1. ГОСТ 13109-97. Электрическая энергия. Совместимость технических средств электромагнитная. Нормы качества электрической энергии в системах электроснабжения общего назначения. – Введ. 01.01.2000. – К.: Держстандарт України, 1999. – 32 с. 2. ГОСТ 23875-88. Качество электрической энергии. Термины и определения. – Введ. 01.07.89. – М.: Изд-во стандартов, 1988. – 16 с. 3. Ванько В.М., Столярчук П.Г. Проблеми контролю якості електроенергії в електричних мережах // Вимірювальна техніка та метрологія. – 2001. – №58. – С. 47-56. 4. Ванько В.М., Чайковський О.І. Інформаційно-вимірювальна система діагностики статичних і динамічних характеристик якості електроенергії // Праці 2-ї Укр. конф. з автоматичного керування "Автоматика-95". Львів, 26-30 вересня 1995р. – Том 2. – Львів: НВЦ "ІТІС". – 1995. – С. 76-77. 5. ГОСТ 30206-94. Статические счетчики ватт-часов активной енергии переменного тока (классы точности 0.2 и 0.5). – Введ. 19.01.2001. – К.: Держстандарт України, 2001. – 51 с. 6. ГОСТ 27487-87. Электрооборудование производственных машин. Общие технические требования и методы испытаний. – Введ. 01.07.88. – М: Изд-во стандартов, 1988. – 96 с. 7. Гурвич И.С. Защита ЭВМ от внешних помех. – 2-е изд., перераб. и доп. – М.: Энергоатомиздат, 1984. – 224с.

УДК 004.932.4; 004.415.2; 004.415.3

А. Ковальчук, Д. Пелешко
Національний університет " Львівська політехніка ",
кафедра інформаційних технологій видавничої справи

ВИКОРИСТАННЯ МАТРИЦЬ АДАМАРА ДЛЯ ШИФРУВАННЯ – ДЕШИФРУВАННЯ ЗОБРАЖЕНЬ

Описано використання апарату матриць Адамара для шифрування – дешифрування зображень. Шифрування – дешифрування проводиться без і з додатковим зашумленням.

Ключові слова: шифрування, дешифрування, матриця Адамара, зашумлення.

We describe the use of Hadamard matrices apparatus for encryption - decryption of images. Encryption - decryption is performed without and with additional noise.

Keywords: encryption, decryption, Hadamard matrix, noise.

Вступ

Вважатимемо, що зображенню відповідає матриця інтенсивностей кольорів

$$\mathbf{C}=\begin{pmatrix} c_{1,1} & \dots & c_{1,m} \\ \dots & \dots & \dots \\ c_{n,1} & \dots & c_{n,m} \end{pmatrix}.$$

Важливою характеристикою зображення є наявність в зображенні контурів. Задача виділення контура вимагає використання операцій над сусідніми елементами, які є чутливими до змін і пригашають області постійних рівнів яскравості, тобто, контури – це ті області, де виникають зміни, стаючи світлими, тоді як інші частини зображення залишаються темними [2].

Математично ідеальний контур – це розрив просторової функції рівнів яскравості в площині зображення. Тому виділення контура означає пошук найбільш різких змін, тобто максимумів модуля вектора градієнта [2].

Відносно зображення існують певні проблеми його шифрування, а саме частково зберігаються контури на різко флуктуаційних зображеннях [3, 4]. Однією з причин, через що контури залишаються в зображенні під час шифрування в системі RSA, є та, що шифрування тут ґрунтується на піднесенні до степеня за модулем деякого натурального числа. При цьому, на контурі і на сусідніх до контура пікселах піднесення до степеня значення яскравостей дає ще більший розрив.

1. Матриці Адамара

Матриці Адамара – в математиці це ортогональні квадратні матриці, елементи яких можуть набувати значень тільки (+1) та (-1). Названі на честь французького математика Жака Адамара.

Такі матриці застосовуваться в алгоритмах коригування помилок (коди Адамара, коди Ріда–Мюллера).

Матриця Адамара ***H*** порядку ***n*** задовольняє рівняння:

$$H^{\mathrm{T}} H = nI,$$

де ***I*** – одинична матриця розміру *n*.

Отже

$$\det H = \pm n^{n/2}.$$

Розмір матриць Адамара може бути 1, 2 чи бути кратним 4.

Будь-які два довільні стовпці чи рядки мають рівно половину збіжних пар елементів.

Одним з способів побудови матриць Адамара великих розмірностей є така рекурсивна процедура Сильвестра.

$$H_1 = 1;\ N = 2^{\mathrm{r}},\ H_N = \begin{bmatrix} H_{N/2} & H_{\mathrm{N/2}} \\ H_{\mathrm{N/2}} & H_{\mathrm{N/2}} \end{bmatrix};$$

$$H_2 \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix};\ H_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix};\ H_8 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix} \text{ і т.д.}$$

Кожний рядок матриці $\boldsymbol{H}_{\mathbf{N}}$ є множиною значень функцій Адамара:

$\boldsymbol{h}_0(x), \boldsymbol{h}_1(x), \ldots, \boldsymbol{h}_{N-1}(x)$. Для $\boldsymbol{N} = \mathbf{8}$ значення функцій Адамара такі:

$\boldsymbol{h}_0(x) = \{ 1 \ \ 1 \ \ 1 \ \ 1 \ \ 1 \ \ 1 \ \ 1 \ \ 1 \}$,

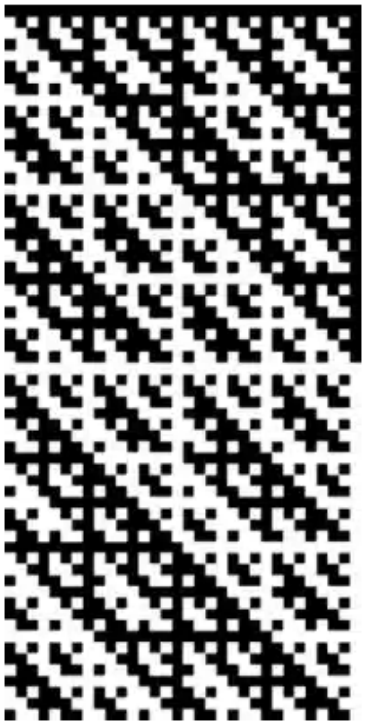
$\boldsymbol{h}_1(x) = \{ 1 \ -1 \ \ 1 \ \ -1 \ \ 1 \ -1 \ \ 1 \ -1 \}$,

$\boldsymbol{h}_2(x) = \{ 1 \ \ 1 \ -1 \ \ -1 \ \ 1 \ \ 1 \ -1 \ -1 \}$, і т.д.

Функції $\boldsymbol{h}_0(x), \boldsymbol{h}_1(x), \ldots, \boldsymbol{h}_7(x)$ називаються впорядкованими за Адамаром.

Функції $\boldsymbol{w}_0(x), \boldsymbol{w}_1(x), \ldots, \boldsymbol{w}_7(x)$ називаються впорядкованими за Уолшом, якщо $\boldsymbol{w}_0(x) = \boldsymbol{h}_0(x)$, $\boldsymbol{w}_1(x) = \boldsymbol{h}_4(x)$, $\boldsymbol{w}_2(x) = \boldsymbol{h}_6(x)$, $\boldsymbol{w}_3(x) = \boldsymbol{h}_2(x)$, $\boldsymbol{w}_4(x) = \boldsymbol{h}_3(x)$, $\boldsymbol{w}_5(x) = \boldsymbol{h}_7(x)$, $\boldsymbol{w}_6(x) = \boldsymbol{h}_5(x)$, $\boldsymbol{w}_7(x) = \boldsymbol{h}_1(x)$.

Під час візуалізації матриці Адамара створюється така картина



2. Шифрування

Нехай P і Q – пара довільних простих чисел. Виберемо числа

$$N = PQ, \varphi(N) = (P-1)(Q-1), ed \equiv 1 \ (mod\ \varphi(N)),$$

$$A = -P, B = -Q, C = d,\ D = e\ .$$

У кожному рядку матриці зображення вибираються чотири послідовні значення інтенсивностей пікселів $u_i, u_{i+1}, u_{i+2}, u_{i+3}$, $i = \overline{0, \dots, n-1}$, причому кожне значення інтенсивності вибирають тільки одного разу. Тоді отримуємо:

$$\begin{cases} v_i = Au_i + Bu_{i+1} + Cu_{i+2} + Du_{i+3} \\ v_{i+1} = Bu_i - Cu_{i+1} + Du_{i+2} - Au_{i+3} \\ v_{i+2} = Cu_i + Du_{i+1} - Au_{i+2} - Bu_{i+3} \\ v_{i+3} = Du_i - Au_{i+1} - Bu_{i+2} + Cu_{i+3} \end{cases}, \qquad (1)$$

де знаки вибирають відповідно до матриці Адамара H_4.

3. Дешифрування

Для дешифрування розв'язується система (1) лінійних рівнянь відносно $u_i, u_{i+1}, u_{i+2}, u_{i+3}$, $i = \overline{0, \dots, n-1}$, з правими частинами $v_i, v_{i+1}, v_{i+2}, v_{i+3}$.

Тоді

$$u_i = \frac{\alpha}{a}, u_{i+1} = \frac{\beta}{a}, u_{i+2} = \frac{\gamma}{a}, u_{i+3} = \frac{\delta}{a}, \qquad (2)$$

де

$$a = \begin{vmatrix} A & B & C & D \\ B & -C & D & -A \\ C & D & -A & -B \\ D & -A & -B & C \end{vmatrix}, \alpha = \begin{vmatrix} v_i & B & C & D \\ v_{i+1} & -C & D & -A \\ v_{i+2} & D & -A & -B \\ v_{i+3} & -A & -B & C \end{vmatrix}, \beta = \begin{vmatrix} A & v_i & C & D \\ B & v_{i+1} & D & -A \\ C & v_{i+2} & -A & -B \\ D & v_{i+3} & -B & C \end{vmatrix},$$

$$\gamma = \begin{vmatrix} A & B & v_i & D \\ B & -C & v_{i+1} & -A \\ C & D & v_{i+2} & -B \\ D & -A & v_{i+3} & C \end{vmatrix}, \delta = \begin{vmatrix} A & B & C & v_i \\ B & -C & D & v_{i+1} \\ C & D & -A & v_{i+2} \\ D & -A & -B & v_{i+3} \end{vmatrix}$$

4.4. Шифрування – дешифрування з додатковим зашумленням

Якщо співвідношення (1) замінити на

$$\begin{cases} v_i = Au_i + Bu_{i+1} + Cu_{i+2} + Du_{i+3} + g(i) \\ v_{i+1} = Bu_i - Cu_{i+1} + Du_{i+2} - Au_{i+3} + f(i) \\ v_{i+2} = Cu_i + Du_{i+1} - Au_{i+2} - Bu_{i+3} + G(i) \\ v_{i+3} = Du_i - Au_{i+1} - Bu_{i+2} + Cu_{i+3} + F(i) \end{cases},$$

де $g(i), f(i), G(i), F(i)$ – деякі задані функції, то шифрування відбуватиметься з додатковим зашумленням.

Дешифрування здійснюється за формулами (2), де

$$\alpha = \begin{vmatrix} v_i - g(i) & B & C & D \\ v_{i+1} - f(i) & -C & D & -A \\ v_{i+2} - G(i) & D & -A & -B \\ v_{i+3} - F(i) & -A & -B & C \end{vmatrix}, \beta = \begin{vmatrix} A & v_i - g(i) & C & D \\ B & v_{i+1} - f(i) & D & -A \\ C & v_{i+2} - G(i) & -A & -B \\ D & v_{i+3} - F(i) & -B & C \end{vmatrix},$$

$$\gamma = \begin{vmatrix} A & B & v_i - g(i) & D \\ B & -C & v_{i+1} - f(i) & -A \\ C & D & v_{i+2} - G(i) & -B \\ D & -A & v_{i+3} - F(i) & C \end{vmatrix}, \delta = \begin{vmatrix} A & B & C & v_i - g(i) \\ B & -C & D & v_{i+1} - f(i) \\ C & D & -A & v_{i+2} - G(i) \\ D & -A & -B & v_{i+3} - F(i) \end{vmatrix}.$$

Результати шифрування-дешифрування наведено на рис. 1 – 6.

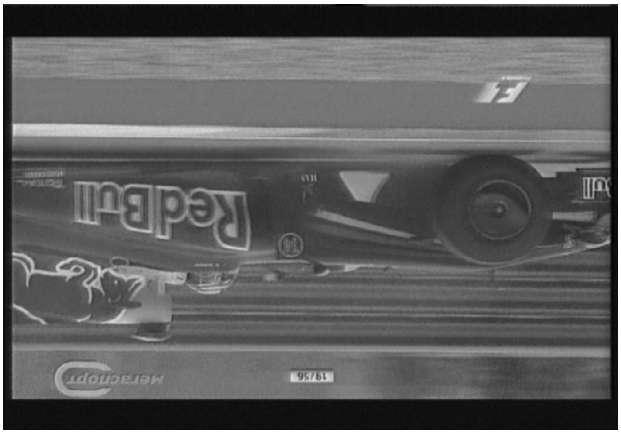


Рис. 1. Початкове зображення P = 3, Q =13

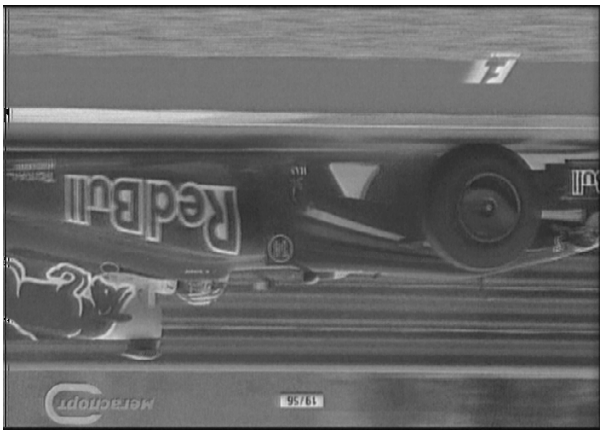


Рис.2. Дешифроване зображення P = 3, Q =13

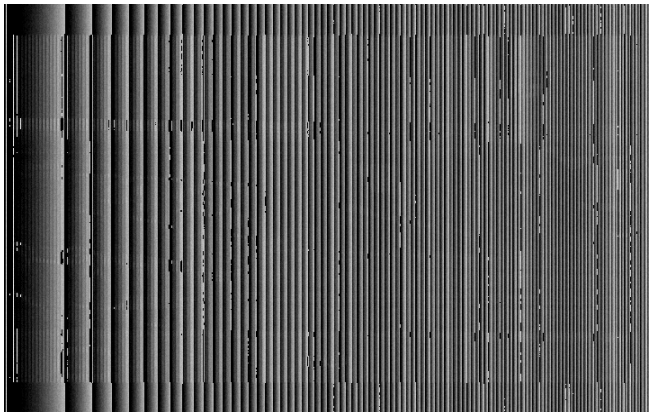


Рис. 3. Зашифроване зображення P = 3, Q =13

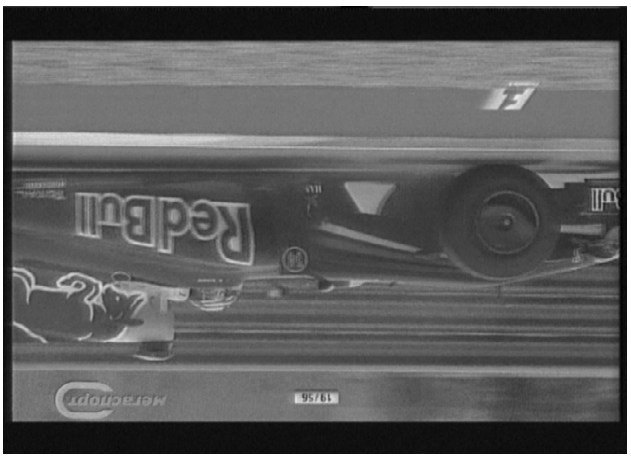


Рис. 4. Початкове зображення P = 31, Q = 47

Рис.5. Зашифроване зображення P = 31, Q =47

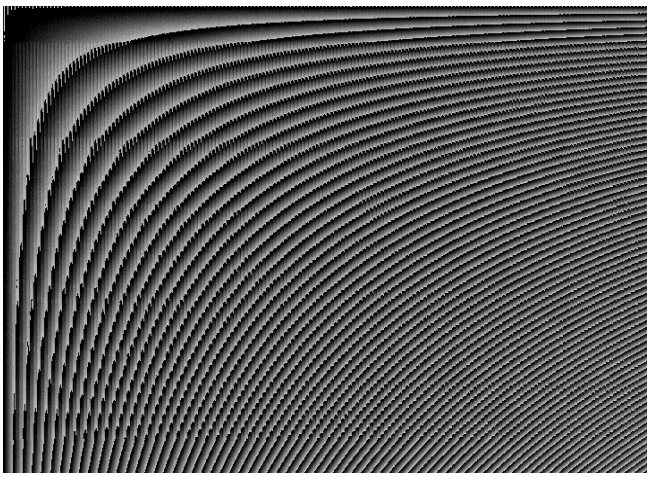


Рис. 6. Зашифроване зображення P = 31, Q = 47

Висновок

З рис. 3 і 6 видно, що шифрування без зашумлення відрізняється від шифрування з застосуванням додаткового зашумлення. Контури в усіх трьох зашифрованих зображеннях відсутні. Цей алгоритм може бути використаний для передавання графічних зображень. Запропоновані модифікації можна використати стосовно будь-якого типу зображень, але найбільших переваг досягають у випадку використання зображень, які дають змогу чітко виділяти контури.

Обидві модифікації можна використати і стосовно кольорових зображень. Однак, незалежно від типу зображення, пропорційно до розмірності вхідного зображення може зрости розмір шифрованого зображення.

1. Яне Б. Цифровая обработка изображений. – М., Техносфера, 2007. – 583 с. 2. Шнайер Б. Прикладная криптография. – М.: Триумф, 2003. – 815 с. 3. Ковальчук А., Пелешко Д., Хомин М., Борзов Ю. Поєднання алгоритму RSA і побітових операцій при шифруванні-дешифруванні зображень // Вісник НУ "Львівська політехніка". – № 694. – С. 309–313. 4. Rashkevych Y., Kovalchuk A., Peleshko D., Kupchak M. Stream Modification of RSA Algorithm For Image Coding with precize contour extraction. Proceedings of the X-th International Conference CADSM 2009. 24–28 February 2009, Lviv-Polyana, Ukraine, Pp. 469–473.