

**РАЗРАБОТКА МЕТОДОВ ЗАЩИТЫ СИСТЕМ  
БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ ОТ  
ТАРГЕТИРОВАННЫХ АТАК**

*Круглова Светлана Ивановна*

*Студент*

*Факультет ВМК МГУ имени М. В. Ломоносова, Москва, Россия*

*E-mail: ms.kr666@mail.ru*

*Научный руководитель — Применко Эдуард Андреевич*

Одним из наиболее широко распространенных типов атак на биометрические системы идентификации являются так называемые спуфинг-атаки или состязательные атаки [1], заключающиеся в подмене биометрического образа. Состязательные атаки преобразуют биометрический образ так, чтобы он позволял получить доступ к системе, и одновременно в некотором смысле не раскрывал факт атаки.

Выявление слабых сторон системы распознавания и возможностей состязательных атак приводит к эффективным средствам защиты [2]. В данной работе исследуется возможность построения устойчивого к состязательным атакам метода биометрической идентификации на основе выделения характеристик с помощью модифицированного алгоритма LBP. Эффективность предложенного метода оценивается с помощью ошибок 1 и 2 рода, а именно, полученные значения ошибок для модифицированного алгоритма сравниваются с результатами системы идентификации, построенной на основе стандартного алгоритма LBP.

Метод LBP основан на операторе, применяемом к пикселям изображения [4]. Оператор сопоставляет окрестность пикселя с двоичным представлением выбранной области. Пусть  $A = (a_{ij})_{m \times n}$  — матрица яркости изображения,  $a_{ij} \in [0, 255]$ ,  $i = \overline{1, m}$ ,  $j = \overline{1, n}$ .  $P = (p_{ij})_{l \times l}$  — подматрица изображения  $A$ , к которой применяется оператор LBP,  $l$  — параметр оператора LBP, определяющий размер окрестности пикселя и, соответственно, длину итогового двоичного вектора,  $l$  — нечетное. Оператор LBP:  $[0, 255]^{l \times l} \rightarrow V_{4(l-1)}$  действует на подматрицу  $P$  функцией:

$$LBP(P) = \sum_{t=0}^{4(l-1)} 2^t s(b_t - p_{i_c j_c}),$$

1

где  $(i_c, j_c)$  — координаты центрального пикселя  $P$  с яркостью  $p_{i_c j_c}$ ,  $b_t$  — яркость пикселя с номером  $t$  из множества

$B = p_{11}, p_{12}, \dots, p_{1l}, p_{21}, \dots, p_{ll}, p_{l, l-1}, \dots, p_{1l}, p_{l-1, 1}, \dots, p_{21}$  мощности  $4(l-1)$ , которое состоит из граничных элементов подматрицы  $P$ .  $s(x)$  — функция Хевисайда.

Для модификации метода LBP предлагается для каждого изображения выработать перестановку  $\sigma \xrightarrow{U} \mathcal{S}_n$ , где  $n = 4(l-1)$ ,  $U$  — равномерное распределение на множестве перестановок  $\mathcal{S}_n$ . В соответствии с этой перестановкой изменяется множество  $B$ . Таким образом функция оператора LBP принимает вид:

$$LBP(P) = \sum_{t=0}^{4(l-1)} 2^t s(b_{\sigma(t)} - p_{i_c j_c}).$$

В алгоритме распознавания исходное изображение разделяется на подблоки фиксированного размера  $(m' \times n')$ , для каждого подблока формируются подматрицы  $P$ . К подматрицам  $P$  применяется оператор LBP, который возвращает для каждой подматрицы некоторый двоичный вектор. Все полученные вектора переводятся в десятичные числа и объединяются в гистограмму. Сформированная гистограмма соответствует рассматриваемому блоку изображения. Все гистограммы блоков конкатенируются в одну гистограмму исходного изображения, которая называется локальными бинарными гистограммой (LBPН) и используется для дальнейшей классификации изображений, с помощью метода ближайшего соседа, который определяет наименьшее расстояние между характеристиками по метрике  $\chi^2$ :

$$d(H_1, H_2) = \sum_i \frac{(H_1(i) - H_2(i))^2}{H_1(i) + H_2(i)}.$$

Исследование модифицированного алгоритма проводилось на основе базы данных, разработанной компьютерной лабораторией Кембриджского университета (AT&T Database).

В рамках исследования сравниваются ошибки 1 и 2 рода при использовании стандартного и модифицированного алгоритмов LBP при построении системы аутентификации, описанной ранее. Так же были построены ошибки обоих родов для случая, когда для рассматриваемой базы данных используется один способ построения характеристик, а для входного изображения другой. Результаты исследования при  $l = 3$  представлены в таблице 1.

Алгоритм LBP для базы	Алгоритм LBP для образа	Порог	Ошибка 1 рода, %	Ошибка 2 рода, %
Станд.	Станд.	50	24.4	11.3
Станд.	Станд.	55	58.5	6.1
Станд.	Модиф.	50	0	100
Станд.	Модиф.	55	1.8	97.5
Модиф.	Модиф.	50	24.4	11.3
Модиф.	Модиф.	55	58.5	6.1
Модиф.	Станд.	50	0	100
Модиф.	Станд.	55	1.3	96.2

Таблица 1: Таблица результатов идентификации для стандартного и предложенного методов при  $l = 3$

Результаты показывают принципиальную возможность противодействия состязательным атакам с помощью предлагаемого подхода.

#### Литература

1. Лаврентьева Г. М., Новосёлов С. А., Козлов А. В., Кудашев О. Ю., Шемелинин В. Л., Матвеев Ю. Н., Де Марсико М. Методы детектирования спуфинг-атак повторного воспроизведения на голосовые биометрические системы. // Научно-технический вестник информационных технологий, механики и оптики. 2018. Т. 18. № 3. С. 428–436.
2. Määttä J., Hadid A., Pietikäinen M. Face spoofing detection from single images using micro-texture analysis. // 2011 international joint conference on Biometrics (IJCB). IEEE. 2011. P. 1–7.
3. Chingovska I., Anjos A., Marcel S. On the effectiveness of local binary patterns in face anti-spoofing. // 2012 BIOSIG-proceedings of the international conference of biometrics special interest group (BIOSIG). IEEE. 2012. P. 1–7.
4. Ahonen T., Hadid A., Pietikäinen M. Face description with local binary patterns: Application to face recognition. // IEEE transactions on pattern analysis and machine intelligence. 2006. Т. 28. № 12. P. 2037–2041.