**Лаба 1**

**ФИО**

Голунов Егор Владиславович, Петров Вадим Сергеевич (гр. 6114-100503D)

**Topic**

Fragile Watermarking; Image Authentication; Hashing

**Описание предметной области**

Цифровой водяной знак (digital watermark), (ЦВЗ) - это специальная метка, встраиваемая в цифровой контент, называемый контейнером с целью защиты авторских прав и подтверждения целостности самого документа. Наряду с различными изображениями (фотографиями, рисунками, отсканированными бумажными документами и т.д.) встречаются и аудиозаписи, несущие внутри себя ЦВЗ, и видео (например, DVD-диски). ЦВЗ активно используются при размещении уникальных фотографий, видео, аудиотреков в электронном виде в глобальной сети Интернет.

**Недостаток**

Недостатки научной проработки в области Fragile Watermarking, Image Authentication и Hashing включают недостаточную эффективность алгоритмов при высокой степени компрессии изображений, недостаточную устойчивость к различным типам атак, таким как геометрические и цифровые атаки. Требуется более глубокое изучение, чтобы разработать алгоритмы, которые обеспечивают высокую степень защиты и надежности в различных условиях использования.

**Идея**

Мы предполагаем использовать сверточные нейронные сети для создания эффективного механизма внедрения и аутентификации цифровых водяных знаков, что позволит минимизировать ложноположительные и ложноотрицательные результаты. В ходе исследования планируется обширное тестирование предложенного метода на различных наборах изображений с различными типами атак для демонстрации его эффективности и применимости в реальных сценариях использования, таких как цифровая аутентификация изображений и защита от подделок. Нейросетевой подход может позволить создавать как надежные, так и незаметные цифровые водяные знаки.

**Краткий текст обзора**

Концепция Fragile Watermarking в области изображений предполагает внедрение уникальных меток или цифровых подписей в изображения с такой чувствительностью, что они становятся неустойчивыми к любым изменениям или манипуляциям.[[1]](https://www.zotero.org/google-docs/?UsoC0s) Эти метки служат для аутентификации изображений и обеспечивают возможность обнаружения любых даже минимальных изменений, таких как редактирование, ретушь или вставка. Fragile watermarking может использоваться в различных областях, включая цифровую фотографию, медицинскую диагностику (например, для обеспечения целостности медицинских изображений), судебно-следственную экспертизу, охрану авторских прав и обеспечение целостности документов и изображений в цифровых системах. Этот метод имеет важное значение там, где обеспечение неподдельности и целостности изображений играет ключевую роль.

Сейчас в подавляющем большинстве случаев используются алгоритмы, которые могут быть несовершенными, т.е. давать ложноположительные или ложноотрицательные результаты[[2]](https://www.zotero.org/google-docs/?f6IK8g), быть неустойчивыми к разным типам атак[[3]](https://www.zotero.org/google-docs/?fdwAS8). Кроме того, сравнительные тесты ([[1], [4], [5]](https://www.zotero.org/google-docs/?LPSAvC)) показывают, что алгоритмы бывают либо надежные, либо дают невидимые водяные знаки, почти незаметные как для человеческого глаза, так и для машины. Создание алгоритма, который будет одновременно и надежным и незаметным практически невозможно.[[6]](https://www.zotero.org/google-docs/?4bXE7w)

Решением указанных выше проблем может быть применение сверточных нейронных сетей для создания цифровых водяных знаков. Такой подход позволит объединить преимущества алгоритмического подхода, исключив его недостатки, такие как низкая скорость работы, заметность водяных знаков, высокая степень компрессии изображения, ненадежность (неустойчивость к различным атакам[[6]](https://www.zotero.org/google-docs/?dwsf5x)).

**References**

[[1] N. R. N. Raj и R. Shreelekshmi, «A survey on fragile watermarking based image authentication schemes», *Multimed. Tools Appl.*, т. 80, вып. 13, сс. 19307–19333, май 2021, doi: 10.1007/s11042-021-10664-y.](https://www.zotero.org/google-docs/?uPHnKv)

[[2] E. Gul и S. Ozturk, «A novel hash function based fragile watermarking method for image integrity», *Multimed. Tools Appl.*, т. 78, вып. 13, сс. 17701–17718, июл. 2019, doi: 10.1007/s11042-018-7084-0.](https://www.zotero.org/google-docs/?uPHnKv)

[[3] M. Li, D. Xiao, и Y. Zhang, «Attack and Improvement of the Fidelity Preserved Fragile Watermarking of Digital Images», *Arab. J. Sci. Eng.*, т. 41, вып. 3, сс. 941–950, мар. 2016, doi: 10.1007/s13369-015-1941-1.](https://www.zotero.org/google-docs/?uPHnKv)

[[4] K. Sreenivas и V. Kamkshi Prasad, «Fragile watermarking schemes for image authentication: a survey», *Int. J. Mach. Learn. Cybern.*, т. 9, вып. 7, сс. 1193–1218, июл. 2018, doi: 10.1007/s13042-017-0641-4.](https://www.zotero.org/google-docs/?uPHnKv)

[[5] X. Yu, C. Wang, и X. Zhou, «Review on Semi-Fragile Watermarking Algorithms for Content Authentication of Digital Images», *Future Internet*, т. 9, вып. 4, с. 56, сен. 2017, doi: 10.3390/fi9040056.](https://www.zotero.org/google-docs/?uPHnKv)

[[6] S.-H. Han и C.-H. Chu, «Content-based image authentication: current status, issues, and challenges», *Int. J. Inf. Secur.*, т. 9, вып. 1, сс. 19–32, фев. 2010, doi: 10.1007/s10207-009-0093-2.](https://www.zotero.org/google-docs/?uPHnKv)