Способи фальсифікації слідів рук

Олег Боровик
завідувач сектору дактилоскопічних досліджень відділу криміналістичних видів досліджень,
Полтавський науково-дослідний експертно-криміналістичний центр Міністерства внутрішніх справ України, м. Полтава, Україна, merlot281@gmail.com

Досліджено способи фальсифікації слідів рук, що застосовуються з метою введення в оману правоохоронних органів та біометричних систем.

***Ключові слова**: дактилоскопія; сліди рук; фальсифікація слідів; підробка відбитків пальців; біометричні системи.*

Methods of Handprints Forging

Oleh Borovyk

The paper examines methods of handprints forging used to mislead law enforcement agencies and biometric systems.

***Keywords**: dactyloscopy; handprints; traces forgery; fingerprint falsification; biometric systems.*

Сліди рук є одним із важливих джерел доказової інформації в криміналістиці, що обумовлено їх унікальністю та стабільністю папілярних узорів. Водночас широке застосування дактилоскопії як у криміналістиці, так і в біометричних системах безпеки сприяло розвитку способів їх підроблення. Як зазначено в наукових дослідженнях, поширення біометричних технологій стимулює зловмисників до створення штучних відбитків з метою обходу систем ідентифікації [1, с. 1—2].

Одним із найбільш розповсюджених способів фальсифікації є виготовлення штучних відбитків із полімерних матеріалів. Зокрема, у сучасних дослідженнях описано застосування силікону, латексу та поліуретану для створення так званих «штучних пальців». Такі матеріали дають змогу відтворити рельєф папілярних ліній із високим ступенем точності та можуть застосовуватися для введення в оману як технічних систем, так і людини-експерта [2, с. 2846—2848; 3, с. 534—536].

Експериментальні дослідження підтверджують, що подібні матеріали ефективні для створення підроблених відбитків, здатних імітувати реальні сліди рук [3, с. 537—538].

Іншим важливим напрямом є застосування методів копіювання та перенесення відбитків. Суть цього способу полягає в знятті сліду з однієї поверхні та перенесення на іншу. Хоча такі відбитки можуть зберігати загальну конфігурацію папілярного узору, вони часто втрачають природні характеристики, пов'язані з динамікою дотику (тиск, деформації, розподіл речовин шкіри), що дає змогу виявити їх під час експертного дослідження [4, с. 42—44].

З розвитком цифрових технологій з'явилися більш складні способи фальсифікації, пов'язані зі скануванням та подальшим відтворенням відбитків за допомогою комп'ютерних технологій. Зокрема, можливе створення цифрових моделей відбитків та їх матеріалізація за допомогою 3D-друку або інших методів. Наукові дослідження свідчать, що сучасні біометричні системи можуть бути вразливими до таких атак, оскільки штучно створені відбитки здатні імітувати реальні біометричні параметри [5, с. 385—390; 6, с. 2—4].

Окрему групу становлять новітні матеріали для фальсифікації, зокрема гідрогелі та інші полімерні композиції, які спеціально розробляються для обходу біометричних систем. Дослідження свідчать, що такі матеріали можуть відтворювати не лише форму папілярних ліній, але й фізичні властивості шкіри, що значно ускладнює їх виявлення [3, с. 538—540].

Важливо зазначити, що фальсифікація слідів рук може здійснюватися як із залученням носія, так і без нього шляхом використання залишених слідів або їх цифрових копій. Це підвищує ризики зловживань та ускладнює процес доказування в кримінальному провадженні [1, с. 3–4].

Виявлення підроблених слідів рук базується на аналізі їх морфологічних і фізико-хімічних характеристик. Основні ознаки фальсифікації — відсутність природної варіативності тиску, спрощення структури папілярних ліній, дефекти матеріалу (бульбашки, тріщини), а також відсутність пороскопічних елементів [2, с. 2850—2852].

Окрім того, сучасні підходи передбачають застосування алгоритмів машинного навчання, які дають змогу автоматично відрізняти справжні відбитки від штучних [6, с. 5—7].

Отже, фальсифікація слідів рук є складним багатокомпонентним явищем, що постійно розвивається під впливом науково-технічного прогресу. Незважаючи на високий рівень надійності дактилоскопічної ідентифікації, існує необхідність постійного вдосконалення методів виявлення підробок, що є важливим завданням сучасної криміналістики.

Перелік джерел посилання

1. Gao Q. A Preliminary Study of Fake Fingerprints. *International Journal of Computer Network and Information Security*. 2014. Vol. (12). Pp. 1—8. DOI: 10.5815/ijcnis.2014.12.01 (дата звернення: 26.03.2026).
2. Tan B., Schuckers S. Spoofing protection for fingerprint scanner by fusing ridge signal and valley noise. *Pattern Recognition*. 2010. Vol. 43. Is. 8. Pp. 2845—2857. DOI: 10.1016/j.patcog.2010.01.023 (дата звернення: 26.03.2026).
3. Saguy M., Almog J., Cohn D., Champod Ch. Proactive forensic science in biometrics: Novel materials for fingerprint spoofing. *Journal of Forensic Sciences*. 2022. Vol. 67. Is. 2. Pp. 534—542. DOI: 10.1111/1556-4029.14908 (дата звернення: 26.03.2026).
4. Espinoza M., Champod Ch., Margot P. Vulnerabilities of fingerprint reader to fake fingerprints attacks. *Forensic Science International*. 2011. Vol. 204. Is. 1—3. Pp. 41—49. DOI: 10.1016/j.forsciint.2010.05.002 (дата звернення: 26.03.2026).
5. Fingerprint Synthesis and Spoof Detection / Advances in Biometrics. Pp. 385—406. URL: https://link.springer.com/chapter/10.1007/978-1-84628-921-7_20 (дата звернення: 26.03.2026).
6. Nelson J., Luck A., Candies V. Fingerprint Spoof Detection Using Machine Learning and Multimodal Biometrics. 2024. URL: https://www.researchgate.net/publication/393607962_Fingerprint_Spoof_Detection_Using_Machine_Learning_and_Multimodal_Biometrics (дата звернення: 26.03.2026).