ОПИСАНИЕ ПОЛЕЗНОЙ МОДЕЛИ К ПАТЕНТУ

(12)

РЕСПУБЛИКА БЕЛАРУСЬ

НАЦИОНАЛЬНЫЙ ЦЕНТР ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **BY** (11) **5665**

(13) **U**

(46) **2009.10.30**

(51) МПК (2006)
H 04K 1/02

(54) КРИПТОГРАФИЧЕСКИЙ КОДЕК ДЛЯ МУАРОВОГО МАСКИРОВАНИЯ ИЗОБРАЖЕНИЙ

(21) Номер заявки: u 20090252
(22) 2009.03.27

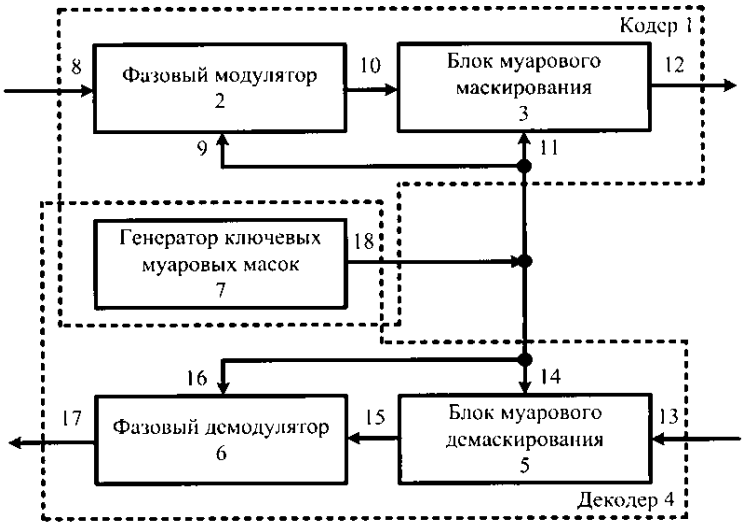
(71) Заявитель: Учреждение образования "Белорусский государственный университет информатики и радиоэлектроники" (BY)

(72) Авторы: Борискевич Анатолий Антонович; Цветков Виктор Юрьевич (BY)

(73) Патентообладатель: Учреждение образования "Белорусский государственный университет информатики и радиоэлектроники" (BY)

(57)

Криптографический кодек для муарового маскирования изображений, состоящий из кодера, включающего фазовый модулятор и блок муарового маскирования, декодера, включающего фазовый демодулятор и блок муарового демаскирования, и генератора ключевых муаровых масок, общего для кодера и декодера, причем первый вход фазового модулятора является входом кодера, выход фазового демодулятора является выходом декодера, вторые входы модулятора и демодулятора соединены с выходом генератора ключевых муаровых масок, **отличающийся** тем, что содержит блоки муарового маскирования и демаскирования, первый вход блока муарового маскирования соединен с выходом фазового модулятора, выход блока муарового маскирования является выходом кодера, первый вход блока муарового демаскирования является входом декодера, выход блока муарового демаскирования соединен со входом фазового демодулятора, вторые входы блоков муарового маскирования и демаскирования подключены к выходу генератора ключевых муаровых масок.



Фиг. 1

BY 5665 U 2009.10.30

(56)

1. Chen G., Mao Y., Chui C.K. A symmetric image encryption scheme based on 3D chaotic cat maps / Chaos, Solitons and Fractals 21, 2004. - P. 749-761.

2. Munoz-Rodriguez J.A., Rodriguez-Vera R. Image encryption based on moire pattern performed by computational algorithms / Optics Communications 236, 2004. - P. 295-301.

Полезная модель относится к области информационной безопасности и может быть использована в системах передачи и хранения данных для визуального шифрования цифровых изображений. Целью полезной модели является повышение уровня зашиты зашифрованных изображений от дешифрования, надежное визуальное маскирование высокочастотных объектов изображений и восстановление изображений без потерь в результате расшифрования. Данная цель достигается введением блоков муарового маскирования и демаскирования, а также использованием генератора ключевых муаровых масок, формируемых на основе обратимых целочисленных функций.

Известен криптографический кодек изображений, использующий множество трехмерных хаотических масок и состоящий из генератора ключей, блока преобразования данных, блока наложения маски и блока нормировки [1]. Однако данный кодек обладает низким быстродействием и значительной сложностью из-за итерационного характера процесса визуального шифрования изображений.

Наиболее близким к предлагаемой полезной модели является криптографический кодек изображений, использующий муаровые образы для восстановления изображений и состоящий из кодера, включающего фазовый модулятор, декодера, включающего сумматор и низкочастотный фильтр, и генератора двухмерных ключевых масок, общего для кодера и декодера, причем первый вход фазового модулятора является входом кодера, выход фазового модулятора является выходом кодера, первый вход сумматора является входом декодера, выход сумматора соединен со входом низкочастотного фильтра, выход которого является выходом декодера, вторые входы фазового модулятора и сумматора соединены с выходом генератора двухмерных ключевых масок [2]. Однако данный кодек имеет низкий уровень защищенности зашифрованных изображений от дешифрования без знания ключа и не обеспечивает надежное муаровое маскирование высокочастотных деталей изображений из-за использования генератора двухмерных ключевых масок, формируемых на основе необратимых гармонических функций, которые не устраняют психовизуальную избыточность. Данный кодек не позволяет восстановить без потерь зашифрованное изображение из муарового образа из-за использования низкочастотного фильтра в декодере.

Техническая задача, на решение которой направлена полезная модель, - создание криптографического кодека для шифрования изображений посредством их преобразования в муарограммы с помощью ключевых муаровых масок, формируемых на основе обратимых целочисленных функций. Техническим результатом, который может быть получен при использовании данной полезной модели, является повышение уровня защиты зашифрованных изображений от дешифрования, надежное муаровое маскирование высокочастотных деталей изображений, восстановление изображений без потерь в результате расшифрования и отсутствие эффекта размножения ошибок при передачи по каналу с помехами.

Поставленная задача решается тем, что криптографический кодек для муарового маскирования изображений, состоящий из кодера, включающего фазовый модулятор и блок муарового маскирования, декодера, включающего фазовый демодулятор и блок муарового демаскирования, и генератора ключевых муаровых масок, общего для кодера и декодера, причем первый вход фазового модулятора является входом кодера, выход фазового демодулятора является выходом декодера, вторые входы модулятора и демодулятора соедине-

ны с выходом генератора ключевых муаровых масок, отличающийся тем, что содержит блоки муарового маскирования и демаскирования, первый вход блока муарового маскирования соединен с выходом фазового модулятора, выход блока муарового маскирования является выходом кодера, первый вход блока муарового демаскирования является входом декодера, выход блока муарового демаскирования соединен со входом фазового демодулятора, вторые входы блоков муарового маскирования и демаскирования подключены к выходу генератора ключевых муаровых масок.

Сущность заявляемой полезной модели заключается в том, что предлагаемый криптографический кодек позволяет преобразовать изображение в муарограмму и восстановить изображение без потерь из муарограммы за счет использования генератора ключевых муаровых масок, формируемых на основе обратимых целочисленных функций.

Предложение иллюстрируется следующими чертежами. На фиг. 1 представлена структурная схема криптографического кодека для муарового маскирования изображений, на фиг. 2 - обратимые целочисленные функции, аппроксимирующие гармоническую функцию, на фиг. 3 - ключевые муаровые маски, на фиг. 4 - тестовое изображение, составная муаровая маска и составная муарограмма, на фиг. 5 - дешифрованные образы тестового изображения, извлеченные из муарограммы.

Криптографический кодек для муарового маскирования изображений состоит из кодера (1), включающего фазовый модулятор (2) и блок муарового маскирования 3, декодера (4), включающего блок муарового демаскирования 5 и фазовый демодулятор (6), и генератора ключевых муаровых масок (7), общего для кодера и декодера, причем первый вход 8 фазового модулятора (2) является входом кодера (1), выход 12 блока муарового маскирования 3 является выходом кодера (1), первый вход 13 блока муарового демаскирования 5 является входом декодера (4), выход 17 фазового демодулятора (6) является выходом декодера (4), второй вход 9 фазового модулятора (2), второй вход 16 фазового демодулятора (6), второй вход 11 блока муарового маскирования 3 и второй вход 14 блока муарового демаскирования 5 соединены с выходом 18 генератора ключевых муаровых масок (7) (фиг. 1).

В предложенном криптографическом кодеке для надежного муарового маскирования высокочастотных деталей изображения используются ключевые муаровые маски, формируемые с помощью обратимых целочисленных функций. На фиг. 2 в качестве примера представлены две обратимые целочисленные дискретные функции $F = \phi(d)$, аппроксимирующие гармоническую функцию, которая используется при моделировании муар-эффекта (муарового образа), где d - номер дискрета на периоде функции $\phi(d)$. Значения $b^K_{x,y}$ пикселей ключевой муаровой маски могут быть вычислены с помощью соотношения $b^K_{x,y} = \phi(D)$, где $D = (f_0 \cdot S(x,y,x_0,y_0,\varphi_0),Q_M)$ - точка в пространстве ключей; f_0 - частотный параметр, характеризующий частоту муаровых полос в маске; $S(x,y,x_0,y_0,\varphi_0)$ - структурная функция, определяющая форму муаровых полос; (x, y) - координаты пикселя в пространственной области; $x = \overline{0, X-1}$, $y = \overline{0, Y-1}$; $X \times Y$ - размер муарограммы, ключевой муаровой маски и шифруемого изображения; (x_0,y_0) - координаты центра поворота структуры муаровой маски; φ_0 - угол поворота структуры муаровой маски; Q_M - значение динамического диапазона муарограммы, равное значениям динамических диапазонов шифруемого изображения и муаровой маски. Множество всех возможных значений параметров ключевой муаровой маски $\{f_0, (x_0, y_0), \varphi_0\}$ образуют пространство секретных ключей, размер которого определяет криптостойкость муарограммы. Целочисленные значения функции $\phi(D)$, ограниченные динамическим диапазоном Q_M, могут быть вычислены с помощью выражения $\phi(D) = ([f_0 \cdot S(x,y,x_0,y_0, \varphi_0)])\mathrm{mod}Q_M$, где [•] - операция округления до ближайшего целого; $\mathrm{mod}Q_M$ - операция по модулю Q_M. Функция $S(x,y,x_0,y_0, \varphi_0)$ может быть задана, например, одним из следующих выражений:

$|c_x \cdot \cos(c_y)|$, $c_x \cdot \sqrt{c_x^2 + c_y^2}$, $c_x^2 + c_y^2$, $c_x \cdot c_y$, $|c_x \cdot \cos(c_x \cdot c_y)|$

и т.д., где $c_x = \frac{(x - x_0) \cdot \cos(\varphi_0) + (y - y_0) \cdot \sin(\varphi_0)}{S}$

и $c_y = \frac{(x - x_0) \cdot \sin(\varphi_0) - (y - y_0) \cdot \cos(\varphi_0)}{S}$ - структурные параметры, определяющие характер изменения структуры ключевой муаровой маски в направлении x и y; $|\cdot|$ - операция вычисления абсолютного значения; $S = \begin{cases} X \text{ при } X \geq Y, \\ Y \text{ при } X < Y. \end{cases}$ - размер квадратной муаровой маски, определяемый размером большей стороны шифруемого изображения. В качестве примера на фиг. 3 приведены полутоновые изображения ключевых муаровых масок $b_{x,y}^K$ для обратимой целочисленной функции, задаваемой выражением $\phi(D) = ([f_0 \cdot S(x, y, x_0, y_0, \varphi_0)])\bmod Q_M$, и структурной функции, задаваемой выражением $S(x,y,x_0,y_0,\varphi_0) = |c_x \cdot \cos(c_y)|$, при $Q_M = 256$, $\varphi_0 = 30°$, $x_0 = 0$, $y_0 = 0$ и $f_0 = \{10^4,10^6,10^8\}$. Защищенность зашифрованных изображений от дешифрования без знания ключа определяется количеством ключевых муаровых масок, которое зависит от чувствительности их маскирующих свойств к изменению параметров f_0, (x_0,y_0) и φ_0 и определяется с помощью выражения $V_K = V_{x,y} \cdot V_\varphi \cdot V_f$, где $V_{x,y} = X \cdot Y / \Delta s$ – число возможных центров поворота структуры муаровой маски; Δs - шаг сдвига центра поворота структуры муаровой маски по осям x и y; $V_\varphi = 360/\Delta\varphi$ - число возможных угловых ориентации структуры муаровой маски относительно центра поворота; $\Delta\varphi$ - шаг изменения угловой ориентации структуры муаровой маски; $V_f = (f_{max} - f_{min})/\Delta f$ - число возможных значений частотного параметра; f_{max} и f_{min} - максимальное и минимальное значения частотного параметра; Δf - шаг изменения частотного параметра. Для полутоновых изображений размером 512×512 пикселей чувствительность структуры ключевой муаровой маски к изменению начальных параметров f_0, (x_0,y_0) и φ_0 составляет соответственно $\Delta f \approx 5 \cdot 10^5$ (при $f_0 = \overline{10^3,10^{15}}$), $\Delta s \approx 5$ (при $x_0 = \overline{0,511}$, $y_0 = \overline{0,511}$) и $\Delta\varphi \approx 1°$ (при $\varphi_0 = \overline{0°,360°}$). Восстановление изображения невозможно, если значение хотя бы одного из секретных параметров f_0, (x_0,y_0) и φ_0 отличается от исходного значения более чем на установленные значения Δf, Δs и $\Delta\varphi$. Минимальное число ключевых муаровых масок для полутонового изображения с 8-битовым представлением пикселей размером 512×512 пикселей составляет $V_K = V_{X,Y} \cdot V\varphi \cdot V_f \approx 38 \cdot 10^{15} \approx 2^{55}$ из общего числа $2^{512 \times 512 \times 8} = 2^{2097152}$ возможных двухмерных ключей.

Криптографический кодек для муарового маскирования изображений работает следующим образом.

При зашифровании на первый вход 8 фазового модулятора (2) поступают значения $b_{x,y}^I$ пикселей шифруемого изображения. На второй вход 9 фазового модулятора (2) поступают значения $b_{x,y}^K$ пикселей маски, формируемой генератором ключевых муаровых масок (7). На выходе 10 фазового модулятора (2) формируются значения $b_{x,y}^{KI}$ пикселей модулированной муаровой маски, вычисляемые в соответствии с выражением $b_{x,y}^{KI} = \phi\left(f_0 \cdot S(x, y, x_0, y_0, \varphi_0) + b_{x,y}^I, Q_M\right)$. При вычислении значений функции $\phi(D)$ с использованием формулы $\phi(D) = ([f_0 \cdot S(x, y, x_0, y_0, \varphi_0)])\bmod Q_M$ значения $b_{x,y}^{KI}$ определяются с помощью выражения $b_{x,y}^{KI} = \left(f_0 \cdot S(x, y, x_0, y_0, \varphi_0) + b_{x,y}^I\right)\bmod Q_M = \left(b_{x,y}^K + b_{x,y}^I\right)\bmod Q_M$, где $b_{x,y}^K = (f_0 \cdot S(x, y, x_0, y_0, \varphi_0))\bmod Q_M$. С выхода 10 фазового модулятора (2) значения

$b^{KI}_{x,y}$ пикселей модулированной муаровой маски поступают на первый вход блока муарового маскирования 3. На второй вход 11 блока муарового маскирования 3 поступают значения $b^{K}_{x,y}$ пикселей маски, формируемой генератором ключевых муаровых масок (7) с секретными параметрами $\{f_0,(x_0,y_0),\varphi_0\}$. На выходе 12 блока муарового маскирования 3 формируются значения $b^{M}_{x,y}$ пикселей муарограммы, вычисляемые в соответствии с выражением $b^{M}_{x,y} = \left(b^{KI}_{x,y} + b^{K}_{x,y}\right) \bmod Q_M$. Муарограмма передается по каналу связи или записывается в память. В качестве примера на фиг. 4 представлены тестовое изображение, составная ключевая муаровая маска из шести частей и соответствующая маске составная муарограмма. Составная ключевая муаровая маска сформирована с помощью структурной функции вида $S(x,y,x_0,y_0,\varphi_0) = |c_x \cdot \cos(c_y)|$ при различных значениях частотного параметра f_0 и фиксированных значениях (x_0,y_0) и φ_0. В табл. 1 приведены значения частотного параметра f_0 для различных структурных частей ключевой муаровой маски и муарограммы, приведенных на фиг. 4 и определяемых координатами i и j.

Таблица 1

Значения частотного параметра f_0

j	0		1		2	
i	0	1	0	1	0	1
f	10^3	$2{,}5\cdot10^3$	$5\cdot10^3$	10^4	10^6	10^8

При расшифровании на первый вход 13 блока муарового демаскирования 5 поступают значения $b^{M}_{x,y}$ пикселей муарограммы. На второй вход 14 блока муарового демаскирования 5 поступают значения $b^{K}_{x,y}$ пикселей маски, формируемой генератором ключевых муаровых масок (7) с секретными параметрами $\{f_0,(x_0,y_0),\varphi_0\}$. На выходе 15 блока муарового демаскирования 5 восстанавливаются значения $b^{KIR}_{x,y}$ пикселей модулированной муаровой маски, вычисляемые в соответствии с выражением

$$b^{KIR}_{x,y} = \left(Q_M - 1 + b^{M}_{x,y} - b^{K}_{x,y}\right) \bmod Q_M = \left(Q_M - 1 + \left(b^{KI}_{x,y} + b^{K}_{x,y}\right) \bmod Q_M - b^{K}_{x,y}\right) \bmod Q_M.$$

С выхода 15 блока муарового демаскирования 5 значения $b^{KIR}_{x,y}$ пикселей восстановленной модулированной муаровой маски поступают на первый вход фазового демодулятора 6. На второй вход 16 фазового демодулятора (6) поступают значения $b^{K}_{x,y}$ пикселей маски, формируемой генератором ключевых муаровых масок (блок 7) с секретными параметрами $\{f_0,(x_0,y_0),\varphi_0\}$. На выходе 17 фазового демодулятора (6) формируются значения $b^{IR}_{x,y}$ восстановленных пикселей изображения, вычисляемые в соответствии с выражением $b^{IR}_{x,y} = \phi^{-1}\left(b^{KIR}_{x,y}, f_0 \cdot S(x,y,x_0,y_0,\varphi_0), Q_M\right)$. При вычислении значений функции $\phi(D)$ по формуле $\phi(D) = ([f_0 \cdot S(x,y,x_0,y_0,\varphi_0)]) \bmod Q_M$ значения $b^{IR}_{x,y}$ определяются с помощью выражения $b^{IR}_{x,y} = \left(Q_M - 1 + b^{KIR}_{x,y} - b^{K}_{x,y}\right) \bmod Q_M$. Для полного восстановления исходного изображения и обеспечения для $\forall x \forall y$ равенства $b^{IR}_{x,y} = b^{I}_{x,y}$ необходимо знание структурной функции $S(x,y,x_0,y_0,\varphi_0)$ и множества секретных параметров $\{f_0,(x_0,y_0),\varphi_0\}$. В качестве примера на фиг. 5 представлены дешифрованные образы тестового изображения, извлеченные из муарограммы, сформированной на основе обратимой целочисленной функции $\phi(D) = ([f_0 \cdot S(x,y,x_0,y_0,\varphi_0)]) \bmod Q_M$ и структурной функции $S(x,y,x_0,y_0,\varphi_0) = |c_x \cdot \cos(c_y)|$ при

следующих значениях ключевых параметров $f_0 = 10^6$, ($x_0 = 0$, $y_0 = 0$), $\varphi_0 = 0$ и незнании одного из параметров: f_0, (x_0,y_0) или φ_0. Ошибка дешифрования исходного изображения зависит от различий $\Delta f_0 = \left|f_0 - \tilde{f}_0\right|$, $\Delta x_0 = \left|x_0 - \tilde{x}_0\right|$, $\Delta y_0 = \left|y_0 - \tilde{y}_0\right|$ и $\Delta\varphi_0 = \left|\varphi_0 - \tilde{\varphi}_0\right|$ значений параметров $\tilde{f}_0, (\tilde{x}_0, \tilde{y}_0)$ и $\tilde{\varphi}_0$, подбираемых при дешифровании, от истинных ключевых значений f_0, (x_0,y_0) и φ_0.

Маскирующие свойства ключевых муаровых масок по отношению к высокочастотным деталям изображений зависят от статистических характеристик масок. Дня оценки статистических характеристик ключевых муаровых масок, а также шифруемых изображений и муарограмм целесообразно использовать энтропию H и дисперсию D энтропии, определяемые с помощью выражений $H = -\sum_{i=0}^{Q_M-1} p_i \cdot \log_2(p_i)$ и $D = \sum_{i=0}^{Q_M-1} p_i \cdot \left(-\log_2(p_i)\right)^2 - \left(\sum_{i=0}^{Q_M-1} p_i \cdot \left(-\log_2(p_i)\right)\right)^2$, где $p_i = \frac{l_i}{Y \cdot X}$ - вероятность появления i-го значения интенсивности пикселей исходного изображения, ключевой муаровой маски и муарограммы; l_i – число появлений пикселей с i-м значением интенсивности. В табл. 2 представлены значения статистических характеристик для тестового изображения, приведенного на фиг. 4, ключевой муаровой маски, сформированной с помощью обратимой функции $\phi(D) = ([f_0 \cdot S(x,y,x_0,y_0,\varphi_0)])\mathrm{mod}Q_M$ и структурной функции $S(x,y,x_0,y_0,\varphi_0) = |c_x \cdot \cos(c_y)|$ при $f_0 = 10^6$, ($x_0 = 0$, $y_0 = 0$), $\varphi_0 = 0$, и муарограммы.

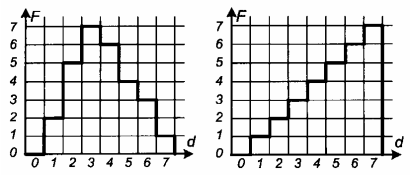
Таблица 2

Статистические характеристики тестового изображения, муаровой маски и муарограммы

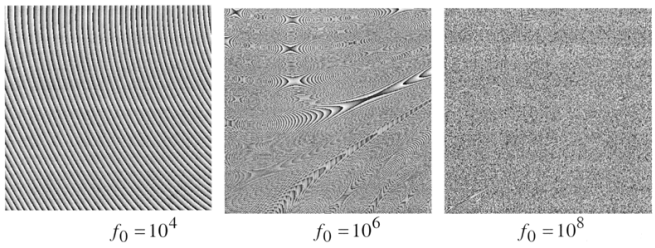
Статистические параметры	H	D
Тестовое изображение "Lena"	7,45	0,45
Муаровая маска	8,0	$2{,}0 \cdot 10^{-3}$
Муарограмма	8,0	$1{,}91 \cdot 10^{-3}$

Из табл. 2 видно, что муарограмма приобретает статистические характеристики ключевой муаровой маски, свойства которой несущественно отличаются от случайного процесса, и практически не зависит от статистических характеристик шифруемого изображения. Это позволяет надежно маскировать как низкочастотные, так и высокочастотные объекты изображений.

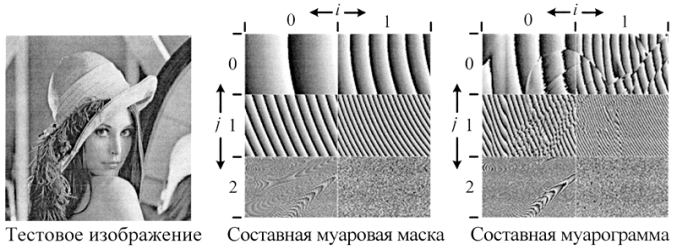
Технико-экономическое преимущество предложенного криптографического кодека для муарового маскирования изображений по сравнению с прототипом заключается в повышении уровня защищенности изображении от дешифрования за счет увеличения числа ключей, надежном маскировании высокочастотных деталей изображений за счет использования ключевых муаровых масок и муарограмм, имеющих статистические характеристики случайных процессов, и восстановлении зашифрованных изображений без потерь за счет исключения низкочастотного фильтра из декодера и использования генератора ключевых муаровых масок, формируемых с помощью обратимых целочисленных функций. Таким образом, предложенный кодек обеспечивает высокий уровень защищенности изображений от дешифрования, высокую надежность муарового маскирования высокочастотных деталей изображений, восстановление изображений без потерь в результате расшифрования и отсутствие эффекта размножения ошибок при передачи по каналу с помехами.



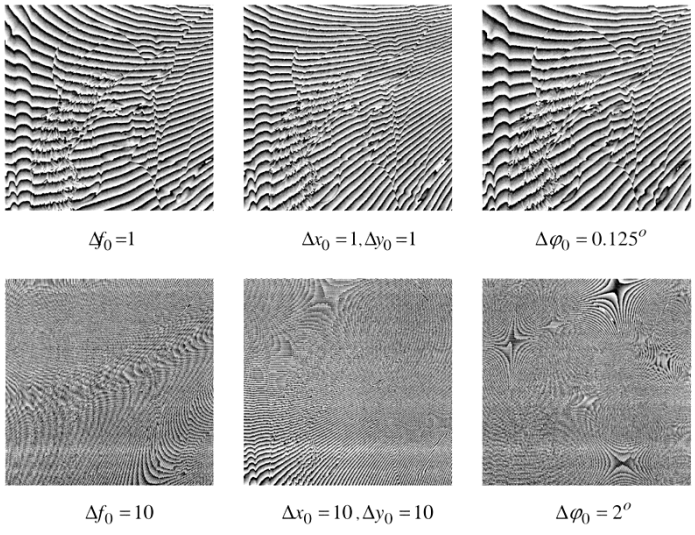
Фиг. 2



Фиг. 3



Фиг. 4



Фиг. 5

Национальный центр интеллектуальной собственности.
220034, г. Минск, ул. Козлова, 20.