Применение гауссовых вращений для защиты графической информации*

А. Н. Каркищенко, В. Б. Мнухин
karkishalex@gmail.com; mnukhin.valeriy@mail.ru
Южный федеральный университет, Россия, г. Ростов-на-Дону, ул. Большая Садовая, 105/42

Рассматриваются цифровые изображения над «конечными комплексными полями». Вводится преобразование *гауссова вращения* таких изображений и доказывается, что при определенных условиях его результат напоминает несколько уменьшенных и повернутых копий оригинала, несмотря на то что эти «копии» образованы различными пикселями. Рассмотрена возможность создания на основе гауссовых вращений защитных фонов и текстур для предотвращения несанкционированного изменения документов. Приведен метод верификации защищенных таким образом документов.

Ключевые слова: *цифровое изображение; конечные поля; гауссовы целые; вращение; защита документов; стеганография*

DOI: 10.21469/22233792.3.1.05

1 Введение

Интенсивно происходящий во всем мире процесс построения «информационного общества» делает актуальными задачи разработки и исследования новых методов работы с дискретной информацией, в частности методов решения задач обработки, распознавания и классификации цифровых изображений. В настоящее время такие задачи, как правило, решаются в предположении непрерывности заданного изображения, что позволяет применять мощный аппарат классического математического анализа и интегральных преобразований. Однако на практике применение подобных методов неизбежно приводит к появлению систематических ошибок, связанных с дискретностью реальных изображений и невозможностью адекватного переноса на дискретный случай многих понятий непрерывной математики.

В качестве примера укажем на такие понятия, как вращение и полярная система координат на плоскости. Будучи естественными и элементарными в непрерывном случае $\mathbb{R}^2$, они утрачивают эти качества на дискретной плоскости $\mathbb{Z}^2$ [1, с. 568]. Традиционные методы вращения цифровых изображений основаны, как правило [2, с. 390], на формальном округлении результатов непрерывных вращений; ряд работ посвящен альтернативным методам, основанным на преобразовании Фурье, функциях Эрмита и пр. [3–7].

В связи с этим возникает задача разработки методов, изначально ориентированных на цифровые изображения и опирающихся на аппарат алгебры и теории чисел. В частности, использование различных теоретико-числовых преобразований над конечными полями позволяет проводить быстрые и безошибочные вычисления на основе модулярной арифметики [8–11].

Рассматриваемый в данной работе метод основан на использовании конечых полей, обладающих свойствами, до некоторой степени аналогичными свойствам непрерывного комплексного поля. Такие «конечные комплексные плоскости» имеют характеристику $p = 4k + 3 \geqslant 3$ и могут рассматриваться как дискретные торы $\mathbb{Z}_p \times \mathbb{Z}_p$, а функции на

*Работа выполнена при поддержке РФФИ, проекты № 16-07-00648-а и № 17-20-02017-офи_м_РЖД.

них — как цифровые изображения. Идея построения таких полей восходит, по-видимому, к работе [12] и затем развивалась в работах [13–19] и др. Учитывая связь этих полей с целыми гауссовыми числами [20], будем называть их *конечными гауссовыми полями*

Как известно, вращения на непрерывной комплексной плоскости $\mathbb{C}$ сводятся к умножению на числа $w \in \mathbb{C}$ с единичным модулем, $|w| = 1$. Естественно возникающая идея рассмотреть преобразование $f(z) \to f(wz)$ над гауссовыми полями послужила мотивацией данной работы. Как оказалось, такие *гауссовы вращения* в некоторых случаях действительно напоминают непрерывные. Точнее говоря, для больших p и при определенных w результат гауссова вращения изображения напоминает несколько уменьшенных и повернутых копий оригинала, несмотря на то что эти «копии» образованы *различными* пикселями. В других случаях гауссовы вращения приводят к существенным искажениям.

Основным результатом работы является строгое доказательство упомянутых выше свойств гауссовых вращений (ранее в [14–17] эти свойства обсуждались без корректных доказательств). Рассмотрена возможность создания на основе гауссовых вращений защитных фонов и текстур для предотвращения несанкционированного изменения документов. Предложен метод верификации защищенных таким образом документов.

2 Конечные поля целых гауссовых чисел

Как обычно, далее $\mathbb{Z}$ и $\mathbb{C}$ обозначают соответственно кольцо целых и поле комплексных чисел. Кольцо классов вычетов по модулю целого $n > 1$ условимся обозначать как $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$, а конечное поле из p^m элементов — как $\mathbb{GF}(p^m)$, где p — простое и $m > 0$.

Напомним, что в теории чисел [20, Ch. 1.4] *гауссовыми целыми* называются комплексные числа $z = a+bi \in \mathbb{C}$ с целыми a и b. Множество $\mathbb{Z}[i]$ таких чисел замкнуто относительно сложения и умножения, но деление в $\mathbb{Z}[i]$, вообще говоря, не определено. Заметим, что $\mathbb{Z}[i]$ можно рассматривать как квадратную решетку на комплексной плоскости. Это позволяет сопоставлять пикселям цифрового изображения гауссовы целые и рассматривать преобразования изображений, соответствующие операциям в кольце $\mathbb{Z}[i]$. Подобный подход был предложен Г. Бейкером [21] в 1993 г., однако отсутствие деления в $\mathbb{Z}[i]$ существенно ограничивает применимость метода. Естественно возникает мысль об использовании для обработки изображений конечных полей, аналогичных, в каком-то смысле, полю $\mathbb{C}$.

Для построения таких полей заметим, что если для целого $k \geqslant 0$ число $p = 4k + 3$ оказывается простым, то над полем $\mathbb{Z}_p$ многочлен x^2+1 будет неприводимым [22]. Вспоминая алгебраический метод построения поля комплексных чисел, приходим к следующему определению.

Определение 1. *Пусть простое $p \geqslant 3$ удовлетворяет условию $p \equiv 3 \pmod 4$. Тогда конечное поле*

$$\mathbb{C}(p) \stackrel{\text{def}}{=\!=} \mathbb{Z}_p[x]/(x^2 + 1) \simeq \mathbb{GF}(p^2)$$

будем называть гауссовым полем.

Таким образом, конечные гауссовы поля имеют p^2 элементов, где $p = 3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83, 103, \ldots$; всего для $3 \leqslant p < 1000$ существует 87 полей $\mathbb{C}(p)$. Каждому $z = a + ib \in \mathbb{Z}[i]$ отвечает единственный элемент $\overline{z} = \overline{a} + \iota\,\overline{b}$ поля $\mathbb{C}(p)$, где $\overline{a}, \overline{b} \in \mathbb{Z}_p$ есть классы вычетов $a, b \in \mathbb{Z}$ по модулю p, а ι — класс вычетов x по модулю идеала $(x^2 + 1)$, так что $\iota^2 = \overline{-1} \in \mathbb{Z}_p$.

Условимся далее там, где это не может привести к недопониманию, отождествлять ι с i, а классы вычетов — с их представителями, обозначая элементы поля $\mathbb{C}(p)$ точно так же, как и гауссовы целые, например $1 + 2i \in \mathbb{C}(p)$. Учитывая аналогию $\mathbb{C}(p)$ с комплексным полем $\mathbb{C}$ и кольцом $\mathbb{Z}[i]$, будем называть элементы поля $\mathbb{C}_p$ *дискретными гауссовыми* или *дискретными комплексными* числами и использовать при работе с ними стандартную терминологию комплексного анализа. В частности, величину $N(z) = a^2 + b^2$ будем называть *нормой*.

3 Вращения изображений над гауссовыми полями

Пусть $f(z) : \mathbb{C}(p) \to \mathbb{R}^+$ — ограниченная действительнозначная функция, определенная на некотором гауссовом поле $\mathbb{C}(p)$ и принимающая только неотрицательные значения. Вспоминая интерпретацию элементов поля $\mathbb{C}(p)$ как пикселей, будем называть $f(z)$ *полутоновым цифровым изображением над полем* $\mathbb{C}(p)$. Такие изображения имеют размер $p \times p$, где $p \equiv 3 \pmod 4$. (Поскольку на практике всякое изображение можно вложить в бóльшее требуемого размера, последнее условие не является ограничением.) Условимся рассматривать изображения над $\mathbb{C}(p)$ как совокупность квадратных пикселей на дискретном торе $\mathbb{Z}_p \times \mathbb{Z}_p$. Будем называть подмножество $D \subseteq \mathbb{C}(p)$ *связным*, если пиксели, отвечающие элементам D, образуют на торе односвязную область.

Заметим, что операции поля $\mathbb{C}(p)$ порождают преобразования изображений. Например, сложению следующим образом отвечает циклический сдвиг: для каждого $w = a+bi \in \mathbb{C}(p)$ рассмотрим преобразование $\mathcal{T}_w : f(z) \to f(z+w)$. Тогда изображение $\mathcal{T}_w[f]$ есть исходный образ $f(z)$, сдвинутый циклически на a единиц вдоль «действительной» оси и на b единиц вдоль «мнимой» оси. Будем называть $\mathcal{T}_w[f]$ *сдвигом изображения f на w*. Как очевидно, сдвиги обратимы: $\mathcal{T}_w^{-1} = \mathcal{T}_{-w}$.

В этой работе нас будет интересовать преобразование $f(z) \to f(wz)$, порождаемое умножением в поле $\mathbb{C}(p)$. Известно, что для *непрерывного* изображения на комплексной плоскости $\mathbb{C}$ подобное преобразование при $0 \neq w = re^{i\alpha} \in \mathbb{C}$ является композицией вращения на угол α вокруг начала координат и масштабирования на r, однако в *дискретном случае* корректное определение вращения и масштабирования оказывается нетривиальным [7, p. 377]. Тем не менее сходство между $\mathbb{C}$ и $\mathbb{C}(p)$ наводит на мысль, что некоторые свойства преобразования $f(z) \to f(wz)$ могут оказаться аналогичными вращениям и в дискретном случае.

Определение 2. *Пусть $f(z)$ — цифровое изображение на гауссовом поле $\mathbb{C}(p)$ и пусть w — ненулевой элемент этого поля. Преобразование $\mathscr{R}_w : f(z) \to f(wz)$ изображения $f(z)$ будем называть его гауссовым вращением на $0 \neq w \in \mathbb{C}(p)$.*

Непосредственно из определения вытекает обратимость гауссовых вращений:

$$\mathscr{R}_w^{-1} = \mathscr{R}_{w^{-1}} \qquad \text{для } 0 \neq w \in \mathbb{C}(p)\ .$$

Таким образом, изображение $\mathscr{R}_w[f]$ полностью сохраняет всю информацию об оригинале и является просто перестановкой его пикселов.

Рассмотрим примеры гауссовых вращений. На рис. 1 показаны изображение креста на поле $\mathbb{C}(71)$ и его образ при вращении на $w = 1 + 2i \in \mathbb{C}(71)$. Вполне предсказуемо по аналогии с непрерывным случаем результат можно рассматривать как непрерывное вращение на угол $\operatorname{arctg} 2$, совмещенное с пятикратным увеличением площади. Однако конечность $\mathbb{C}(p)$ приводит, как правило, к значительным искажениям при гауссовых вращениях. Это демонстрируется на рис. 2, где оригинал показан на рис. 2, *а*. (Важно отметить, что, поскольку изображения заданы на дискретном торе $\mathbb{Z}_{251} \times \mathbb{Z}_{251}$, их противоположные края следует считать склеенными.) На рис. 2, *б* показан результат вращения изображения

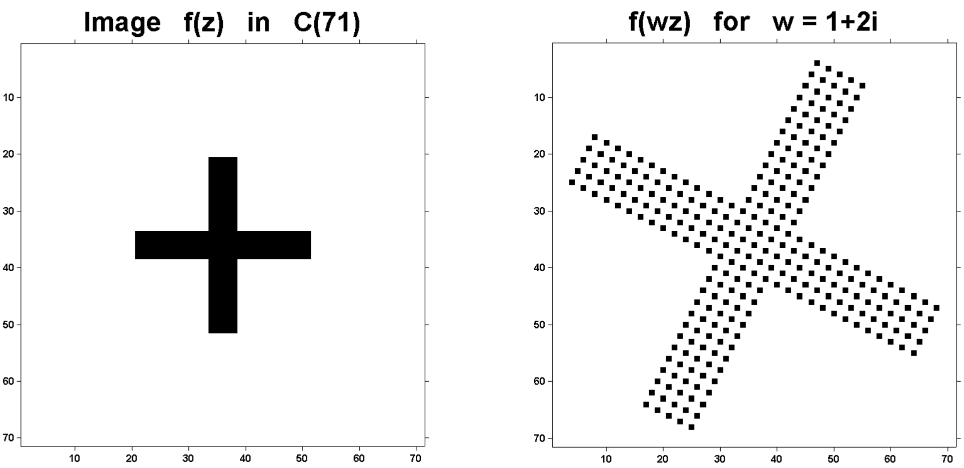


Рис. 1 Пример гауссова вращения над полем $\mathbb{C}(71)$

Ленны на $w = 1+i$. При этом оригинал поворачивается на 45° и «увеличивается» в $\sqrt{2}$ раз, однако конечность тора приводит к взаимопроникновению частей изображения, вызывая его визуальные искажения. (Увеличенный фрагмент исходного изображения различим в левом нижнем углу рис. 2, *б*.) Изображение на рис. 2, *г* соответствует $w = 9 + 13i$, когда искажения оказываются настолько значительными, что результат вращения теряет всякое сходство с оригиналом и выглядит как экзотический орнамент.

На фоне предыдущих примеров несколько парадоксальным выглядит результат вращения на $w = -50+100i = (1+2i)^{-1} \in \mathbb{C}(251)$, показанный на рис. 2, *в*. Визуально он состоит из четырех уменьшенных версий исходного изображения и ряда фрагментов, в совокупности на торе составляющих пятую. Заметим, что эти части изображения, выглядящие одинаковыми, составлены из различных пикселей оригинала. Более того, поскольку общее число пикселей равно p^2, части не могут содержать одно и то же число пикселей.

Следующая теорема объясняет предыдущий пример и демонстрирует его общность.

Теорема 1. *Пусть дано конечное гауссово поле $\mathbb{C}(p)$ и изображение f на нем. Пусть $u = c + di \in \mathbb{Z}[i]$ — гауссово целое такое, что $0 < c, d < p$ и $\gcd(c, d) = 1$. Пусть $\overline{u} \in \mathbb{C}(p)$ — отвечающий элемент поля $\mathbb{C}(p)$, а $w = 1/\overline{u} \in \mathbb{C}(p)$ — обратный к $\overline{u}$ элемент. Тогда если норма u равна $N \in \mathbb{Z}$, то изображение $\mathscr{R}_w[f]$ на торе $\mathbb{Z}_p \times \mathbb{Z}_p$ состоит из N связных непересекающихся частей таких, что пиксели, смежные в одной части, в исходном изображении f находятся на манхэттенском расстоянии $c + d$ друг от друга.*

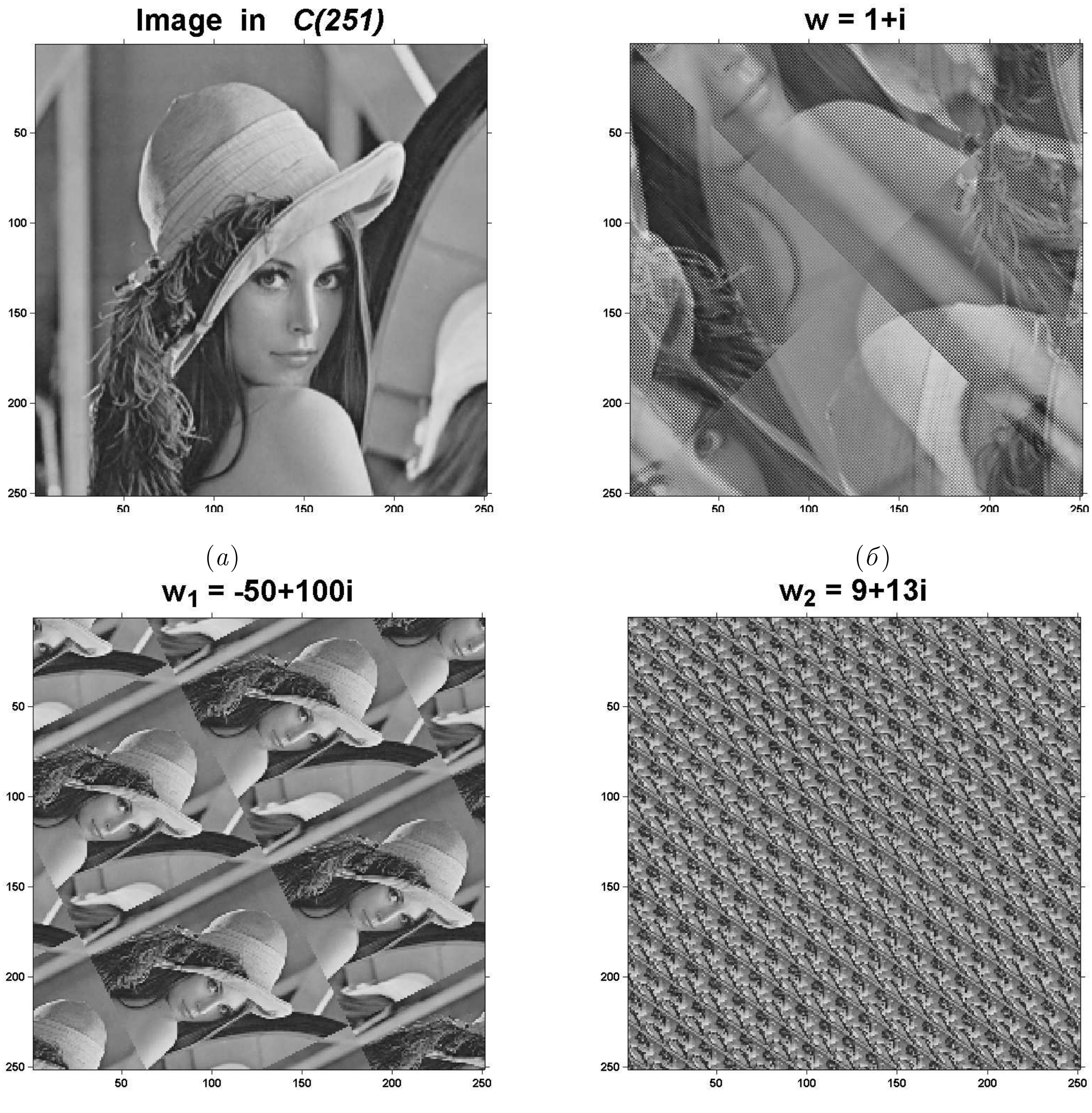
В случае $p \gg 1$ и $N \ll p$ эти части визуально представляются копиями изображения f, повернутого на угол $\operatorname{arctg}(d/c)$ и уменьшенного в $\sqrt{N}$ раз.

Доказательству теоремы посвящен следующий раздел, при первом чтении его можно пропустить. Отметим, что аналоги гауссовых вращений можно ввести и в конечных полях целых Эйзенштейна. Такие *эйзенштейновские вращения* гексагональных изображений рассматривались в [23, 24].

4 Доказательство теоремы

Пусть

$$\Gamma \stackrel{\text{def}}{=\!=} \Big\{ \; a + ib \; : \; a, b \in \mathbb{Z}, \; 0 \leqslant a, b < p \; \Big\} \subset \mathbb{C}$$



(а) (б) (в) (г)

Рис. 2 Гауссовы вращения на $\mathbb{C}(251)$

есть множество гауссовых целых в области $[0, p-1] \times [0, p-1]$ на комплексной плоскости. Будем рассматривать эту квадратную область как развертку дискретного тора $\mathbb{Z}_p \times \mathbb{Z}_p$. Понятно, что между Γ и $\mathbb{C}(p)$ существует взаимно-однозначное соответствие.

На первом этапе доказательства будет построено разбиение множества $\mathbb{Z}[i]$ на N классов, после чего эти классы будут ограничены на Γ и тем самым перенесены на гауссово поле $\mathbb{C}(p)$. Для построения разбиения напомним [25, гл. 1.1], что множество L точек на плоскости $\mathbb{R}^2$ называется *целочисленной решеткой*, если найдутся два линейно независимых вектора $\boldsymbol{v}_1, \boldsymbol{v}_2 \in \mathbb{R}^2$ таких, что

$$L = \left\{ \, a\boldsymbol{v}_1 + b\boldsymbol{v}_2 \ : \ a, b \in \mathbb{Z} \, \right\} \subset \mathbb{R}^2 \, .$$

Упорядоченная пара $\mathscr{B} = \langle \boldsymbol{v}_1, \boldsymbol{v}_2 \rangle$ называется *базисом* решетки L, а область $\Phi_{\mathscr{B}} = \{\alpha_1\boldsymbol{v}_1 + \alpha_2\boldsymbol{v}_2 \ : \ 0 \leqslant \alpha_1, \alpha_2 < 1 \,\} \subset \mathbb{R}^2$ — ее *фундаментальным параллелограммом.* Хотя решетка может порождаться различными базисами и иметь разные фундаментальные параллелограммы, их площадь остается постоянной. Элементы из L называют *узлами* решетки. В частности, $\mathbb{Z}[i]$ можно рассматривать как решетку с базисом $\mathbf{1} = (1, 0)$ и $\boldsymbol{i} = (0, 1)$. Ее фундаментальным параллелограммом является единичный квадрат с вершиной в $(0, 0)$.

Рассмотрим менее тривиальный пример. Для этого с ненулевым гауссовым числом $u = c + di \in \mathbb{Z}[i]$ свяжем два ортогональных вектора $\boldsymbol{v}_1 = (c, d)$ и $\boldsymbol{v}_2 = (-d, c)$ и рассмотрим решетку $\Lambda(u) \subset \mathbb{Z}[i]$ с базисом $\mathscr{B} = \langle \boldsymbol{v}_1, \boldsymbol{v}_2 \rangle$.

Лемма 1. *Если* $\gcd(c, d) = 1$, *то внутри фундаментального параллелограмма* $\Phi_{\mathscr{B}}$ *решетки* $\Lambda(u)$ *находится ровно* $N - 1$ *узлов решетки* $\mathbb{Z}[i]$.

Доказательство. Понятно, что $\Phi_{\mathscr{B}}$ представляет собой квадрат со сторонами $\boldsymbol{v}_1$ и $\boldsymbol{v}_2$, имеющий площадь

$$\big|[\boldsymbol{v}_1, \boldsymbol{v}_2]\big| = \begin{vmatrix} c & -d \\ d & c \end{vmatrix} = c^2 + d^2 = N(u) = N \, .$$

Тогда, согласно формуле Пика [26],

$$N = r + \frac{s}{2} - 1 \, ,$$

где r — число узлов решетки внутри $\Phi_{\mathscr{B}}$; s — число узлов на его границе. Взаимная простота чисел c и d означает, что единственными точками на границах фундаментального параллелограмма являются его вершины, так что $s = 4$. Следовательно, $r = N - 1$, что завершает доказательство леммы.

Далее будем считать узлы решеток целыми гауссовыми числами. Тогда $\mathbb{Z}[i]$ является абелевой группой относительно сложения, а $\Lambda(u)$ — ее подгруппой. Нетрудно заметить, что индекс $\Lambda(u)$ в $\mathbb{Z}[i]$ равен $N(u)$:

$$\big|\, \mathbb{Z}[i]/\Lambda(u) \,\big| = N(u) \, ,$$

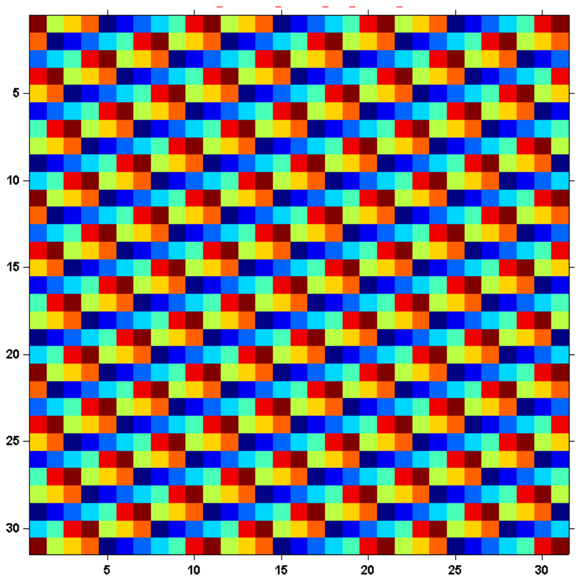
причем классы смежности имеют вид:

$$\Lambda_k(u) = h_k + \Lambda(u), \qquad k = 0, \ldots, N(u) - 1 \, ,$$

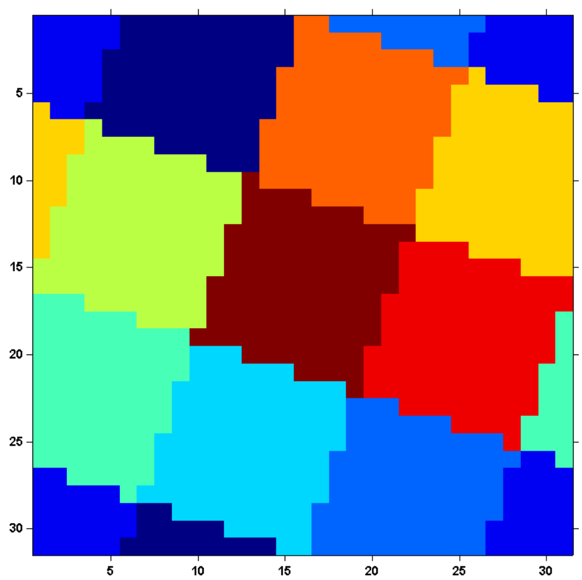
где $h_0 = 0$, а числа h_k при $k \geqslant 1$ соответствуют внутренним узлам фундаментального параллелограмма $\Phi_{\mathscr{B}}$.

Каждый класс смежности $\Lambda_k(u)$ содержит бесконечное число узлов решетки $\mathbb{Z}[i]$. Ограничим классы на множество Γ, оставляя в каждом классе только узлы, лежащие внутри квадрата $[0, p-1] \times [0, p-1]$. Поскольку между Γ и $\mathbb{C}(p)$ существует естественное взаимно-однозначное соответствие, каждый ограниченный класс $\Lambda_k(u) \cap \Gamma$ определяет множество $\Theta_k(u) \subset \mathbb{C}(p)$. Тем самым получаем разбиение поля $C(p)$ на непересекающиеся классы:

$$\mathbb{C}(p) = \bigcup_{k=0}^{N-1} \Theta_k(u) \, , \qquad \Theta_k(u) \cap \Theta_l(u) = \varnothing \quad \text{при } k \neq l.$$



(*а*)



(*б*)

Рис. 3 Разбиение поля $\mathbb{C}(31)$ для $u = 3 + i$ (*а*) и его образ при вращении на $w = u^{-1}$ (*б*)

Разумеется, эти классы не обязаны иметь одно и то же число элементов. Такое разбиение поля $\mathbb{C}(31)$ для $u = 3 + i$ показано на рис. 3, *а*, где пиксели, соответствующие элементам одного класса, имеют одно и то же значение, различное для разных классов. В результате все 10 классов показаны различными псевдоцветами, в частности класс $\Theta_0(u)$ показан коричневым. Этот класс содержит 97 элементов, а все остальные — по 96.

На рис. 3, *б* показан результат гауссова вращения изображения (см. рис. 3, *а*) на $w = 1/\overline{u} \in \mathbb{C}(31)$. Видно, что это вращение «собирает вместе» элементы классов $\Theta_k(u)$, формируя из них связные на торе блоки пикселей.

Покажем справедливость сделанного выше наблюдения в общем случае. Для этого заметим, что решетку $\Lambda(u)$ можно задать и следующим образом:

$$\Lambda(u) = \left\{ a\boldsymbol{v}_1 + b\boldsymbol{v}_2 \ : \ a, b \in \mathbb{Z} \right\} = \left\{ uz \ : \ z = a + ib \in \mathbb{Z}[i] \right\},$$

так что

$$\Theta_k(u) = \left\{ \overline{h}_k + \overline{uz} \ : \ z \in \mathbb{Z}[i] \quad \text{такое, что } uz \in \Gamma \right\},$$

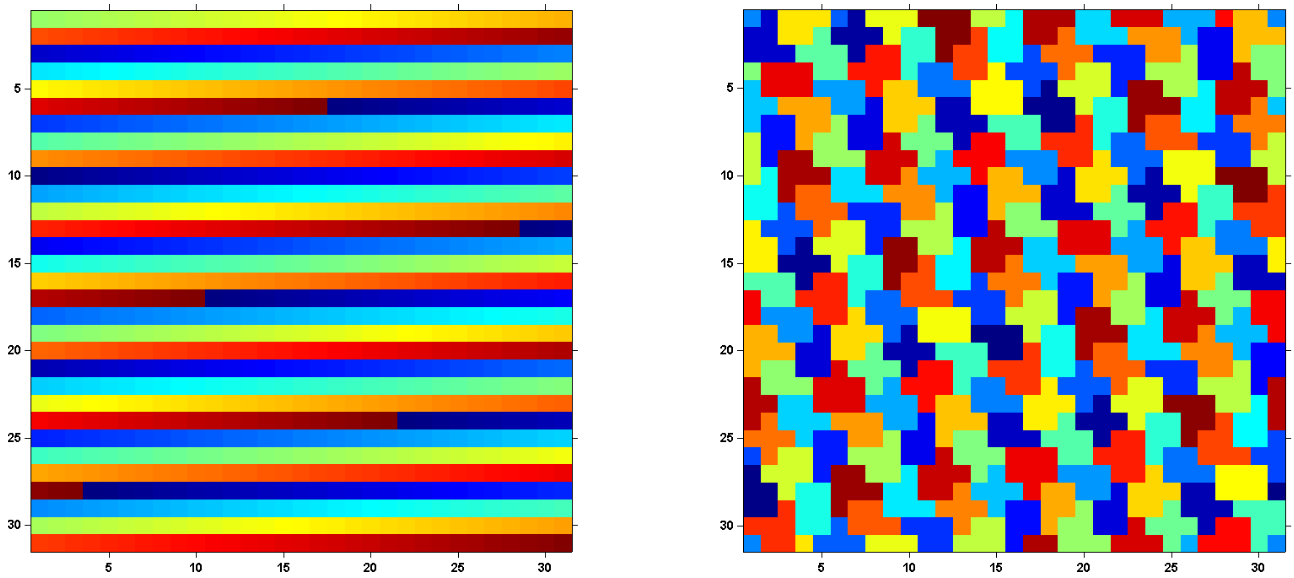
и, поскольку $w\overline{u} = 1$,

$$\mathscr{R}_w\big[\Theta_k(u)\big] = w\Theta_k(u) = \left\{ w\overline{h}_k + \overline{z} \ : \ uz \in \Gamma \text{ для } z \in \mathbb{Z}[i] \right\}.$$

Здесь z пробегает элементы связного множества, поэтому связным будет и множество $\mathscr{R}_w\big[\Theta_k(u)\big]$. Тем самым гауссово поле $\mathbb{C}(p)$ разбивается на непересекающиеся связные фрагменты.

Пусть теперь $x, y \in \mathbb{C}(p)$ — два смежных в классе $\mathscr{R}_w\big[\Theta_k(u)\big]$ пикселя, тогда $x - y = \pm 1$ или $x - y = \pm i$. Поскольку $\mathscr{R}_w^{-1} = \mathscr{R}_{w^{-1}} = \mathscr{R}_{\overline{u}}$, до вращения этим пикселам отвечали $\mathscr{R}_w^{-1}[x] = \overline{u}x$ и $\mathscr{R}_w^{-1}[y] = \overline{u}y$, причем

$$\mathscr{R}_w^{-1}[x] - \mathscr{R}_w^{-1}[y] = \overline{u}x - \overline{u}y = \overline{u}(x - y) = \pm\overline{u} \quad \text{или} \quad \pm\, i\overline{u}\,.$$



(*а*) (*б*)

Рис. 4 Разбиение поля $\mathbb{C}(31)$ для $u = 7+11i$ с $N = 170$ (*а*) и его образ при гауссовом вращении (*б*)

Поскольку $u = c+id$, пиксели $\mathscr{R}_w^{-1}[x]$ и $\mathscr{R}_w^{-1}[y]$ на торе находятся на манхэттенском расстоянии $c+d < N$ друг от друга, поэтому для малых N и достаточно больших p фрагменты $\mathscr{R}_w\big[\Theta_k(u)\big]$ выглядят идентичными исходному изображению. Это завершает доказательство теоремы.

Заметим, что для больших N искажения при гауссовых вращениях могут быть весьма значительными. Пример этого показан на рис. 4, где $u = 7+11i$ и значение $N = 170$ велико по сравнению с $p = 31$. После вращения изображение разбивается на 170 фрагментов, один из которых содержит 4 пиксела, 73 — по 5 пикселей, 80 — по 6, и 16 — по 7 пикселей.

5 Защита документов на базе гауссовых вращений

Рассмотренные выше свойства гауссовых вращений позволяют использовать их для защиты документов путем создания на их основе защитных сеток и текстур [27] (рис. 5 и 6). Рисунок 5 демонстрирует пример защитной сетки, состоящей из визуально неразличимых, но *различных* фрагментов. Тем самым сетку невозможно воссоздать, просто копируя уменьшенные и повернутые копии исходного изображения. Рисунок 6 показывает, как повернутое должным образом изображение можно превратить в декоративный фон, позволяющий полностью воссоздать оригинал и тем самым не позволяющий вносить в него изменения. При этом параметр поворота может быть каким-либо образом связан с особенностями изображения, скажем, быть результатом хеширования даты рождения изображенного лица.

Покажем, как провести верификацию защищенного таким образом документа. Ключевой идеей является введение в гауссовых полях «комплексного логарифма». Вспомним вначале, как это делается на непрерывной комплексной плоскости.

Пусть $\mathbb{C}^*$ — мультипликативная группа комплексного поля, а $\mathbb{R} = \langle \mathbb{R}, + \rangle$ — аддитивная группа поля действительных чисел. Заметим, что биекция

$$0 \neq z = re^{i\theta} = e^{\ln r + i\theta} \;\leftrightarrow\; (l, \theta),$$

(a) ($б$)

Рис. 5 Пример защитной сетки: (a) исходное изображение размера 751×751; ($б$) результат его вращения на $(3 + 2i)^{-1} \in \mathbb{C}(751)$

(a) ($б$)

Рис. 6 Пример защитной текстуры: (a) изображение Elaine на поле $\mathbb{C}(503)$; ($б$) его поворот на $w = (37 + 31i)^{-1} \in \mathbb{C}(503)$

где $l = \ln r \in \mathbb{R}$ и $0 \leqslant \theta < 2\pi$, между ненулевыми комплексными числами z и их полярно-логарифмическими координатами (l, θ) порождает изоморфизм

$$\mathbb{C}^* \simeq \mathbb{R} \times (\mathbb{R}/2\pi\mathbb{Z}). \tag{1}$$

Перенесем предыдущую конструкцию на поле $\mathbb{C}(p)$. Для этого заметим, что его мультипликативная группа $\mathbb{C}^*(p) = \mathbb{C}(p) \setminus \{0\}$ является циклической [22, с. 314], и тем самым порождается некоторым примитивным элементом g. В частности, нетрудно проверить, что элементы $g = 2 + 7i$ и $p = 1 + 19i$ примитивны в $\mathbb{C}^*(71)$, а $g = 1 + 5i$ — примитивен для $p = 251$.

Следующий результат элементарно проверяется.

Лемма 2. *Для каждого $p = 4k + 3$ числа $m = (p - 1)/2 = 2k + 1$ и $n = 2(p + 1) = 8(k + 1)$ являются взаимно-простыми,* $\gcd(m, n) = 1$.

Поскольку $mn = p^2 - 1 = |\mathbb{C}^*(p)|$, отсюда немедленно вытекает [22, с. 163] следующий аналог разложения (1).

Утверждение 1. *Мультипликативная группа гауссового поля $\mathbb{C}(p)$ есть прямое произведение циклических групп порядков $m = (p - 1)/2$ и $n = 2(p + 1)$,*

$$\mathbb{C}^*(p) \simeq \mathbb{Z}_m \times \mathbb{Z}_n \,. \tag{2}$$

Будем называть (2) *полярным разложением* поля $\mathbb{C}(p)$. Перенесем с его помощью на $\mathbb{C}(p)$ понятие комплексного логарифма. Для этого определим отображение $\mathrm{Exp}_g : \mathbb{Z}_m \times \times \mathbb{Z}_n \to \mathbb{C}^*(p)$ следующим образом:

$$\mathrm{Exp}_g(l, \theta) = g^{nl+m\theta} = z \in \mathbb{C}^*(p),$$

где $(l, \theta) \in \mathbb{Z}_m \times \mathbb{Z}_n$. Таким образом, Exp_g является изоморфизмом между аддитивной группой кольца $\mathbb{Z}_m \times \mathbb{Z}_n$ и мультипликативной группой поля $\mathbb{C}(p)$.

Определение 3. *Отображение $\mathrm{Exp}_g : \mathbb{Z}_m \times \mathbb{Z}_n \to \mathbb{C}^*(p)$ будем называть модулярной экспонентой по основанию g, а обратное отображение $\mathrm{Ln}_g : \mathbb{C}^*(p) \to \mathbb{Z}_m \times \mathbb{Z}_n$ — модулярным логарифмом по основанию g. Группу $\mathbb{Z}_m \times \mathbb{Z}_n$ назовем полярной областью поля $\mathbb{C}(p)$.*

Непосредственно из определения вытекает «основное логарифмическое тождество»:

$$\mathrm{Ln}_g(z_1 z_2) = \mathrm{Ln}_g(z_1) + \mathrm{Ln}_g(z_2) \,. \tag{3}$$

Заметим, что $\mathrm{Ln}_g(0)$ не определен, а для нахождения $(l, \theta) = \mathrm{Ln}_g(z)$ для произвольного $z = g^s \in \mathbb{C}^*(p)$ необходимо решить диофантово уравнение $nx + my = s$ и взять

$$(l, \theta) = (x \mod m \;,\; y \mod n) \in \mathbb{Z}_m \times \mathbb{Z}_n \,.$$

Пример 1. Пусть $g = 1 + 2i \in \mathbb{C}^*(7)$ и $z = g^2 = 4 + 4i$. Тогда $s = 2$, $m = 3$, $n = 16$ и уравнение $16x + 3y = 2$ имеет очевидное решение $x = 2$, $y = -10$. Следовательно, $\mathrm{Ln}_g(4 + 4i) = (2 \bmod 3 \;,\; -10 \bmod 16) = (2, 6) \in \mathbb{Z}_3 \times \mathbb{Z}_{16}$.

Назовем пару $(l, \theta) \in \mathbb{Z}_m \times \mathbb{Z}_n$ «полярно-логарифмическими координатами» элемента $z \in \mathbb{C}^*(p)$ на полярной области.

Рассмотрим изображение f в новых координатах, определив функцию $\psi : \mathbb{Z}_m \times \mathbb{Z}_n \to \mathbb{R}$ так, что

$$\psi(\mathrm{Ln}_g(z)) = f(z), \qquad 0 \neq z \in \mathbb{C}^*(p) \,.$$

Определение 4. *Преобразование $\mathscr{P}_g[f] \stackrel{\text{def}}{=\!=} \psi$ назовем полярно-логарифмическим преобразованием f по основанию g или просто полярным преобразованием. Изображение ψ на торе $\mathbb{Z}_m \times \mathbb{Z}_n$ будем называть полярной формой для f.*

Следующее утверждение показывает, что преобразование $\mathscr{P}$ действительно может считать дискретным аналогом перехода в полярно-логарифмическую систему координат. Его доказательство немедленно следует из «основного логарифмического тождества» (3).

Утверждение 2. *Если* $\mathscr{P}_g\big[f(z)\big] = \psi(l,\theta)$, *то*

$$\mathscr{P}\big[f(wz)\big] = \psi(l - l_0, \theta - \theta_0)\ ,$$

где $0 \neq w \in \mathbb{C}(p)$ *и* $\mathrm{Ln}(w) = (l_0, \theta_0)$.

Другими словами, справедливо

Следствие 1. *Гауссов поворот изображения равносилен циклическому сдвигу его полярной формы.*

Как хорошо известно [28], циклические сдвиги изображений легко распознаются, например, с помощью преобразования Фурье. В частности, модули Фурье-образов изображений на рис. 5 и 6 совпадают, а их различие означало бы попытку взлома защитной сетки или текстуры. Более того, анализ Фурье-образов позволяет определить и параметр поворота w, тем самым верифицируя подлинность защитной текстуры.

Заметим, что методы защиты информации на конечных полях, использующие преобразования, отличные от гауссовых вращений, рассматривались в [29–31].

6 Заключение

В работе рассмотрено преобразование цифровых изображений над «конечными комплексными полями», называемое *гауссовым вращением* и строящееся как формальный аналог вращения в непрерывной комплексной плоскости. Доказано, что при определенных условиях результат такого «вращения» напоминает несколько уменьшенных и повернутых копий оригинала, несмотря на то что эти «копии» образованы различными пикселями. Рассмотрена возможность создания на основе гауссова вращения защитных фонов и текстур для предотвращения несанкционированного изменения документов. Приведен метод верификации защищенных таким образом документов.

Авторы благодарят неизвестного рецензента за замечания, способствовавшие улучшению работы.

Литература

[1] *Hoggar S. G.* Mathematics of digital images: Creation, compression, restoration, recognition. — Cambridge: Cambridge University Press, 2006. 854 p.

[2] *Pratt W. K.* Digital image processing. — John Wiley & Sons, 2007. 782 p.

[3] *Owen C., Makedon F.* High quality alias free image rotation // 30th Asilomar Conference on Signals, Systems, and Computers Proceedings. — Pacific Grove, CA, USA, 1996.

[4] *Larkin K., Oldfield M., Klemm H.* Fast Fourier method for the accurate rotation of sampled images // Opt. Commun., 1997. Vol. 139. P. 99–106.

[5] *Cox R. W., Tong R.* Two and three dimensional image rotation using the FFT // IEEE T. Image Proc., 1999. Vol. 8. No. 9. P. 1297–1299.

[6] *Park W., Leibon G., Rockmore D. N., Chirikjian G. S.* Accurate image rotation using hermite expansions // IEEE T. Image Proc., 2009. Vol. 18. No. 9. P. 1988–2003.

[7] *Каркищенко А. Н., Мнухин В. Б.* Топологическая фильтрация для распознавания и анализа симметрии цифровых изображений // Машинное обучение и анализ данных, 2014. Т. 1. № 8. С. 966–987.

[8] *Лабунец В. Г.* Теоретико-числовые преобразования над квадратичными полями // Сложные системы управления. — Киев: Институт кибернетики УССР, 1982. С. 30–37.

[9] *Вариченко Л.В., Лабунец В. Г., Раков М.А.* Абстрактные алгебраические системы и цифровая обработка сигналов. — Киев: Наукова Думка, 1986. 248 с.

[10] *Чернов В. М. Корепанов А. О.* Теоретико-числовые преобразования в задачах цифровой обработки сигналов. — Самара: Изд-во СГАУ, 2006. 112 с.

[11] *Чернов В. М.* Арифметические методы синтеза быстрых алгоритмов дискретных ортогональных преобразований. — М.: Физматлит, 2007. 264 с.

[12] *Campello de Souza R. M., de Oliveira H. M., Kauffman A. N.* Trigonometry in finite fields and a new Hartley transform // Symposium (International) on Information Theory Proceedings. — Cambridge, MA, USA, 1998. P. 293.

[13] *Bandeira J., Campello de Souza R.* New trigonometric transforms over prime finite fields for image filtering // 6th Telecommunications Symposium (International) Proceedings. — Fortaleza-Ce, Brazil, 2006. P. 628–633. doi: 10.1109/ITS.2006.4433235.

[14] *Мнухин В. Б.* Цифровые изображения на комплексном дискретном торе // Машинное обучение и анализ данных, 2013. Т. 1. №5. С. 542–551.

[15] *Каркищенко А. Н., Мнухин В. Б.* Применение модулярных логарифмов на комплексных дискретных торах в задачах обработки цифровых изображений // Вестник Ростовского гос. ун-та путей сообщения, 2013. Т. 3. С. 147–153.

[16] *Mnukhin V. B.* Fourier–Mellin transform on a complex discrete torus // 11th Conference (International) "Pattern Recognition and Image Analysis: New Information Technologies" Proceedings. — Samara, 2013. P. 102–105. doi: 10.13140/RG.2.1.4366.4086.

[17] *Mnukhin V. B.* Transformations of digital images on complex discrete tori // Pattern Recognition Image Anal., 2014. Vol. 24. No. 4. P. 552–560. doi: 10.1134/S1054661814040142.

[18] *Campello de Souza R. M., de Oliveira H. M., Silva D.* The Z transform over finite fields. arXiv preprint 1502.03371, 2015.

[19] *Karkishchenko A. N., Mnukhin V. B.* Fourfold symmetry detection in digital images based on finite Gaussian fields // Adv. Intell. Syst., 2016. Vol. 451. P. 153–162. doi: 10.1007/978-3-319-33816-3_16.

[20] *Ireland K., Rosen M.* A classical introduction to modern number theory. — New York, NY, USA: Springer, 1994. 416 p.

[21] *Baker H. G.* Complex Gaussian integers for Gaussian graphics // ACM Sigplan Notices, 1993. Vol. 28. No. 11. P. 22–27.

[22] *Dummit D. S., Foote R. M.* Abstract algebra. — John Wiley & Sons, 2004. 932 p.

[23] *Karkishchenko A. N., Mnukhin V. B.* Threefold symmetry detection in hexagonal images based on finite Eisenstein fields // Comm. Com. Inf. Sc., 2017. Vol. 661. P. 281–292. doi: 10.1007/978-3-319-52920-2_26.

[24] *Karkishchenko A. N., Mnukhin V. B.* Hexagonal images processing over finite Eisenstein fields // Procedia Engineer., 2017. Vol. 201. P. 287–295. doi: 10.1016/j.proeng.2017.09.633.

[25] *Conway J. H., Sloane N. J. A.* Sphere-packings, lattices, and groups. — New York, NY, USA: Springer-Verlag, 1987. 792 p.

[26] *Barvinok, A.* Integer points in polyhedra. — Zuerich, Switzerland: European Mathematical Society Publishing House, 2008. 199 p. doi: 10.4171/052.

[27] *Cheddad A., Condell J., Curran K., Mc Kevitt P.* Digital image steganography: Survey and analysis of current methods // Signal Process., 2010. Vol. 90. No. 3. P. 727–752. doi: 10.1016/j.sigpro.2009.08.010.

[28] *Easton R. L., Jr.* Fourier methods in imaging. — John Wiley & , 2010. 930 p.

[29] *Lima J. B., de Souza R. M.* Histogram uniformization for digital image encryption // 25th SIBGRAPI Conference on Graphics, Patterns and Images Proceedings. — Washington, D.C., USA: IEEE Computer Society, 2012. P. 55–62. doi: 10.1109/SIBGRAPI.2012.17.

[30] *Lima J. B., Lima E. A. O., Madeiro F.* Image encryption based on the finite field cosine transform // Image Commun., 2013. Vol. 2. No. 10. P. 1537–1547. doi: 10.1016/j.image.2013.05.008.

[31] *Lima J. B., Madeiro F., Sales F. J. R.* Encryption of medical images based on the cosine number transform // Image Commun., 2015. Vol. 35. No. 3. P. 1–8. doi: 10.1016/j.image.2015.03.005.

Поступила в редакцию 01.09.2017

Gaussian rotations for graphic information protection*

A. N. Karkishchenko and V. B. Mnukhin

karkishalex@gmail.com; mnukhin.valeriy@mail.ru

Southern Federal University, 105/42 Bolshaya Sadovaya Str., Rostov-on-Don, Russia

Digital images over "finite complex planes" are considered jointly with transformations of *Gaussian rotations*. It is proved that under some special conditions, results of such transformations seem to be formed by several zoomed out copies of the rotated original, though all such "copies" are formed by different pixels of the original image. Based on Gaussian rotations, some methods for tamper resistent protection of graphic information are considered. A method for verification of protected information is also introduced.

Keywords: *digital image; finite field; Gaussian integers; rotations; security printing; steganography*

DOI: 10.21469/22233792.3.1.05

References

[1] Hoggar, S. G. 2006. *Mathematics of digital images: Creation, compression, restoration, recognition.* Cambridge: Cambridge University Press. 854 p.

[2] Pratt, W. K. 2007. *Digital image processing*. John Wiley & Sons. 782 p.

[3] Owen, C., and F. Makedon. 1996. High quality alias free image rotation. *30th Asilomar Conference on Signals, Systems, and Computers Proceedings*. Pacific Grove, CA.

[4] Larkin, K., M. Oldfield, and H. Klemm. 1997. Fast Fourier method for the accurate rotation of sampled images. *Opt. Commun.* 139:99–106.

[5] Cox, R. W., and R. Tong. 1999. Two and three dimensional image rotation using the FFT. *IEEE T. Image Proc.* 8(9):1297–1299.

[6] Park, W., G. Leibon, D. N. Rockmore, and G. S. Chirikjian. 2009. Accurate image rotation using hermite expansions. *IEEE T. Image Proc.* 18(9):1988–2003.

[7] Karkishchenko, A. N., and V. B. Mnukhin. 2014. Topologicheskaya fil'tratsiya dlya raspoznavaniya i analiza simmetrii tsifrovykh izobrazheniy [Topological filtration for digital images recognition and symmetry analysis]. *J. Machine Learning Data Anal.* 1(8):966–987.

*The research was supported by the Russian Foundation for Basic Research (grants 16-07-00648 and 17-20-02017).

[8] Labunets, V. 1982. Teoretiko-chislovye preobrazovaniya nad kvadratichnumi polyami [Number-theoretic transforms over quadratic fields]. *Slozhnye sistemy upravleniya* [Complex Control Systems]. Kiev: Institute of Cybernetics of the USSR. 30–37.

[9] Varitschenko, L., V. Labunets, and M. Rakov. 1986. *Abstraknye algebraicheskie sistemy i tsifrovaya obrabotks signalov* [Abstract algebraic systems and digital signal processing]. Kiev: Naukova Dumka. 248 p.

[10] Chernov, V. M., and A. O. Korepanov. 2006. *Teoretiko-chislovye preobrazovaniya v zadachakh tsifrovoy obrabotki signalov* [Number-theoretic transforms in digital image processing]. Samara: SGAU. 112 p.

[11] Chernov, V. M. 2007. *Arifmeticheskie metody sinteza bystrykh algoritmov diskretnykh ortogonal'nykh preobrazovaniy* [Arithmetic methods for fast algorithms for discrete orthogonal transforms development]. Moscow: FIZMATLIT. 264 p.

[12] Campello de Souza, R. M., H. M. de Oliveira, and A. N. Kauffman. 1998. Trigonometry in finite fields and a new Hartley transform. *Symposium (International) on Information Theory Proceedings*. Cambridge, MA. 293.

[13] Bandeira, J., and R. Campello de Souza. 2006. New trigonometric transforms over prime finite fields for image filtering. *6th Telecommunications Symposium (International) Proceedings*. Fortaleza-Ce, Brazil. 628–633. doi: 10.1109/ITS.2006.4433235.

[14] Mnukhin, V. B. 2013. Tsifrovye izobrazheniya na kompleksnom diskretnom tore [Digital images on a complex discrete torus]. *J. Machine Learning Data Anal.* 1(5):540–548.

[15] Karkishchenko, A. N., and V. B. Mnukhin. 2013. Primenenie modulyarnykh logarifmov na konpleksnykh diskretnykh torakh v zadachakh obrabotki tsifrovykh izobrazheniy [Applications of modular logarithms on complex discrete tori in problems of digital image processing]. *Vestnik Rostovskogo gos. un-ta putey soobshcheniya* [Bull. of the Rostov State University of Railway Transport] 3:147–153.

[16] Mnukhin, V. B. 2013. Fourier–Mellin transform on a complex discrete torus. *11th Conference (International) "Pattern Recognition and Image Analysis: New Information Technologies" Proceedings*. Samara. 102–105. doi: 10.13140/RG.2.1.4366.4086.

[17] Mnukhin, V. B. 2014. Transformations of digital images on complex discrete tori. *Pattern Recognition Image Anal.* 24(4):552–560. doi: 10.1134/S1054661814040142.

[18] Campello de Souza, R. M., H. M. de Oliveira, and D. Silva. 2015. The Z transform over finite fields. arXiv preprint 1502.03371.

[19] Karkishchenko, A. N., and V. B. Mnukhin. 2016. Fourfold symmetry detection in digital images based on finite Gaussian fields. *Adv. Intell. Syst.* 451:153–162. doi: 10.1007/978-3-319-33816-3_16.

[20] Ireland, K., and M. Rosen. 1994. *A classical introduction to modern number theory*. New York, NY: Springer. 416 p.

[21] Baker, H. G. 1993. Complex Gaussian integers for Gaussian graphics. *ACM Sigplan Notices* 28(11):22–27.

[22] Dummit, D. S., and R. M. Foote. 2004. *Abstract algebra*. John Wiley & Sons. 932 p.

[23] Karkishchenko, A. N., and V. B. Mnukhin. 2017. Threefold symmetry detection in hexagonal images based on finite Eisenstein fields. *Comm. Com. Inf. Sc.* 661:281–292. doi: 10.1007/978-3-319-52920-2_26.

[24] Karkishchenko, A. N., and V. B. Mnukhin. 2017. Hexagonal images processing over finite Eisenstein fields. *Procedia Engineer.* 201:287–295. doi: 10.1016/j.proeng.2017.09.633.

[25] Conway, J. H., and N. J. A. Sloane. 1987. *Sphere-packings, lattices, and groups*. New York, NY: Springer-Verlag. 792 p.

[26] Barvinok, A. 2008. *Integer points in polyhedra*. Zuerich, Switzerland: European Mathematical Society Publishing House. 199 p. doi: 10.4171/052.

[27] Cheddad, A., J. Condell, K. Curran, and P. Mc Kevitt. 2010. Digital image steganography: Survey and analysis of current methods. *Signal Process.* 90(3):727–752. doi: 10.1016/j.sigpro.2009. 08.010.

[28] Easton, R. L. Jr. 2010. *Fourier methods in imaging*. John Wiley & Sons. 930 p.

[29] Lima, J. B., and R. M. de Souza. 2012. Histogram uniformization for digital image encryption. *25th SIBGRAPI Conference on Graphics, Patterns and Images Proceedings*. Washington, D.C.: IEEE Computer Society. 55–62. doi: `http://dx.doi.org/10.1109/SIBGRAPI.2012.17`

[30] Lima, J. B., E. A. O. Lima, and F. Madeiro. 2013. Image encryption based on the finite field cosine transform. *Image Commun.* 28(10):1537–1547. doi: 10.1016/j.image.2013.05.008.

[31] Lima, J. B., F. Madeiro, and F. J. R. Sales. 2015. Encryption of medical images based on the cosine number transform. *Image Commun.* 35(3):1–8. doi: 10.1016/j.image.2015.03.005.

Received September 01, 2017