep Learning Techniques. 3-26. 10.1007/978-3-319-49445-6_1.

Benjamin Timon. Non-profiled deep learning-based side-channel attacks. IACR Cryptology, ePrint Archive, 2018: 196, 2018.

# Обнаружение вторжений


- Z. Yu and J. J. Tsai, A framework of machine learning based intrusion detection for wireless sensor networks. Sensor Networks, Ubiquitous and Trustworthy Computing, 2008. SUTC'08. IEEE International Conference on. P. 272–279, IEEE, 2008.
- X. Xu. Adaptive intrusion detection based on machine learning: feature extraction, classifier construction and sequential pattern prediction. International Journal of Web Services Practices, vol. 2, no. 1-2, pp. 49–58, 2006.
- A. A. Alsadhan and M. M. A. Alani. Detecting ndp distributed denial of service attacks using machine learning algorithm based on flow-based representation. Developments in eSystems Engineering (DeSE), 2018. Eleventh International Conference on, IEEE, 2018.

# Синтез криптосистем на основе нейронных сетей

Поточные шифры:

Long, H. Stream Cipher Method Based on Neural Network / H.Long // Proceedings of the 2012 National Conference on Information Technology and Computer Science, CITCS. – 2012

Блочные шифры:

Lian, S. A block cipher based on chaotic neural networks / S. Lian // Neurocomputing, Vol. 72. – 2009

V. Sagar and K. Kumar. A symmetric key cryptographic algorithm using counter propagation network (cpn). Proceedings of the 2014 International Conference on Information and Communication Technology for Competitive Strategies, p. 51, ACM, 2014

Функция хэширования:

S.Lian, J.Sun, Z. Wang One-way Hash Function Based on Neural Network. – arXiv:0707.4032

# Криптоанализ с использованием нейронных сетей

Albassal, A.M.B. Neural network based cryptanalysis of a Feistel type block cipher / A. M. B. Albassal, A. M. A. Wahdan // International Conference on Electrical, Electronic and Computer Engineering, 2004. ICEEC '04. – 2004. – P. 231–237.

Chou, J. On the eectiveness of using state-of-the-art machine learning techniques to launch cryptographic distinguishing attacks / J. Chou, S. Lin, C. Cheng // Proceedings of the 5th ACM workshop on Security and articial intelligence, ACM. – 2012. – P 105–110

Jan Wabbersen. Cryptanalysis of block ciphers using feedforward neural networks. Georg-August-Universitat Gottingen, 2019.

Aron Gohr. Improving attacks on Speck32/64 using deep learning. IACR Cryptology ePrint Archive, 2019:37, 2019

Alani, M.M. Neuro-cryptanalysis of DES and triple-DES / M.M.Alani // Int. Conf. on Neural information processing. – N.Y.: Springer, 2012. – P.637-646.

# Анализ трафика

R. Alshammari and A. N. Zincir-Heywood. Machine learning based encrypted traffic classification: Identifying ssh and skype. Computational Intelligence for Security and Defense Applications, 2009. CISDA 2009. IEEE Symposium on, pp. 1–8, IEEE, 2009.

M. Conti, L. V. Mancini, R. Spolaor, N. V. Verde, Analyzing android encrypted network traffic to identify user actions // IEEE Transactions on Information Forensics and Security, vol. 11, no. 1, pp. 114– 125, 2016.

| Apps | Actions | Description | Precision | Recall | F-measure |
|---|---|---|---|---|---|
| Facebook | *send message* | send a direct message to a friend | 1.00 | 1.00 | 1.00 |
| | *post user status* | post a status on the user's wall | 1.00 | 0.95 | 0.97 |
| | *open user profile* | select user profile page from menu | 0.96 | 0.91 | 0.94 |
| | *open message* | select a conversation on messages | 0.98 | 1.00 | 0.99 |
| | *status button* | select "*write a post*" on user's wall | 1.00 | 1.00 | 1.00 |
| | *post on wall* | post a message on a friend's wall | 1.00 | 0.98 | 0.99 |
| | *open facebook* | open the Facebook app | 1.00 | 1.00 | 1.00 |
| | *other facebook* | other Facebook network traffic | 0.99 | 1.00 | 0.99 |
| | Average Facebook | | 0.99 | 0.98 | 0.99 |

# Стеганография

- Yinlong Qian, Jing Dong, Wei Wang, and Tieniu Tan. Deep learning for steganalysis via convolutional neural networks.– SPIE/IS&T Electronic Imaging, P 94090J–94090J. International Society for Optics and Photonics, 2015.
- Robert Jarušek, Eva Volna, and Martin Kotyrba. Neural network approach to image steganography techniques. In Mendel 2015, pages 317–327. Springer, 2015.
- Shumeet Baluja. Hiding images in plain sight: Deep steganography. In I. Guyon, U. V. Luxburg, S. Bengio, H. Wallach, R. Fergus, S. Vishwanathan, and R. Garnett, editors, Advances in Neural Information Processing Systems 30, pages 2069– 2079. Curran Associates, Inc., 2017.

В [Baluja] построены две глубокие ИНС для встраивания одного цветного изображения – секрета *S* в другое – контейнер *C* и последующего извлечения *S* из *C*, изображения *S* и *C* при этом имеют одинаковый размер.

$C$

$S$

$C'$

$S'$

Спасибо за внимание!