УДК 004.021, 004.056, 003.75, 681.3.06

НОВОЕ МЕТРИЧЕСКОЕ ПРОСТРАНСТВО ДЛЯ ЗАДАЧ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Ж.К. Абдурахманов
Андижанский государственный университет, Андижан, Узбекистан

Аннотация. В данной статье рассматриваются возможности применения нового расстояния, введенного автором, в различных аспектах технической защиты информации. Это расстояние обладает рядом преимуществ перед классическими метриками, что делает его полезным инструментом в анализе данных. Рассматриваются четыре ключевых направления его использования: обнаружение аномалий, коррекция ошибок, криптографические алгоритмы и биометрическая аутентификация. В системах обнаружения вторжений новое расстояние позволяет повысить точность выявления аномалий. В коррекции ошибок оно способствует более эффективному декодированию данных. В криптографии его применение улучшает генерацию ключей и устойчивость алгоритмов. В биометрической аутентификации оно повышает точность идентификации. Представлены математические модели и формулы, демонстрирующие преимущества нового расстояния. Работа показывает, что предложенный метод может существенно повысить надежность и эффективность современных средств защиты информации.

Ключевые слова: расстояние; защита информации; криптография; биометрия; коррекция ошибок; аномалии; аутентификация; кодирование; метрики; идентификация.

NEW METRIC SPACE FOR INFORMATION SECURITY TASKS

J. K. Abdurakhmanov
Andijan State University, Andijan, Uzbekistan

Abstract. This paper explores the potential applications of a new distance metric introduced by the author in the field of information security technologies. The proposed metric offers advantages over classical distance measures such as the Hamming distance and the Euclidean metric. The study examines its effectiveness in four key areas: anomaly detection, error correction, cryptographic algorithms, and biometric authentication. The new distance metric enables more accurate differentiation of data anomalies, enhances the reliability of error correction codes, strengthens cryptographic mechanisms, and improves the accuracy of biometric recognition systems. Theoretical foundations are supported by mathematical formulations, illustrating the applicability of the metric in various security-related tasks. The research demonstrates that incorporating this metric into security technologies can increase the accuracy, efficiency, and resilience of information protection systems. Future studies will focus on practical implementations of these theoretical findings in real-world security systems.

Keywords: distance, information security, cryptography, biometrics, error correction, anomalies, authentication, coding, metrics, identification.

Введение

Современные технические средства защиты информации требуют эффективных методов анализа данных и обнаружения угроз. Одним из ключевых аспектов является возможность точного измерения различий между объектами данных. В данной работе предлагается применение нового расстояния, обладающего рядом преимуществ перед классическими метриками, такими как Хэммингово расстояние и Евклидова метрика.

Новое расстояние, предложенное в [1], определяется следующим образом. Пусть заданы два конечных множества X и Y. Тогда расстояние $d(X,Y)$ вычисляется по формуле:

$$d(X,Y) = \frac{|X \Delta Y|}{2}$$

где $|X \Delta Y|$ обозначает мощность симметрической разности множеств X и Y. Данное расстояние обобщает Хэммингово расстояние, обеспечивая более тонкую градацию различий между объектами.

Рассмотрим иллюстрирующий пример. Пусть даны два множества битовых строк:

$X = \{101, 110, 011\}, Y = \{100, 110, 010\}$.

Симметрическая разность этих множеств равна $\{101, 011, 100, 010\}$, следовательно,

$d(X,Y) = \frac{4}{2} = 2$.

Этот пример демонстрирует, что новое расстояние позволяет учитывать частичные совпадения между объектами, что особенно важно в задачах защиты информации.

Обнаружение аномалий в данных

Аномалии в данных могут указывать на потенциальные угрозы информационной безопасности, включая несанкционированный доступ и сетевые атаки. Новое расстояние позволяет более точно оценивать степень отклонения между нормальными и аномальными данными, что делает его полезным инструментом для систем обнаружения вторжений (IDS). Например:

– В анализе сетевого трафика новое расстояние можно применять для выделения аномальных пакетов данных, используя кластерный анализ аномалий.

– В логах операционной системы можно сравнивать последовательности событий, выявляя подозрительные отклонения от нормального поведения.

– В анализе данных IoT-устройств новое расстояние может использоваться для распознавания неожиданных паттернов активности, сигнализирующих о компрометации устройства.

Математически, если заданы два набора данных X и Y, то степень аномальности можно оценить с помощью следующего выражения:

$$A(X,Y) = \frac{d(X,Y)}{d_{max}}$$

где d_{max} – некоторый эталонный (или максимальный) уровень расстояния, соответствующий нормализующей константе. Например, это может быть:

– максимальное расстояние между объектами в обучающей выборке;

– среднее расстояние в нормальных условиях;

– фиксированный порог аномальности.

Улучшение коррекции ошибок

Передача данных по шумным каналам требует механизмов исправления ошибок. Обобщая известные методы кодирования, новое расстояние может способствовать разработке более эффективных корректирующих кодов. Например:

В кодах с обнаружением и исправлением ошибок новое расстояние можно применять для оптимизации декодирования в условиях высокой зашумленности.

В системах передачи данных по спутниковым каналам оно позволяет адаптивно изменять кодовые параметры в зависимости от уровня помех.

В хранилищах больших данных новое расстояние можно использовать для автоматического восстановления поврежденных фрагментов информации на основе избыточных данных.

Математически, если $d(x,y)$ – новое расстояние между кодовыми словами, а $H(x,y)$ – Хэммингово расстояние, то в ряде случаев выполняется неравенство:

$$d(x,y) \leq \frac{H(x,y)}{2},$$

что позволяет детектировать ошибки на более тонком уровне и применять эффективные алгоритмы исправления. Дополнительно, вероятность ошибки декодирования можно оценить как:

$$P_e = e^{-\alpha d(x,y)},$$

где α – коэффициент, зависящий от характеристик канала передачи данных.

Оптимизация криптографических алгоритмов

Многие криптографические алгоритмы зависят от устойчивости метрик различия. Новое расстояние предлагает ряд преимуществ:

В генерации ключей новое расстояние можно использовать для усиления криптографической стойкости за счет выбора ключей с максимальным различием.

В алгоритмах цифровых подписей оно может обеспечивать более надежную проверку подлинности.

В механизмах хеширования новое расстояние можно применять для улучшения коллизионной устойчивости.

Допустим, ключ K генерируется на основе входных данных X, тогда использование нового расстояния может обеспечивать более равномерное распределение ключей:

$$H(K_1, K_2) > 2d(K_1, K_2).$$

Дополнительно, криптографическая стойкость алгоритма можно выразить через энтропию ключей:

$$S = -\sum p_i \log p_i$$

где p_i – вероятность выбора конкретного ключа.

Биометрическая аутентификация

Современные системы идентификации используют методы сравнения биометрических данных. Новое расстояние позволяет более точно анализировать различия между биометрическими шаблонами, что способствует повышению надежности распознавания. Например:

– в системах распознавания лиц его можно применять для более точного измерения различий между векторными представлениями изображений;

– в системах аутентификации по отпечаткам пальцев оно может повысить точность идентификации при частичных отпечатках;

– в голосовой биометрии новое расстояние может использоваться для выделения тонких различий в акустических характеристиках.

Заключение

Рассмотренные направления демонстрируют широкие возможности применения нового расстояния в технических средствах защиты информации. Его использование может повысить точность обнаружения угроз, улучшить корректирующие коды, усилить криптографические механизмы и повысить надежность биометрической аутентификации. Дальнейшие исследования направлены на практическую реализацию данных идей в конкретных системах безопасности.

Список использованных источников / References

1. Jamolidin Abdurakhmanov . New distance for any finite sets, half the Hamming distance. *TechRxiv*. April 05, 2023.

Сведения об авторе

Абдурахманов Ж.К., кандидат физико-математических наук, доцент, доцент кафедры Информационных технологий Андижанского государственного университета. jamolidinkamol@gmail.com.

Information about the author

Abdurakhmanov J.K., Ph.D. in Physical and Mathematical Sciences. Associate Professor. Associate Professor of the Department of Information Technology at Andijan State University. jamolidinkamol@gmail.com.