УДК 004.056
doi: 10.26583/bit.2024.4.09

Данил А. Шиняев[1], Леонид Н. Кессаринский[2], Егор А. Симахин[3]
[1,2,3]Национальный исследовательский ядерный университет «МИФИ», Каширское ш., 31, Москва, 115409, Россия
[1]ООО «ИРМ», Профсоюзная ул., 25А, Москва, 117418, Россия
[1]e-mail: DAShinyaev@mephi.ru, https://orcid.org/0009-0001-6599-4670
[2]e-mail: LNKessarinskiy@mephi.ru, https://orcid.org/0000-0001-7756-6166
[3]e-mail: EASimakhin@mephi.ru, https://orcid.org/0000-0003-4019-9694

ВЫЧИСЛИТЕЛЬНЫЕ МЕТОДЫ И ТЕХНИЧЕСКИЕ СРЕДСТВА ОБРАБОТКИ СИГНАЛОВ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ

Аннотация. Цель данной работы заключается в разработке метода повышения качества восстановленного изображения на основе сигналов побочных электромагнитных полей с помощью постобработки изображений. В работе рассмотрена проблема анализа побочного электромагнитного излучения (ПЭМИ) от видеодисплеев и пути её решения. Проведен анализ непреднамеренного излучения электромагнитных волн от кабелей передачи информации, включая видеоинтерфейс HDMI. Вследствие 10-битного помехоустойчивого кодирования видеоинформации для цифровых интерфейсов передачи данных анализ сигналов и восстановление изображения по нему наиболее затруднительны. Данное кодирование расширяет полосу пропускания для ПЭМИ и приводит к нелинейному отображению наблюдаемого сигнала и уменьшению интенсивности излучения от пикселей дисплея. Поэтому программно-аппаратные комплексы для анализа аналоговых интерфейсов получают нечеткие восстановленные изображения при анализе цифровых интерфейсов. Предлагаемое решение заключается в преобразовании восстановленного изображения в исходное с помощью обучения модели на сверточной нейронной сети. Несмотря на эффективность, данный подход требует тщательного математического анализа ПЭМИ. Разработан комплекс для проведения экспериментов, основанный на доступном программно-определяемом радиоустройстве. Основным критерием эффективности восстановления и улучшения изображения после принятия приемником побочных электромагнитных сигналов является частота символьных ошибок. Данный показатель уменьшен на 60% по сравнению с восстановлением изображения без постобработки. Для оценки сбоеустойчивости предложены методы, позволяющие уменьшить вероятность восстановления изображения с помощью описанного комплекса и других аналогов. Полученные результаты имеют практическое значение для лабораторных исследований, направленных на оценку защищенности данных в различных системах общего назначения. В будущих исследованиях планируется обучить модель на обновленном наборе данных с другими аналогами нейронных сетей, чтобы оптимизировать процесс прогнозирования переменных в регрессионной модели.

Ключевые слова: вычислительные системы и их элементы, информационная безопасность, побочное электромагнитное излучение, видеоинтерфейсы, программно-определяемые радиоустройства, сверточные нейронные сети, регуляризация.

Для цитирования: ШИНЯЕВ, Данил А.; КЕССАРИНСКИЙ, Леонид Н.; СИМАХИН, Егор А. ВЫЧИСЛИТЕЛЬНЫЕ МЕТОДЫ И ТЕХНИЧЕСКИЕ СРЕДСТВА ОБРАБОТКИ СИГНАЛОВ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ. Безопасность информационных технологий, [S.l.], т. 31, № 4, с. 128–140, 2024. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1721. DOI: http://dx.doi.org/10.26583/bit.2024.4.09.

Danil A. Shinyaev[1], Leonid N. Kessarinskiy[2], Egor A. Simakhin[3]
[1,2,3]National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Kashirskoe shosse, 31, Moscow, 115409, Russia
[1]LLC «IDM», Profsoyuznaya str., 25A, Moscow, 117418, Russia
[1]e-mail: DAShinyaev@mephi.ru, https://orcid.org/0009-0001-6599-4670
[2]e-mail: LNKessarinskiy@mephi.ru, https://orcid.org/0000-0001-7756-6166
[3]e-mail: EASimakhin@mephi.ru, https://orcid.org/0000-0003-4019-9694

Computational methods and technical means of processing signals of side electromagnetic emanation

Abstract. The aim of this work is to develop a method to improve the quality of the reconstructed image based on the signals of side electromagnetic fields using post-image processing. To do this, the paper considers the problem of analyzing the side electromagnetic radiation from video displays and ways to solve it. The analysis of the side radiation of electromagnetic waves from information transmission cables, including the HDMI video interface, has been carried out. Due to the 10-bit noise-resistant encoding of video information for digital data transmission interfaces, signal analysis and image restoration are most difficult. Since this encoding expands the bandwidth for side electromagnetic radiation and leads to a nonlinear display of the observed signal and a decrease in the intensity of radiation from the display pixels. Therefore, hardware and software complexes for analyzing analog interfaces receive fuzzy reconstructed images when analyzing digital interfaces. The proposed solution to the problem is to transform the reconstructed image into the original one by training the model on a convolutional neural network. Despite its effectiveness, this approach requires careful mathematical analysis of spurious emissions. This paper will consider this aspect. The complex for conducting experiments is based on an accessible software-defined radio device. The main criterion for the effectiveness of image restoration and improvement after receiving side electromagnetic signals is the Char Error Rate. This indicator has been reduced by more than 60% compared to image restoration without post-processing. To assess fault tolerance, methods are proposed to reduce the probability of image restoration using the complexes described analogues. The results obtained are of practical importance for laboratory studies aimed at assessing data security in various general-purpose systems. In future studies, it is planned to train the model on an updated dataset with other neural network analogues in order to optimize the process of predicting variables in the regression model.
Keywords: computing systems and their elements, information security, side electromagnetic radiation, video interface, software-defined radio devices, convolutional neural networks, regularization.
For citation: SHINYAEV, Danil A.; KESSARINSKIY, Leonid N.; SIMAKHIN, Egor A. Computational methods and technical means of processing signals of side electromagnetic emanation. IT Security (Russia), [S.l.], v. 31, no. 4, p. 128–140, 2024. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1721. DOI: http://dx.doi.org/10.26583/bit.2024.4.09.

Введение

Развитие технологий программно-определяемых радиоприемников (SDR) и методов анализа ПЭМИ [1, 2] открыло новые возможности для обработки информации с электронных устройств. В настоящее время все больше внимания уделяется разработке систем, способных извлекать изображения с экранов мониторов [3], телефонов [4] и веб-камер [5] с помощью анализа ПЭМИ.

Существующие исследования в области ПЭМИ демонстрируют успехи в анализе информации с использованием традиционных методов обработки сигналов для видеоинтерфейсов DVI [6], HDMI [7], DisplayPort [8, 9]. Однако, с появлением нейронных сетей, в частности, сверточных нейронных сетей (CNN) [10], открываются новые перспективы для повышения точности и эффективности анализа данных, полученных с помощью SDR-приемников [11].

Несмотря на значительный прогресс, ряд ключевых вопросов, связанных с качеством восстановленного изображения и его точностью остается нерешенным [12, 13]. Необходимо совершенствовать алгоритмы обработки изображений, восстановленных по электромагнитным утечкам, чтобы повысить их качество и свести к минимуму влияние помех. Кроме того, требуется исследовать возможности применения различных архитектур CNN: DRUNet[10], ResNet [14], UNet [15] для оптимизации процесса извлечения информации из электромагнитных сигналов.

Целью данного исследования является улучшение качества восстановления информации с дисплеев видеомониторов с использованием программно-аппаратного комплекса (ПАК) из SDR-приемника и математического программного обеспечения, также оценка потенциала применения CNN для улучшения качества обработки изображений, полученных с помощью побочных электромагнитных утечек. В рамках исследования будут рассмотрены преимущества и недостатки различных архитектур CNN и определены оптимальные параметры для достижения максимальной точности и эффективности восстановления информации.

В современных исследованиях все методы борьбы с шумом при обработке сигналов используют фильтры низких частот и демодуляцию сигналов [2] без последующей обработки восстановленного изображения. Поскольку мощность побочных электромагнитных волн мала, то методы и инструменты для обработки сигналов требуют значительных ресурсов. Уменьшение стоимости комплекса возможно при применении SDR [12]. Для решения проблемы зашумленности восстановленного изображения предлагается метод обработки сигналов на основе глубокого обучения. Алгоритм глубокого обучения направлен на удаление шума из восстановленного изображения для улучшения распознавания текста. Метод обучения с использованием CNN доказал свою эффективность в снижении шума сложных изображений в других сферах, например, в обработке спутниковых снимков [15].

Для успешного проведения анализа ПЭМИ необходимо провести большую часть подготовительных работ:

1) Провести анализ характеристик ПЭМИ линий передачи информации и анализ излучения интерфейсов передачи данных LCD-монитора. По полученному анализу сформировать критерии поиска информативного сигнала на определенных частотах гармоник.

2) Сформировать математические требования к ПАК, необходимые для цифровой обработки сигнала на выбранных частотах гармоник и при заданных значениях разрешения изображения анализируемого монитора в реальном времени.

3) Провести анализ существующих ПАК и сформировать оптимальный комплект для решения задачи восстановления изображения с дисплея монитора в реальном времени по его ПЭМИ.

4) Разработать методику восстановления информации по полезному сигналу при помощи сформированного ПАК для различных частот и параметров изображения, создаваемого на анализируемом мониторе в реальном времени и реализовать методику в программном обеспечении.

5) Провести эксперименты и оптимизировать ПАК с помощью постобработки полученных изображений.

6) Предложить меры противодействия данного анализа и проанализировать их пригодность.

Подробное описание данных этапов работы представлено в разделах данной статьи.

1. Анализ характеристик и формирование математических требований к ПАК

Для анализа изображений жидкокристаллического(ЖК) монитора с разрешением не выше 1920×1080 пикселей и частотой обновления кадров 60 Гц по интерфейсам TMDS, LVDS, VGA, HDMI, Display Port нижняя граница анализируемых частот формируется из нижней частоты интерфейса TMDS, как наиболее медленного интерфейса, и соответствует 74,25 МГц. Исходя из ширины полезного сигнала, анализируемого от TMDS (рис. 1), можно сказать, что начало интервала анализируемых частот с учетом погрешности приемника должно находиться на 70 МГц. По теореме Котельникова (Найквиста-Шеннона) для сигналов, состоящих из последовательности дискретных отсчетов, точное восстановление непрерывного сигнала возможно при частоте дискретизации (sample rate) приемного устройства отличающейся не менее чем в 2 раза от максимальной частоты анализируемого сигнала. Верхняя частота анализируемого диапазона задается частотой работы интерфейса HDMI:

$$f_s = \frac{1}{t_s} = x_t y_t f_v n_b. \quad (1)$$

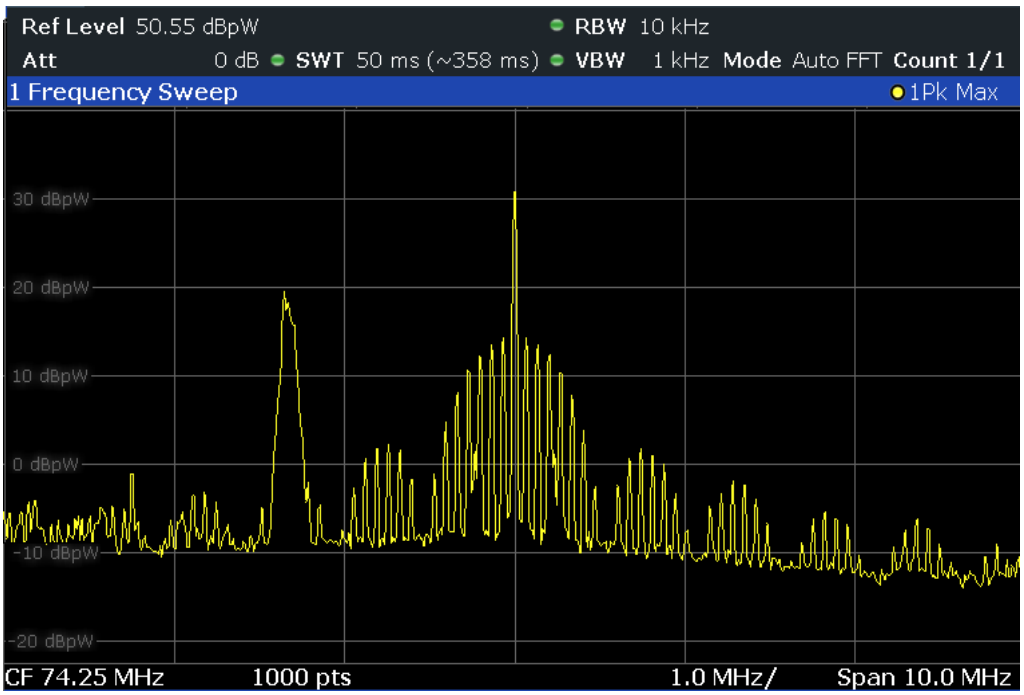

Рис. 1. Спектр информативного сигнала TMDS на частоте 74,5 МГц

В соответствии со стандартом VESA-DMT v1.0, rev.13 кадр содержит в себе горизонтальное и вертикальное гашение, при котором картинка не передается. В течение этих периодов вместо изображения происходят периоды управления и передачи данных. Это означает, что количество пикселей в кадре на самом деле выше, чем на изображении. Например, для популярного «FullHD» видеорежима 1920x1080: $x_t = 2200$ пикселей, $y_t = 1125$ линий (определяются стандартом VESA), $n_b = 10$ – количество бит, определяющих цвет пикселя, частота монитора $f_v = 60$Гц и рассчитанная для HDMI частота:

$$\frac{1}{t_s} = 2200 \times 1125 \times 60 \times 10 \cong 1485\text{МГц}. \quad (2)$$

Тогда расчетная частота дискретизации приемника должна быть не менее чем в 2 раза больше, что соответствует примерно 3 ГГц.

Нижняя частота дискретизации приемника должна быть как минимум больше 8 МГц, т. к. данная частота будет формировать свойства приемника как полосового фильтра, а для достоверного анализа даже самого узкого спектра от TMDS необходимо покрытие полосовым фильтром трех гармоник справа от центральной частоты, как гармоник с наиболее высокой мощностью. Верхняя частота дискретизации приемника при этом не ограничена, что следует из описанного выше. SDR среднего уровня имеют ограниченную частоту дискретизации, что не позволяет получить отдельные биты данных, передаваемые монитором. Например, наиболее доступная USRP B200-mini, используемая в исследовании далее, имеет $f_s = 56$ МГц, что значительно меньше частоты пикселей (1485 МГц). Это означает, что каждая выборка SDR будет представлять собой комбинацию нескольких сотен битов, затрудняя восстановление изображения. Поэтому коэффициентом, определяющим цвет пикселя, будем пренебрегать, что позволит уменьшить частоту дискретизации 1485 МГц на порядок – до 148,5 МГц. В таком случае изображение будет восстановлено без информации о цвете пикселя, т.е. в оттенках черного и белого, что позволит уменьшить выборку SDR с нескольких сотен до нескольких битов. Такое восстановление будет «склеивать» информацию о нескольких пикселях в один путем усреднения интенсивности излучаемого от них сигнала. Увеличение частоты дискретизации до уровня, достаточного для выделения отдельных битов, непрактично – требуется дорогостоящий SDR с очень высокой полосой пропускания. Кроме того, увеличенная полоса пропускания приводит к большему количеству шумов и сложностям в обработке данных. Таким образом, при проведении анализа возможность точного восстановления исходной последовательности битов отсутствует. Однако, целью является не восстановление точной последовательности, а получение наиболее вероятного изображения, соответствующего полученным данным.

Для передачи аналогового сигнала SDR приемником в программное обеспечение необходимо получить копию видеосигнала и принять значение амплитуды вектора квадратурной модуляции (IQ), характеризующего интенсивность пересылаемого пикселя. Для этого необходимо применить полосовой фильтр с центром, находящимся на частоте сигнала излучаемого от пикселей дисплея или на кратном значении данной частоты для анализа второй и последующих гармоник. Также для успешного анализа видеосигнала необходимо подобрать полосу пропускания приемника, соответствующую спектральному диапазону видеосигнала. После этого требуется синхронизировать внутренние часы приемника с частотой пикселей дисплея для точного расчета предполагаемой интенсивности пикселей, рис. 2.

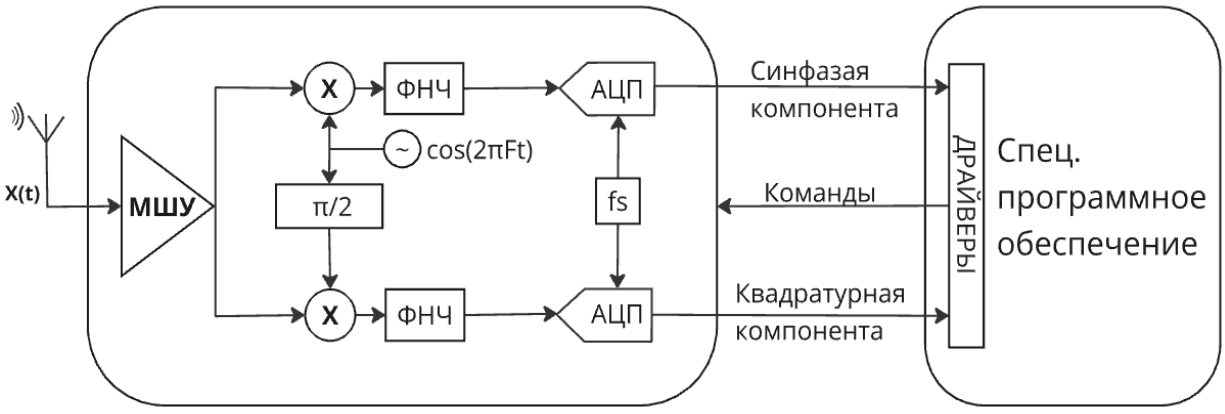

Рис. 2. Приемный тракт SDR и схема передачи действительной (синфазной) и мнимой (квадратурной) части квадратурно-модулированной выборки на драйверы ПК

Первый шаг можно реализовать с помощью приемника АМ (амплитудной модуляции). Необходимая полоса пропускания сигнала значительно превышает возможности стандартных АМ-приемников. Однако некоторые программно-определяемые радиоприемники, такие как NI USRP B200, способны обеспечить требуемую полосу пропускания (до 56 МГц в реальном времени), покрывая большую часть диапазона, необходимого для анализа излучений видеосигналов. Программно-определяемые радиоприемники предоставляют радиосигналы в виде квадратурного вектора, где угол соответствует мгновенной фазе относительно внутреннего генератора. Длина вектора пропорциональна амплитуде, измеренной для каждой квадратурно-модулированной (IQ) выборки, согласно определению:

$$A_n = \sqrt{I_n^2 \cdot + Q_n^2}, \quad (3)$$

где I_n – синфазная компонента, Q_n – квадратурная компонента

В случае АМ-сигнала информация о фазе не требуется, так как видеосигнал передается на постоянной частоте. Поэтому можно использовать обычный амплитудный демодулятор, извлекая длину вектора для каждого отсчета. Когда частота дискретизации приемника совпадает с частотой пикселей, каждая выборка представляет собой оценку средней интенсивности пикселей в определенном интервале времени, определяющимся в (1). Для цифровых сигналов это соответствует битовому шаблону, представляющего интенсивность текущего пикселя. Параллельно с поиском повторений сигнала необходимо проводить передискретизацию сигнала с увеличением частоты кадров изображения до 60 Гц или с уменьшением, в соответствии с загруженностью процессора-обработчика. Далее необходимо обрабатывать сигнал используя фильтр нижних частот, усиливать и проводить синхронизацию с автокоррелированными значениями. Данные действия реализованы в специальном программном обеспечении (СПО) для программируемой логической интегральной схемы (ПЛИС) в SDR-приемнике и дальнейшей обработке на ПК. Архитектура СПО в составе ПАК представлена на рис. 3.

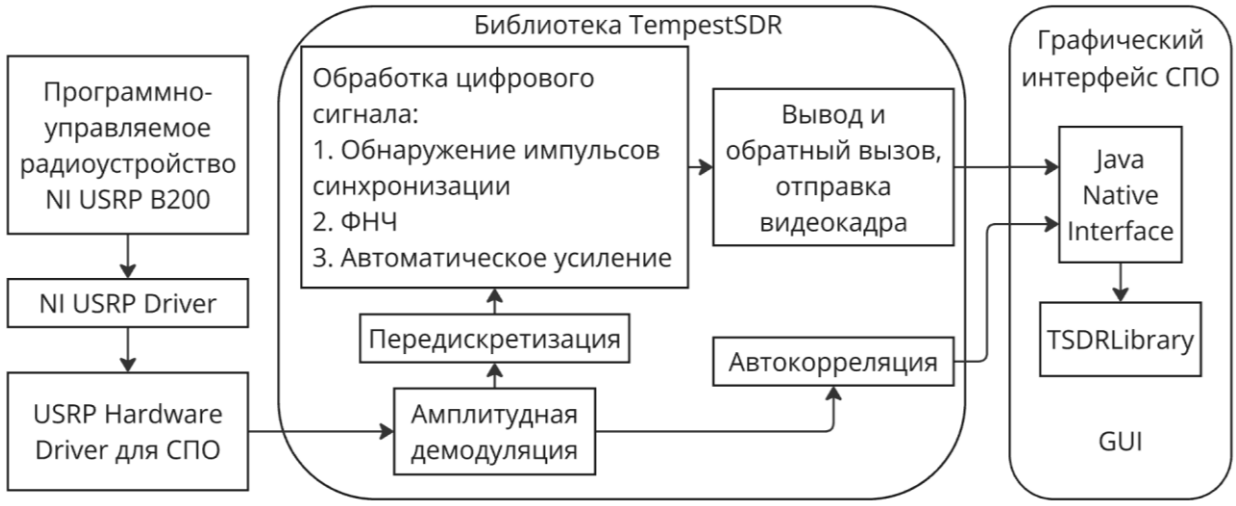

Рис. 3. Схема архитектуры специального программного обеспечения

Таким образом, для поставленной задачи необходимо сформировать требования к аппаратно-программному комплексу со стороны необходимого диапазона анализируемых частот для решения задачи цифровой обработки полученного сигнала:

- Диапазон анализируемых частот: 70 МГц – 3 ГГц;

- Частота дискретизации приемника > 8 МГц;
- Программное обеспечение, обрабатывающее в реальном времени поток сигналов из квадратурной и синфазной составляющих.

Наиболее доступным и подходящим вариантом аппаратной составляющей комплекса является SDR-приемник «NI USRP B200» с диапазоном поддерживаемых частот 70 МГц – 6 ГГц и частотой дискретизации до 56 МГц. Антенна «АШН-6» с диапазоном рабочих частот 70 МГц – 4 ГГц. Ноутбук с процессором «Intel(R) Core(TM) i5-8265U 1800 МГц» на 4 ядра с интегрированным графическим процессором «Intel(R) UHD Graphics 620» и 8 ГБ оперативной памяти с частотой 2133 МГц (рис. 4).

Рис. 4. Программно-аппаратный комплекс для анализа изображения

2. Проведение эксперимента

На разработанном комплексе был проведен эксперимент в офисном помещении с большим количеством электронного оборудования, создающего шумы и помехи. В ходе эксперимента проанализирован полезный сигнал от монитора «AOC 24P1W1» с разрешением 1920x1080 и частотой кадров 60 Гц. Расстояние между принимающей сигнал антенной и излучающим сигнал монитором – 1 м. Оригинал изображения и восстановленное по нему изображение представлены на рис. 5. При значении частоты дискретизации 54 МГц заметно невысокое качество восстановленного изображения. На полученном изображении размыты буквы и человеческому глазу сложно различить шрифт менее 48 пт. Это связано с тем, что мощность полезного сигнала сопоставима с мощностью помех и шумов принимаемых антенной при данных параметрах настройки приемника. Вследствие чего процесс распознавания полезного сигнала в шумовой дорожке становится затруднительным. Размытие происходит из-за того, что значение интенсивности излучаемых сигналов от нескольких соседних пикселей усредняется, т.к. частота дискретизации приемника меньше в несколько раз той частоты, которая необходима для точного восстановления в соответствии с теоремой Котельникова, описанной в разделе 1.

Полученные результаты свидетельствуют о том, что после восстановления изображения необходима его дополнительная обработка, чтобы текст на изображении стал

различим для человека. Подобное восстановление информации на зашумленных изображениях возможно с помощью сверточных нейронных сетей.

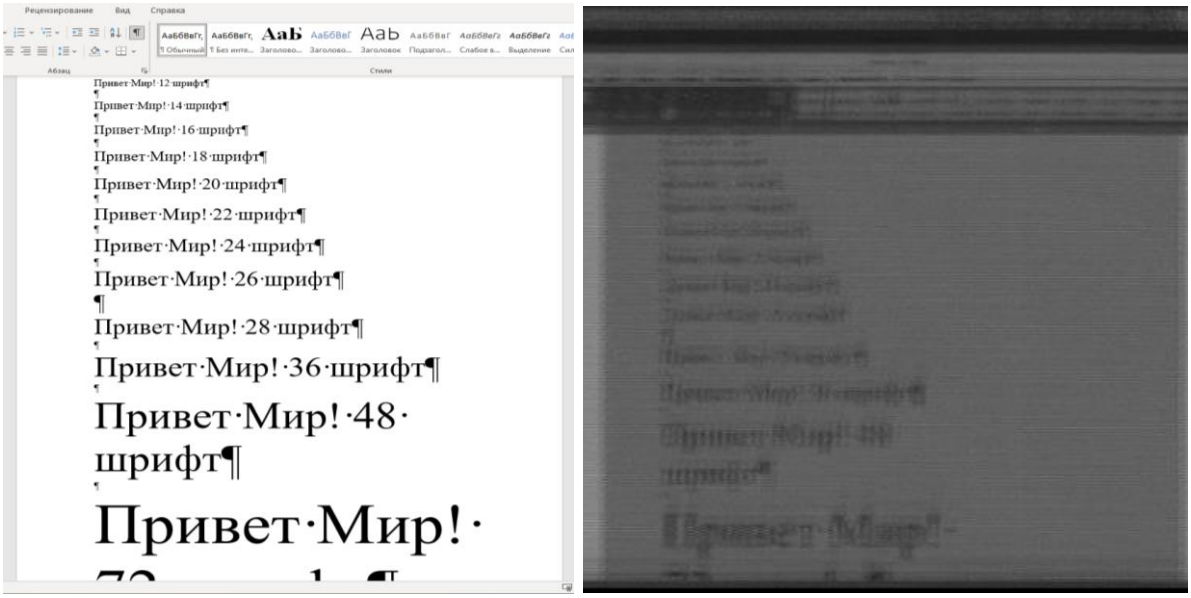

Рис. 5. Оригинал изображения, переданного по HDMI и его восстановленный вариант, полученный на частоте 594 МГц с частотой дискретизации приемника 54 МГц с расстояния 1 м

3. Свёрточные нейронные сети для улучшения качества восстанавливаемых изображений

Для того, чтобы обработать изображение, восстановленное методами анализа побочных электромагнитных излучений, необходимо провести ряд действий по обратному преобразованию полученного зашумленного сигнала $y(t)$ в исходный сигнал $x(t)$. Обратная задача восстановления исходного изображения X состоит из анализа искаженного наблюдения Y, представляющего собой массив комплексных чисел из синфазных и квадратурных компонент, размер которых равен размеру исходного изображения. Данное наблюдение можно описать следующей формулой:

$$Y = F(X) + Z, \tag{4}$$

где F является оператором нелинейной деградации сигнала, а Z является аддитивным комплексным шумом, для которого действительная и мнимая части считаются взаимно независимыми, причем каждая из них представляет собой изображение белого гауссовского шума с дисперсией σ^2.

Из-за вышеупомянутого межсимвольного наложения и ограниченности частоты дискретизации приемника оператор деградации F возможно определить только с точностью Θ-большое, поэтому, добиться идеального восстановления исходного изображения практически невозможно. Вследствие чего постараемся уменьшить оценку Θ путем введения регуляризации и постараемся максимально приблизиться к исходному изображению, в соответствии с Байесовской оценкой для решения максимальной апостериорной задачи, где решение минимизирует элемент данных с параметром регуляризации. В частности, оператор деградации отвечает за требование сходства с реальным процессом деградации сигнала, в то время как регуляризация состоит из функции, которая отвечает за предоставление стабильного решения, которое будет удовлетворять любой комбинации входных данных. Т.е. после достаточно точного подбора

оператора регуляризации можно воспроизводить успешное восстановление исходного изображения на других примерах. Правильный выбор регуляризатора не является тривиальной задачей, поскольку он включает в себя предварительную информацию о типе восстанавливаемых изображений. Метод регуляризация Тихонова не сможет достаточно точно восстановить регуляризирующий оператор, потому что в (4) есть и зависимость от Z. Вследствие чего необходимо подобрать метод, основанный на подходах обучения по наборам больших данных из пар исходных и восстановленных изображений.

Непосредственно изучить отображение из искаженных наблюдений на эталонные изображения возможно с помощью сверточных нейронных сетей. Для создания отображения необходимо обучить модель сквозной глубокой сверточной нейронной сети (CNN) с помощью функции регрессии f для оператора:

$$X = f(Y, \Theta). \quad (5)$$

Данное преобразование позволит отображать зашумленные и искаженные сигналы в очищенные исходные изображения.

Обучение модели проводится путем минимизации определенных потерь на обучающем наборе, содержащем более 1000 пар изображений с чистыми и искаженными данными. Обратим внимание, что регрессор CNN $f(Y, \Theta)$ не зависит от оператора разложения F из (4) явно, но он необходим для вычисления весов для пар изображений с чистым и разложенным изображением. Таким образом при определении веса можно генерировать данные для обучения синтетическим путем.

Для модели $f(Y, \Theta)$ будем использовать нейронную сеть DRUNet (Глубокая остаточная сеть UNet) [10] –популярная CNN с высокой чувствительностью. Архитектура CNN, показанная на рис. 6, состоит из последовательности взаимосвязанных сверточных слоев, функций активации и слоев объединения подвыборки. DRUNet является улучшенным вариантом нейросети для сегментации изображений UNet [15] и использует структуру кодер-декодер. В первой серии сверточных слоев изображение преобразуется в пространство меньшего размера, а затем, во второй серии сверточных слоев, изображение преобразуется в исходный размер. Кроме того, как и в других архитектурах, таких как ResNet [14], можно соединить несмежный сверточный слой, используя остаточные блоки, или пропустить соединения. Данная сеть зарекомендовала себя и показала, что такая стратегия повышает производительность модели.

Каждая пара обучающей выборки основана из двух возможных источников – реальных наблюдаемых сигналах или синтетических данных. Реальные восстановленные изображения были получены с помощью программно-аппаратного комплекса, изображенного на рис. 4. Для обучения модели необходимо сформировать несколько тысяч различных исходных изображений и зафиксировать по ним восстановленные кадры. Важно подчеркнуть, что настройка ПАК для анализа изображений является непростой и достаточно трудозатратной задачей. Поэтому необходимо создать синтетический набор данных для дальнейшего обучения модели. Данный набор был сгенерирован с помощью скрипта на Python. Генератор синтетических изображений имитирует передачу загруженного в него изображения по протоколу передачи HDMI и преобразовывает основную полосу пропускания SDR-приемника, а также фильтрует нижние частоты и проводит передискретизацию. К полученному сигналу добавляется гауссовский шум, небольшие частотные погрешности и случайная задержка.

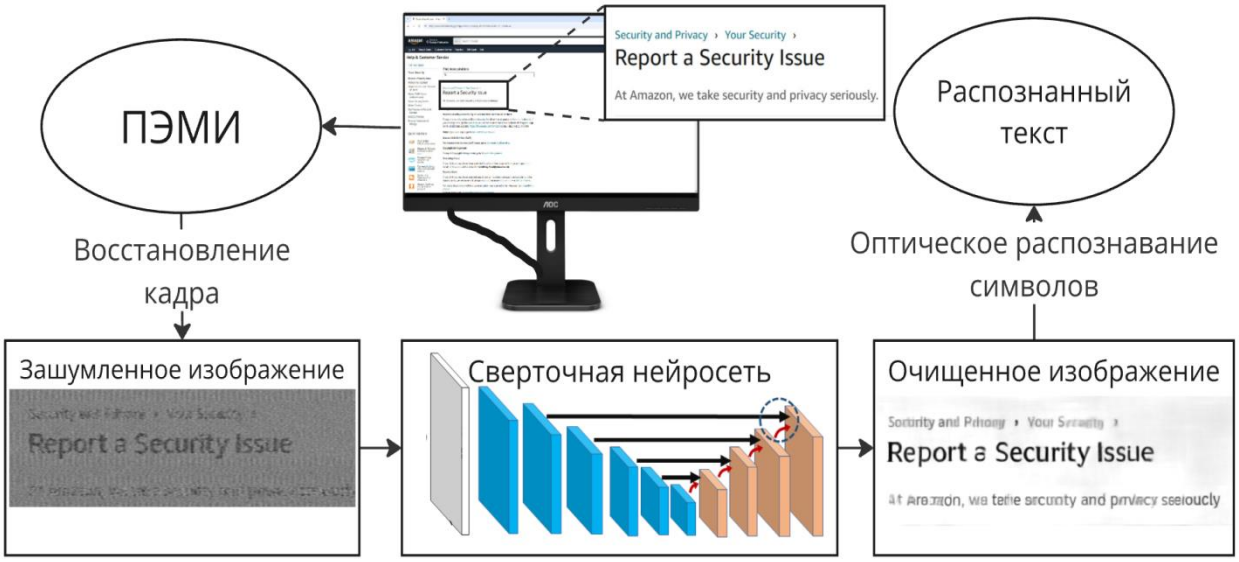

Рис. 6. Схема восстановления изображения с помощью сверточной нейронной сети

При обучении моделей был собран набор из 3000 пар изображений с оригинальными и восстановленными вариантами. В данный набор входили 1500 изображений, полученных с помощью восстановления при помощи оборудования, указанного на рис. 4. Остальные изображения были сгенерированы синтетически. Причем для синтетических моделей часть изображений включали в себя сгенерированный случайным образом текст. Набор данных для восстановления с использованием ПАК включает в себя реальные изображения, отображаемые на экране монитора. Данный набор охватывает различные материалы, начиная со страниц авторизаций и статей конференций, и заканчивая вручную сделанными скриншотами с различных веб-сайтов. Чтобы оценить эффективность обученных моделей, необходимо определить репрезентативный показатель восстановления. Например, показателем для восстановления сигнала является пиковое отношение сигнал/шум (PSNR). Однако для анализа изображения больше всего интересен текст, изображенный на мониторе. В связи с этим для анализа обученных моделей можно воспользоваться частотой символьных ошибок (CER). Данный показатель можно рассчитать с помощью открытой библиотеки для оптического распознавания символов Tesseract OCR. Следовательно, по значению относительной величины CER можно определить эффективность обучения определенной модели.

$$CER = \frac{N_{\text{ошибок}}}{N_{\text{символов}}}, \tag{6}$$

где в числителе указано количество символов, не совпавших с оригинальным текстом, а в знаменателе указано общее количество анализируемых символов. Символы на оригинальном и восстановленном изображениях определены с помощью Tesseract OCR. Для различных сверточных нейронных сетей на одном обучающем наборе данных необходимо усреднить данный коэффициент и рассчитать его в процентах.

Рабочая станция, используемая для обучения нейронных сетей, состоит из 16-ядерного процессора «AMD Ryzen 9 7950X» со 128 ГБ оперативной памяти и графическим процессором «NVIDIA GeForce RTX 3060» с 12 ГБ видеопамяти. «FullHD»-изображение с разрешением 1920x1080 проходит обработку примерно за 0,7 с на графическом процессоре (GPU) и 17 с на центральном процессоре(CPU). Т.е. расчеты на GPU позволяют ускорить процесс обучения в несколько раз.

По результатам обучения моделей с помощью DRUNet и UNet показатель CER составил 38% и 45% соответственно, что является весьма высокими значениями, если учитывать, что изначально восстановленное при помощи SDR изображение имеет CER приблизительно 95%. Таким образом, сеть DRUNet показала преимущество над сетью UNet, так как является более обновленной версией CNN данного типа и в большей степени направлена на уменьшение шумов в изображениях.

4. Методы защиты от восстановления изображения

Важно выявить недостатки системы, описанной в предыдущих разделах. Для того, чтобы противодействовать анализу изображений аналогичного программно-аппаратного комплекса необходимо обеспечивать защиту личной или секретной информации. Например, можно рассмотреть несколько мер, которые при незаметном изменении отображаемого на экране монитора изображения приводят к увеличению соотношения сигнал/шум в восстановленном изображении. Данные меры следуют из анализа побочных электромагнитных излучений, описанного в разделе 1, и используют нелинейность кодирования передаваемой информации по интерфейсу HDMI.

Одним из способов ухудшения качества восстанавливаемого изображения может стать добавление низкоуровневого шума к исходному изображению на дисплее монитора. Данный шум может быть, например, аддитивным гауссовским шумом с постоянной дисперсией. Именно такой шум затруднит нейросетевой анализ текста на сером фоне в восстановленном изображении.

Вторым более заметным решением является использование цветового градиента на фоне изображений. При использовании горизонтального градиента (например, переход от белого к черному) линейно изменяются оттенки серого по всему изображению, что после кодировании видеосигнала приведет к значительным изменениям в перехваченном сигнале.

Заключение

В работе представлен способ подготовки моделей на основе сверточных нейронных сетей, обученных сопоставлять электромагнитный сигнал, исходящий от кабеля HDMI, с изображением, отображаемым на экране монитора. В результате обучения модели собран набор данных из реальных побочных электромагнитных сигналов и исходных изображений, а также из синтетически смоделированных образцов. В результате обучения уменьшена частота символьных ошибок по сравнению с восстановленным изображением после обработки демодулированных сигналов. Проведено сравнение частоты символьных ошибок для различных вариантов сверточных нейронных сетей. Данная работа демонстрирует возможность восстановления читаемого текстового изображения и позволяет задуматься о развитии методов постобработки восстановленных изображений с помощью других нейронных сетей. Важно подчеркнуть, что для получения каждого восстановленного изображения на обученной модели требуется несколько секунд, но это время можно сократить для более быстрого анализа исследуемых сигналов от мониторов различных разрешений с помощью увеличения вычислительной мощности комплекса. Текущие результаты работы могут применяться при проведении исследований анализа защищенности интерфейса HDMI для передачи видеоинформации на видеомониторы.

СПИСОК ЛИТЕРАТУРЫ:

1. Хорев А.А. Некоторые подходы к оценке возможностей перехвата побочных электромагнитных излучений средств вычислительной техники, использующих цифровые интерфейсы. Вестник УрФО. Безопасность в информационной сфере. 2022, № 3(45), с. 5–16. DOI: http://dx.doi.org/10.14529/secur220301.

2. Erdeljan D., Kuhn M. Benefits of coherent demodulation for eavesdropping on HDMI emissions. 2024. DOI: https://doi.org/10.17863/CAM.109111.
3. Антясов И.С., Асяев ГД., Уфимцев М.С. Исследование побочных электромагнитных излучений монитора с помощью RTL-SDR приемника. Вестник УрФО. Безопасность в информационной сфере. 2019, № 4(34), с. 15–21. DOI: http://dx.doi.org/10.14529/secur190402.
4. Liu Z. et al. Screen gleaning: A screen reading TEMPEST attack on mobile devices exploiting an electromagnetic side channel. arXiv preprint arXiv:2011.09877. 2020. DOI: https://doi.org/10.48550/arXiv.2011.09877.
5. Long Y. et al. EM Eye: Characterizing Electromagnetic Side-channel Eavesdropping on Embedded Cameras. Proceedings of ACM NDSS. 2024. DOI: https://10.14722/ndss.2024.24552.
6. Паршуткин А.В., Неаскина М.Р. Повышение защищенности информации от утечки через побочные электромагнитные излучения. Вопросы кибербезопасности. 2022, № 3(49), с. 82–89. DOI: https://doi.org/10.21681/2311-3456-2022-3-82-89.
7. Смирнов Д.А. Исследование побочных электромагнитных излучений интерфейса HDMI. Радиоэлектронные устройства и системы для инфокоммуникационных технологий-РЭУС-2019. 2019, с. 326–330. – EDN: SWJCTA.
8. Симахин Егор А. и др. Анализ компонентов архитектуры интерфейса DisplayPort, влияющих на побочное электромагнитное излучение. Безопасность информационных технологий, [S.I.], т. 29, № 1, с. 108–124, 2022. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2022.1.10.
9. Simakhin E.A., Shinyaev D.A., Kagin I.I., Kessarinskiy L.N. and Durakovskiy A.P. Analysis of Electromagnetic Radiation of LCD Monitor with DisplayPort Interface. 2022 Moscow Workshop on Electronic and Networking Technologies (MWENT), Moscow, Russian Federation. 2022, p. 1–5. DOI: http://dx.doi.org/10.1109/MWENT55238.2022.9802294.
10. Костючек М.И., Макаренко А.В. Применение свёрточных глубоких нейронных сетей для решения некоторых задач анализа траекторных данных. Журнал Радиоэлектроники. 2021, № 11. DOI: http://dx.doi.org/10.30898/1684-1719.2021.11.15.
11. Porkhun A.S. et al. Justification of an Experimental Stand Based on a Software-Defined Radio System for Detecting Technical Channels of Information Leakage. Seminar on Information Computing and Processing (ICP). IEEE. 2023, p. 166–170. DOI: http://dx.doi.org/10.1109/ICP60417.2023.10397202.
12. Иванов А.В. и др. Применение технологии SDR (Software Defined Radio) для восстановления сигналов побочных электромагнитных излучений видеотракта. Безопасность цифровых технологий. 2021, № 4(103), с. 72. DOI: http://dx.doi.org/10.17212/2782-2230-2021-4-72-90.
13. Хорев А.А. Экспериментальные исследования распознавания оператором текстовых символов на экране монитора, полученных с различным разрешением. Вестник УрФО. Безопасность в информационной сфере. 2020, № 4(38), с. 22–30. DOI: http://dx.doi.org/10.14529/secur200402.
14. Филиппов С.А. Классификация изображений с помощью сверточных нейронных сетей. Электронные библиотеки. 2024, т. 27, №. 3, с. 366–382. DOI: http://dx.doi.org/10.31044/1684-2588-2021-0-10-31-39.
15. Демин И.С., Белов Ю.С., Чухраев И.В. Обучение сверточной нейронной сети на базе архитектуры U-Net с использованием минимальных ресурсов. Электромагнитные волны и электронные системы. 2019, т. 24, № 7, с. 24–29. DOI: http://dx.doi.org/10.18127//j15604128-201907-04.

REFERENCES:

[1] Khorev A.A. Some approaches to assessing the possibilities of intercepting spurious electromagnetic radiation from computer equipment using digital interfaces. Bulletin of the Ural Federal District. Information security. 2022, no. 3(45), p. 5–16. DOI: http://dx.doi.org/10.14529/secur220301 (in Russian).
[2] Erdeljan D., Kuhn M. Benefits of coherent demodulation for eavesdropping on HDMI emissions. EMC Europe 2024. DOI: https://doi.org/10.17863/CAM.109111.
[3] Antyasov I.S., Asyaev G.D., Ufimtsev M.S. Investigation of side electromagnetic radiation of a monitor using an RTL-SDR receiver. Bulletin of the Ural Federal District. Information security. 2019, no. 4(34), p. 15–21. DOI: http://dx.doi.org/10.14529/secur190402 (in Russian).
[4] Liu Z. et al. Screen gleaning: A screen reading TEMPEST attack on mobile devices exploiting an electromagnetic side channel. arXiv preprint arXiv:2011.09877. 2020. DOI: https://doi.org/10.48550/arXiv.2011.09877.
[5] Long Y. et al. EM Eye: Characterizing Electromagnetic Side-channel Eavesdropping on Embedded Cameras. Proceedings of ACM NDSS. – 2024. DOI: https://10.14722/ndss.2024.24552.
[6] Parshutkin A.V., Neaskina M.R. Increasing the security of information from leakage through side electromagnetic radiation. Cybersecurity issues. 2022, no. 3(49), p. 82–89. DOI: https://doi.org/10.21681/2311-3456-2022-3-82-89 (in Russian).

[7] Smirnov D. A. Investigation of side electromagnetic radiation of the HDMI interface. Radio electronic devices and systems for infocommunication technologies-REUS-2019. 2019, p. 326–330 (in Russian). – EDN: SWJCTA.
[8] Simakhin Egor A. et al. Analysis of the components of the DisplayPort interface architecture that affect the side electromagnetic radiation. Information Technology Security, [S.I.], v. 29, no. 1, p. 108–124, 2022. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2022.1.10 (in Russian).
[9] Simakhin E.A., Shinyaev D.A., Kagin I.I., Kessarinskiy L.N. and Durakovskiy A.P. Analysis of Electromagnetic Radiation of LCD Monitor with DisplayPort Interface. 2022 Moscow Workshop on Electronic and Networking Technologies (MWENT), Moscow, Russian Federation. 2022, p. 1–5. DOI: http://dx.doi.org/10.1109/MWENT55238.2022.9802294.
[10] Kostyuchek M.I., Makarenko A.V. Application of convolutional deep neural networks for solving some problems of trajectory data analysis. Journal of Radioelectronics. 2021, no. 11. DOI: http://dx.doi.org/10.30898/1684-1719.2021.11.15 (in Russian).
[11] Porkhun A.S. et al. Justification of an Experimental Stand Based on a Software-Defined Radio System for Detecting Technical Channels of Information Leakage. Seminar on Information Computing and Processing (ICP). IEEE. 2023, p. 166–170. DOI: http://dx.doi.org/10.1109/ICP60417.2023.10397202.
[12] Ivanov A.V. et al. The use of SDR (Software Defined Radio) technology to restore the signals of side electromagnetic radiation of the video path. The security of digital technologies. 2021, no. 4(103), p. 72. DOI: http://dx.doi.org/10.17212/2782-2230-2021-4-72-90 (in Russian).
[13] Khorev A.A. Experimental studies of operator recognition of text characters on a monitor screen obtained with different resolutions. Bulletin of the Ural Federal District. Information security. 2020, № 4(38), p. 22–30. DOI: http://dx.doi.org/10.14529/secur200402 (in Russian).
[14] Filippov S.A. Image classification using convolutional neural networks. Electronic libraries. 2024, v. 27, no. 3, p. 366–382. DOI: http://dx.doi.org/10.31044/1684-2588-2021-0-10-31-39 (in Russian).
[15] Demin I.S., Belov Yu.S., Chukhraev I.V. Training of a convolutional neural network based on the U-Net architecture using minimal resources. Electromagnetic waves and electronic systems. 2019, v. 24, no. 7, p. 24-29. DOI: http://dx.doi.org/10.18127//j15604128-201907-04 (in Russian).

Поступила в редакцию – 30 сентября 2024 г. Окончательный вариант – 10 ноября 2024 г.
Received – September 30, 2024. The final version – November 10, 2024.