

**Хамітов Віталій Миколайович**, аспірант кафедри інформаційних систем, Національний університет «Одеська політехніка», Одеса, Україна

**Болтъонков Віктор Олексійович**, кандидат технічних наук, доцент, доцент кафедри інформаційних систем, Національний університет «Одеська політехніка», Одеса, Україна

## **ФОРМУВАННЯ ІНТЕГРАЛЬНОГО ПОКАЗНИКА ЯКОСТІ ШИФРУВАННЯ ЗОБРАЖЕНЬ**

У деяких сегментах глобального трафіку зображень по відкритих каналах зв'язку передаються зображення, які потребують конфіденційності. До таких сегментів, наприклад, відносяться телемедицина, передачі супутникових зображень, інтернет речей. У цьому випадку зображення піддаються шифруванню. Виникають ситуації, коли потрібно порівняти варіанти шифрування за якістю. Це порівняння є багатокритеріальним. У цьому зазвичай застосовуються такі критерії.

1. Кореляція. Якісний алгоритм шифрування має максимально знизити кореляцію між сусідніми пікселями. Коефіцієнт кореляції вказує на лінійний зв'язок між сусідніми пікселями. При ефективному шифруванні він має бути близьким до нуля.

Коефіцієнт кореляції розраховується за такими співвідношеннями:

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)D(y)}}, cov(x,y)=E(x-E(x)y-E(y)), E(x) = \frac{1}{N} \sum_{i=1}^N x_i,$$
$$E(y) = \frac{1}{N} \sum_{i=1}^N y_i, D(x) = \frac{1}{N} \sum_{i=1}^N [x_i - E(x)]^2, D(y) = \frac{1}{N} \sum_{i=1}^N [y_i - E(y)]^2,$$

де  $x$  і  $y$  – пара сусідніх пікселів,  $E(x)$  та  $E(y)$  – математичне очікування інтенсивності пікселів,  $D(x)$  та  $D(y)$  – дисперсія інтенсивності. Для

врахування кореляції між сусідніми пікселями коефіцієнт кореляції повинен оцінюватися для всіх можливих геометричних розташувань сусідніх пікселів : горизонтального –  $r_{xy}^{horiz}$ , вертикального –  $r_{xy}^{vert}$ , діагонального –  $r_{xy}^{diag}$ , антидіагонального –  $r_{xy}^{diag}$ . Для оцінки найбільш «слабкого» напрямку придушення кореляції пікселів вихідного зображення запропоновано розраховувати максимальний коефіцієнт кореляції

$$r_{xy}^{max} = \max(r_{xy}^{vert}, r_{xy}^{horiz}, r_{xy}^{diag}, r_{xy}^{diag}).$$

2. Інформаційна ентропія зашифрованого зображення. Інформаційна ентропія зашифрованого зображення  $C$  розраховується як:

$$H(C) = \sum_{i=0}^{2^N-1} p(m_i) \log \frac{1}{p(m_i)} (bit),$$

$N$  - кількість різних значень пікселів (  $N = 256$  для 8-бітного зображення). Для ідеального шифру  $H(C) = 8$  біт.

3. Локальна ентропія. Більш точною мірою випадковості зашифрованого зображення є ентропія, розрахована локальними блоками зображення. Навіть якщо зашифроване зображення має дуже високу ентропію Шеннона по всьому зображенню, зображення може містити деякі блоки з низькою ентропією. У цьому сенсі воно не є ідеально зашифрованим, незалежно від того, наскільки високою є його глобальна ентропія. Локальна ентропія розраховується за співвідношенням

$$\overline{H(C)} = \sum_{i=1}^k \frac{H(S_k)}{k} (bit),$$

де  $S_1, S_2, \dots, S_k$ - випадково вибрані  $k$  блоків зображення, що не перекриваються, з  $T_B$  пікселями кожен, які знаходяться всередині зашифрованого зображення. Обчислюються  $H(S_k)$   $i \in \{1, 2, \dots, k\}$  і далі оцінюється  $\overline{H(C)}$ . Для ідеального шифру  $\overline{H(C)}$  також 8 біт.

Критерії резистентності до атак.

4. Критерій *NPCR* (Number of Pixels Change Rate) використовується для оцінки лавинного ефекту алгоритму шифрування. Вона вимірює, наскільки сильно змінюється зашифроване зображення після шифрування при зміні одного пікселя у вихідному зображенні. Формується відповідно до алгоритму шифрування зашифроване зображення  $C^{(1)}$ . Далі у вихідному зображенні змінюється один піксель і для зміненого зображення формується зашифроване зображення  $C^{(2)}$ . *NPCR* розраховується як

$$NPCR = \frac{1}{N} \sum_{i=1}^N \left( \frac{C^{(1)} \otimes C^{(2)}}{255} \right) \cdot 100\%,$$

де  $N$  – число пікселів у зображенні,

$\otimes$  - Операція XOR.

*NPCR* показує, яка частка пікселів змінилася за зміни одного біта у вихідному зображенні. Теоретичне ідеальне значення *NPCR* 99.6%.

5. Критерій *UACI* (Unified Average Changing Intensity ) використовується для оцінки якості шифрування зображень, вимірюючи, наскільки сильно змінюється інтенсивність пікселів при зміні одного пікселя у вихідному зображенні. *UACI* розраховується за співвідношенням:

$$UACI = \frac{1}{N} \sum_{i=1}^N \left( \frac{C^{(1)} - C^{(2)}}{255} \right) \cdot 100\%.$$

Теоретичне ідеальне значення *UACI* 33.4% (у припущенні, що інтенсивність пікселів  $C^{(1)}$  має  $C^{(2)}$  рівномірний розподіл).

Для всебічної оцінки якості шифрування зображення запропоновано таку систему оцінки якості, засновану на перелічених критеріях :

$$\begin{cases} Crit_1 = r_{xy}^{max} \\ Crit_2 = H(C) \\ Crit_3 = \overline{H(C)} \cdot \\ Crit_4 = NPCR \\ Crit_5 = UACI \end{cases}$$

При порівняльному аналізі якості шифру з відомими алгоритмами шифрування багатокритеріальна система складна винесення рішення про

перевагу тієї чи іншої варіанта. Запропоновано сформувавши інтегрований показник якості шифрування на основі набору критеріїв. Це здійснено формуванням згортки критеріїв. Для формування згортки застосовано метод відстані від ідеальної точки. Ідеальною точкою називається вектор значень критеріїв, у якому кожен із  $n$  критеріїв досягає свого найкращого значення  $Crit_i^{ideal\_point}, i = \overline{1, n}$ . Тоді інтегральний показник якості  $IntQI$

$$IntQI = \left( \sum_{i=1}^n \lambda_i^p (Crit_i - Crit_i^{ideal\_point})^p \right)^{\frac{1}{p}},$$

де  $\lambda_i, i = \overline{1, n}$  – нормуючі (зважуючі) коефіцієнти,

$p$  – натуральний показник ступеня.

Застосовуючи до останнього виразу норму  $L_2$ , маємо

$$IntQI = \sqrt{\sum_{i=1}^5 \lambda_i^2 (Crit_i - Crit_i^{ideal\_point})^2}.$$

З досвіду  $\lambda_4$  моделювання систем шифрування прийняті такі значення нормуючих коефіцієнтів:  $\lambda_1 = 10^4$ ,  $\lambda_2 = 10^5 \text{ bit}^{-1}$ ,  $\lambda_3 = 10^4 \text{ bit}^{-1}$ ,  $\lambda_4 = 10^2$ ,  $\lambda_5 = 10^2$ . При таких значеннях нормуючих коефіцієнтів значення  $IntQI$  більшості систем шифрування становлять 25...50. Зазначимо, що для розрахунку  $IntQI$  критерії  $NPCR$  і  $UACI$  беруться не у відсотковому виразі, а у вигляді десяткового дробу.

Застосування в практичному шифруванні зображень запропонованого інтегрального показника якості шифрування показало його переваги при спрощенні процесу вибору найкращого варіанту шифрування зображень.

**Vydavatel:**

Publishing house Education and Science s.r.o. IČO : 271 56 877.  
Frýdlanská 15/1314 , Praha 8. MS v Praze , oddíl C, vložka 100614

# **Global Interdisciplinary Summit: Frontier of Science and Future Technologies**

**Proceedings of International Scientific and  
Practical Conference**

**April 3, 2026 in Khalifa University Campus,  
Dubai, UAE**

Signed for printing on April 6, 2026.  
Format 60x90/8. Headset Times New Roman.  
Mental printing. arc. 5,65. Edition online.