ЧЕБЫШЕВСКИЙ СБОРНИК
Том 24. Выпуск 1.

УДК 517.925 DOI 10.22405/2226-8383-2023-24-1-89-103

Применение мегастабильной системы с 2-D полосой скрытых хаотических аттракторов для обеспечения безопасной связи

О. И. Кузнецова

Кузнецова Оксана Игоревна — аспирант, Тульский государственный университет (г. Тула).
e-mail: oxxy4893@mail.ru

Аннотация

Многие реальные динамические системы характеризуются наличием множества сосуществующих аттракторов. Это свойство систем называется мультистабильностью. В мультистабильных системах может произойти внезапный переход к нежелательным или неизвестным аттракторам. Такой переход может привести к катастрофическим событиям. Оказалось, что мультистабильность также связана с возникновением непредсказуемых аттракторов, которые называются скрытыми аттракторами. Одной из определяющих причин изучения мультистабильных хаотических систем с различными характеристиками является широкий спектр их потенциальных инженерных приложений – синхронизация приемника и передатчика, маскировка и восстановление сообщений, фильтрация шумов, восстановление информационных сигналов, а также разработка алгоритмов кодирования декодирования, позволяющих представить произвольное цифровое сообщение через символическую динамику хаотической системы.

В статье предложена не только математическая модель схемы безопасной коммуникации, основанная на адаптивной синхронизации между парой идентичных мегастабильных систем с 2-D полосой скрытых хаотических аттракторов, но и ее численное моделирование с использованием среды MATLAB & Simulink. Использование синхронизации в системах связи имеет фундаментальное значение, поскольку она заставляет системы одновременно производить одинаковые выходные данные и, в свою очередь, приводит к точному восстановлению информационных сигналов. Между тем, на стороне получателя информация может быть успешно восстановлена с помощью адаптивной техники. Представленный метод является устойчивым по отношению к различным уровням аддитивного белого гауссова шума. Схема, используемая для синхронизации, позволила преодолеть известные трудности, представленные в работах ряда специалистов, возникающие в задаче синхронизации в случае мультиустойчивости и сосуществования скрытых колебаний, при неправильном выборе формы управляющего сигнала.

Численное моделирование проводится для проверки осуществимости предложенной синхронизации и повышения производительности метода шифрования с точки зрения гистограммы, устойчивости к шуму и визуальной незаметности. В качестве тестовых примеров рассматриваются три типа замаскированных сообщений (текст, изображение в градациях серого и аудиосигнал).

Ключевые слова: динамические системы, хаос, скрытые аттракторы, счетное число сосуществующих аттракторов, безопасная связь.

Библиография: 30 названий.

Для цитирования:
О. И. Кузнецова. Применение мегастабильной системы с 2-D полосой скрытых хаотических аттракторов для обеспечения безопасной связи // Чебышевский сборник, 2023, т. 24, вып. 1, с. 89–103.

CHEBYSHEVSKII SBORNIK
Vol. 24. No. 1.

UDC 517.925 DOI 10.22405/2226-8383-2023-24-1-89-103

Application of megastable system with 2-D strip of hidden chaotic attractors to secure communications

O. I. Kuznetsova

Kuznetsova Oksana Igorevna — postgraduate student, Tula State University (Tula).
e-mail: oxxy4893@mail.ru

Abstract

Many real dynamical systems are characterized by the presence of a coexisting attractors set. This property of systems is called multistability. In multistable systems, a sudden transition to unwanted or unknown attractors can occur. Such a transition can lead to catastrophic events. It turned out that multistability is also associated with the emergence of unpredictable attractors, which are called hidden attractors. One of the defining reasons for studying multistable chaotic systems with different characteristics is a wide range of their potential engineering applications - synchronization of the receiver and transmitter, masking and recovery of messages, noise filtering, recovery of information signals, as well as the development of decoding and coding algorithms that allow you to present an arbitrary digital message through the symbolic dynamics of a chaotic system.

This paper proposes not only a mathematical model of a secure communication scheme based on adaptive synchronization between a pair of identical megastable systems with a 2-D band of hidden chaotic attractors, but also its numerical simulation using the MATLAB & Simulink environment. The use of synchronization in communication systems is of fundamental importance, since it forces systems to simultaneously output the same output data and, in turn, leads to accurate restoration of information signals. Meanwhile, on the receiver side, information can be successfully recovered using adaptive technology. The presented method is stable with respect to various levels of additive white Gaussian noise. The scheme used for synchronization made it possible to overcome the well-known difficulties presented in the works of a number of specialists that arise in the problem of synchronizing in the case of multistability and coexistence of hidden oscillations, with the wrong choice of the form of the control signal.

Numerical simulations are given to verify the feasibility of proposed synchronization and better performance of image encryption technique in terms of histogram, robustness to noise and visual imperceptibility. Three types of masked messages (text, grayscale image and audio signal) are considered as test examples.

Keywords: dynamical systems, chaos, hidden attractors, countable number of coexisting attractors, secure communications.

Bibliography: 30 titles.

For citation:
O. I. Kuznetsova, 2023, “Application of megastable system with 2-D strip of hidden chaotic attractors to secure communications” , *Chebyshevskii sbornik*, vol. 24, no. 1, pp. 89–103.

1. Введение

Мультистабильность - широко распространенное явление в реальном физическом мире. Ее можно наблюдать, например, в динамических моделях газового лазера [1], биологических

систем [2], волоконных лазеров [3], нейронных сетей [4], полупроводниковых суперрешеток [5]. Мультистабильность динамической системы, содержащей хаотические аттракторы, может создать угрозу в практических инженерных приложениях, ввиду нетривиальной локализуемости в фазовом пространстве и непредсказуемости динамики системы. Это связано с тем, что в зависимости от выбора начальных условий такая система может демонстрировать решения с принципиально различным поведением. После того как были найдены теоретические решения проблем борьбы с хаосом и Пекора и Кэрролл предложили эффективный метод синхронизации двух одинаковых хаотических систем [6], были разработаны различные типы и стратегии синхронизации хаотических систем, включая полную синхронизацию [7—9], синхронизацию с запаздыванием [10-12], кластерную синхронизацию [14], адаптивную синхронизацию [15—17]. Использование синхронизации в системах связи имеет фундаментальное значение, поскольку она заставляет системы одновременно производить одинаковые выходные данные и, в свою очередь, приводит к точному восстановлению информационных сигналов [18; 19]. С тех пор многие исследователи обратились к задачам использования хаоса в технических системах. В настоящее время хаотические сигналы и системы широко используются, в частности, в шифровании изображений [20-22] и безопасной связи [23]. В данном случае роль "секретного ключа" играет определенный выбор начальных условий.

С быстрым ростом Интернета и беспроводных сетей информационная безопасность становится все более важной. В частности, шифрование изображений вызывает все больший интерес из-за того, что большая часть данных изображений должна быть конфиденциальной между отправляющей стороной и принимающей стороной, например, некоторые военные изображения, архитектурные чертежи, медицинские изображения и так далее. Не менее важно, уметь шифровать текст, аудиосигнал или видеосигнал. За последние несколько десятилетий в литературе было предложено множество алгоритмов шифрования, основанных на различных принципах [24-26]. Среди них методы шифрования на основе хаоса пользуются популярностью для практического применения, поскольку эти методы обеспечивают хорошее сочетание скорости, высокой безопасности, высокой чувствительности, сложности. При этом использование мультистабильных моделей в схемах синхронизации может привести к более сложному поведению используемой системы, что, в свою очередь, может быть существенно для различных приложений, включая безопасную связь и разработку криптосистем, а также усложнению задач дешифрования для взломщиков.

2. Метод адаптивной синхронизации для общего класса хаотических вещественных моделей

В работе [17] предложена схема адаптивной синхронизации, которая в общем виде может быть записана следующим образом:

$$\dot{x} = F(x) + G(x)A + H(x)B, \tag{1}$$

где $x = (x_1, x_2, \ldots, x_n)^T \in \mathbb{R}^n, F(x) : \mathbb{R}^n \to \mathbb{R}^n$ – вектор нелинейной функции, $G(x) : \mathbb{R}^n \to$ $\to \mathbb{R}^{n\times m}$ – линейная матрица-функция, $H(x) : \mathbb{R}^n \to \mathbb{R}^{n\times m}$ – нелинейная матрица-функция, $A = (A_1, A_2, \ldots, A_m)^T, B = (B_1, B_2, \ldots, B_m) \in \mathbb{R}^m$ – постоянные векторы параметров модели, которые ассоциируются с линейными и нелинейными членами, соответственно.

Ряд хорошо известных хаотических систем, таких как схема Чуа, гиперхаотическая система Лю, обобщенная система Лоренца, имеют вид уравнения (1).

Пусть ведущая и ведомая системы имеют следующую форму:

$$\dot{x} = F(x) + G(x)A + H(x)B, \tag{2}$$

$$\dot{y} = F(y) + G(y)\hat{A} + H(y)\hat{B} + \theta(x, y). \tag{3}$$

Здесь $x, y \in \mathbb{R}^n$ – векторы состояния, $A, B \in \mathbb{R}^m$ – постоянные векторы параметров ведущей системы, $\hat{A}, \hat{B}$ – неопределенные постоянные векторы параметров ведомой системы, $\theta : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n$ – вектор функции управления ведомой системы (3). Ошибка модуляции параметров $\hat{A}, \hat{B}$ определяются следующим образом: $e_A = \hat{A} - A, e_B = \hat{B} - B$. Состояния ошибки могут быть выражены следующим образом:

$$e(t) = y(t) - x(t). \tag{4}$$

Определение 1. *Ведущая система (2) и ведомая система (3) реализуют адаптивную синхронизацию, если*

$$\lim_{t\to\infty} \|e(t)\| = \lim_{t\to\infty} \|y(t) - x(t)\| = 0.$$

Следуя идеям из [11; 12], выведем векторную функцию управления для достижения синхронизации между системами (2) и (3).

Теорема 1. [17] *Адаптивная синхронизация между ведущей системой (2) и ведомой системой (3) будет достигнута если функция вектора управления построена в следующей форме:*

$$\theta(x, y) = [F(x) - F(y)]A + G(x) - G(y) + [H(x) - H(y)]B - K_1 e - K_2 e_A - K_3 e_B \tag{5}$$

Здесь $K_1 = diag(k_{11}, k_{12}, \ldots, k_{1n}), K_2 = diag(k_{21}, k_{22}, \ldots, k_{2n}), K_3 = diag(k_{31}, k_{32}, \ldots, k_{3n})$ – положительно определенные вещественные диагональные матрицы, а обновление параметров модуляции выбирается в соответствии со следующими уравнениями:

$$\dot{e}_A = \dot{\hat{A}} = -(F(y))^T e + K_2 e, \tag{6}$$

$$\dot{e}_B = \dot{\hat{B}} = -(H(y))^T e + K_3 e. \tag{7}$$

3. Адаптивная синхронизация для мегастабильной системы с 2-D полосой скрытых хаотических аттракторов

В данном подразделе применим схему для достижения адаптивной синхронизации из [17] между двумя идентичными хаотическими системами из [27]. Ведущая и ведомая системы с индексами d и r соответственно могут быть выражены следующим образом:

$$\begin{cases} \dot{x}_d = \operatorname{tg} y_d \\ \dot{y}_d = -x_d - \operatorname{arctg}(|50 z_d| - 10) \operatorname{tg} y_d, \\ \dot{z}_d = (\operatorname{tg}^4 y_d - \frac{a}{1+x_d^8}) \operatorname{sign} z_d \end{cases} \tag{8}$$

$$\begin{cases} \dot{x}_r = \operatorname{tg} y_r + \theta_1 \\ \dot{y}_r = -x_r - \operatorname{arctg}(|50 z_r| - 10) \operatorname{tg} y_r + \theta_2, \\ \dot{z}_r = (\operatorname{tg}^4 y_d - \frac{a}{1+x_r^8}) \operatorname{sign} z_r + \theta_3 \end{cases} \tag{9}$$

где $\theta = (\theta_1, \theta_2, \theta_3)^T$ – вектор-функция управления.

Запишем ведущую систему (8) в виде (2):

$$\begin{gathered} x = (x_d, y_d, z_d)^T, A = (1, 0, 0)^T, B = (0, 0, a)^T, F(x) = \begin{pmatrix} \operatorname{tg} y_d, \\ -x_d - \operatorname{arctg}(|50 z_d| - 10) \operatorname{tg} y_d, \\ (\operatorname{tg}^4 y_d - \frac{a}{1+x_d^8}) \operatorname{sign} z_d \end{pmatrix}, \\ G(x) = \begin{pmatrix} 0 & 0 & 0 \\ -x_d & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, H(x) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -\frac{\operatorname{sign} z_d}{1+x_d^8} \end{pmatrix}. \end{gathered} \tag{10}$$

Аналогично можно записать ведомую систему (9) в виде (3):

$$x = (x_r, y_r, z_r)^T, A =(1,0,0)^T, B = (0,0,\hat{a})^T, \theta = (\theta_1, \theta_2, \theta_3)^T,$$

$$F(x) = \begin{pmatrix} \operatorname{tg} y_r, \\ -x_r - \operatorname{arctg}(|50z_r| - 10)\operatorname{tg} y_r, \\ (\operatorname{tg}^4 y_r - \frac{a}{1+x_r^8})\operatorname{sign} z_r \end{pmatrix}, G(x) = \begin{pmatrix} 0 & 0 & 0 \\ -x_r & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, H(x) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -\frac{\operatorname{sign} z_r}{1+x_r^8} \end{pmatrix}. \tag{11}$$

Векторы ошибок, соответствующие состояниям и модуляции параметров, выражаются следующим образом:

$$e = (e_1, e_2, e_3)^T, \tag{12}$$

$$e_A = (e_{A_1}, e_{A_2}, e_{A_3})^T, \tag{13}$$

$$e_B = (e_{B_1}, e_{B_2}, e_{B_3})^T. \tag{14}$$

По теореме 1, мы получаем следующие функции управления (5):

$$\theta = \begin{pmatrix} \operatorname{tg} y_d, -\operatorname{tg} y_r + \varphi_1 \\ -x_d - \operatorname{arctg}(|50z_d| - 10)\operatorname{tg} y_d + x_r + \operatorname{arctg}(|50z_r| - 10)\operatorname{tg} y_r + \varphi_2 \\ (\operatorname{tg}^4 y_d - \frac{a}{1+x_d^8})\operatorname{sign} z_d - (\operatorname{tg}^4 y_r - \frac{a}{1+x_r^8})\operatorname{sign} z_r + \varphi_3 \end{pmatrix}, \tag{15}$$

где $\varphi_1 = -k_{11}e_1 - k_{21}e_{A_1} - k_{31}e_{B_1}, \varphi_2 = -k_{12}e_2 - k_{22}e_{A_2} - k_{32}e_{B_2}, \varphi_1 = -k_{13}e_3 - k_{23}e_{A_3} - k_{33}e_{B_3}$.

Как показано в [27], при $a = 2$ система (8) не имеет состояний равновесия и обладает 2-D полосой скрытых хаотических аттракторов, представленной на рисунке 1. Ведущая система (8) и ведомая система (9) с управлением (15) решаются численно.

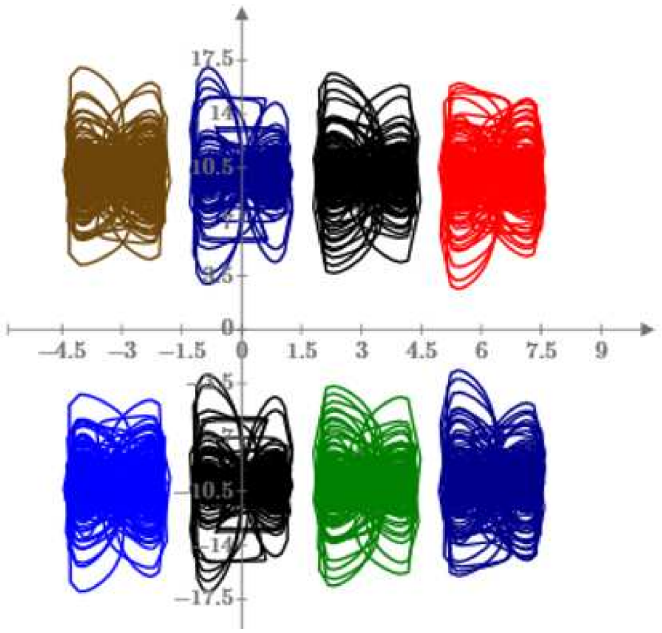

Рис. 1: Скрытый аттрактор системы (2)-(3).

4. Приложение для систем защищенной коммуникации

В данном разделе описана безопасная стратегия связи, основанная на адаптивной синхронизации хаотических систем (8) и (9). Схема построена таким образом, чтобы разделить

сообщение и распределить его между двумя каналами, что повышает безопасность системы связи и усложняет задачу дешифровки злоумышленниками. Некоторый бит информационного сигнала вводится в параметры модуляции и передается по одному из двух каналов; тем временем другой бит вводится в состояния передатчика и передается по второму каналу. На стороне приемника сообщение может быть точно извлечено с помощью адаптивных методов и функции дешифрования. Предложенная схема надежна к различным масштабам аддитивного белого гауссовского шума (АБГШ), что будет продемонстрировано ниже. На рисунке. 2 изображена предложенная схема. Схема включает следующие компоненты:

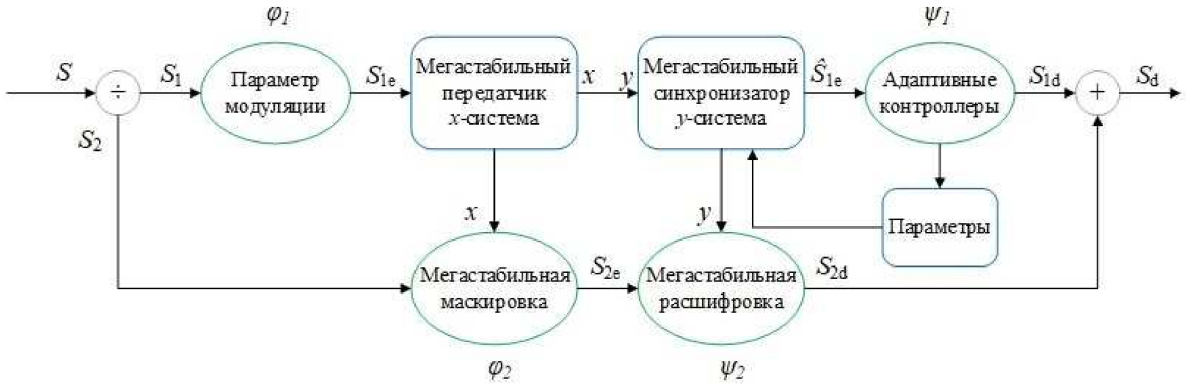

Рис. 2: Скрытый аттрактор системы (2)-(3).

– Системы передатчика и приемника: мегастабильная система с 2-D полосой скрытых хаотических аттракторов из [27], которая генерирует переменные состояния $x(t) \in \mathbb{R}^n$ для передатчика и $y(t) \in \mathbb{R}^n$ для приемника.

– Блок разделения: информационное сообщение $S(t)$ делится на два вектора битов S_1 и S_2, чтобы распределить его по двум каналам.

– Блок модуляции параметров: первая часть сообщения $S_1(t)$ модулируется непрерывной инвертируемой функцией φ_1 в параметры передатчика.

– Мегастабильный хаотический маскирующий блок: вторая часть сообщения $S_2(t)$ шифруется путем введения в нелинейную функцию $\varphi_2 : \mathbb{R}^n \times \mathbb{R} \to \mathbb{R}$, которая для $x \in \mathbb{R}^n$ непрерывна и имеет ассоциированную нелинейную функцию $\psi_2 : \mathbb{R}^n \times \mathbb{R} \to \mathbb{R}$, которая непрерывна для $x \in \mathbb{R}^n$, такую, что $\psi_2(x, \varphi_2(x, S_2)) = S_2$. Шифрующая функция φ_2 строится на основе хаотических состояний. В результате генерируется сигнал $S_{2e}(t)$, который несет часть сообщения.

– Каналы: хаотические состояния, которые содержат параметры модуляции и шифрованную информационную часть S_{2e}, передаются по двум каналам.

– Блок синхронизации: на стороне приемника реализован блок синхронизации для получения сигналов состояния хаоса и предоставления необходимой информации для расшифровки.

– Блок адаптивных контроллеров: на стороне приемника строятся адаптивные контроллеры для отслеживания параметров системы передатчика. После синхронизации функция расшифровки ψ_1 может быть использована для восстановления первой части переданного сообщения S_{1d}.

– Блок мегастабильного хаотического дешифрования: маскированная информация $S_{2e}(t)$ декодируется функцией $S_{2d}(t) = \psi_2(y(t), S_{1e}(t))$.

– Блок сбора: объединив два информационных сигнала S_{1d} и S_{2d}, получаем полное расшифрованное сообщение S_d.

5. Однопараметрическая модуляция и хаотическая маскировка для шифрования звукового сигнала

Первый тип сообщения $S(t)$ - это аудиосигнал, который находится в интервале $[0, 33]$. Для преобразования этого звукового сообщения в вектор цифр используется инструмент MATLAB "double". Пусть $S = [s_1, s_2, \ldots, s_m, s_{m+1}, s_{m+2}, \ldots, s_n]$, согласно предложенной схеме, этот вектор цифр разбивается на два вектора $S_1 = [s_1, s_2, \ldots, s_m]$ и $S_2 = s_{m+1}, s_{m+2}, \ldots, s_n]$. Первый вектор S_1 вводится в параметры передатчика со следующим параметром функции модуляции:

$$S_{1e} = \varphi_1([A, B], S_1) = \frac{S_1}{10d} + a, \tag{16}$$

где $d = max(S(j)) - min(S(j)), j = 1, 2, \ldots, n, a = 2$.
Для второй части сообщения, S_2 вставляется в хаотические состояния передатчика с помощью следующей функции:

$$S_{2e} = \varphi_2(x, S_2) = x^2 + (1 + x^2)S_2. \tag{17}$$

Приемник может расшифровать сообщение с помощью следующих функций:

$$S_{1d} = \psi_1([\hat{A}, \hat{B}], \hat{S}_{1e}) = 10(\hat{S}_{1e} - \hat{a})d, \tag{18}$$

где $\hat{a} = 0$

$$S_{2d} = \psi_2(y, \hat{S}_{2e}) = \frac{S_{2e} - y^2}{1 + y^2}. \tag{19}$$

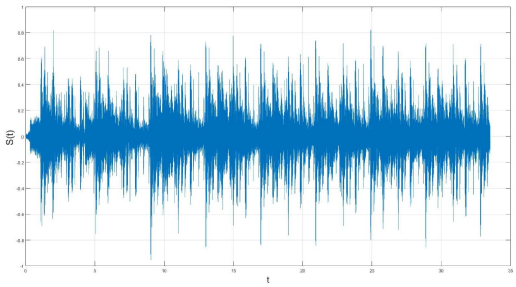

Рис. 3: Исходный сигнал $S(t)$.

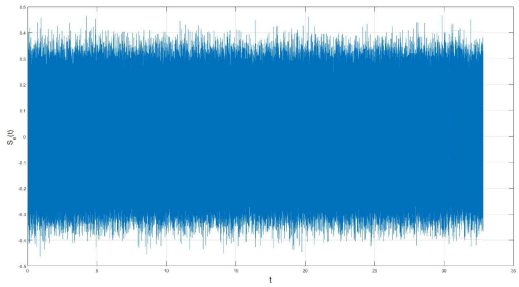

Рис. 4: Зашифрованный сигнал $S_e(t)$.

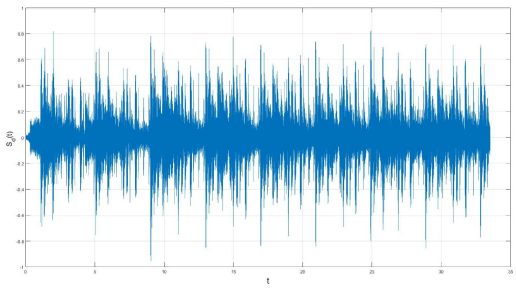

Рис. 5: Расшифрованный сигнал $S_d(t)$.

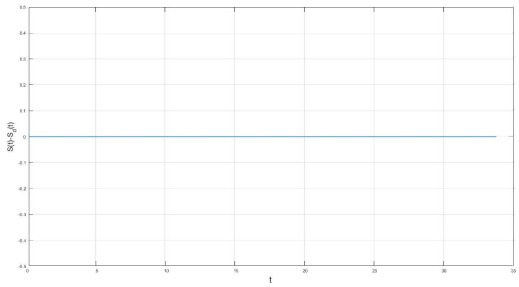

Рис. 6: Ошибка дешифрования $S(t) - S_d(t))$.

Собрав S_{1d} и S_{2d}, получим весь расшифрованный информационный сигнал S_d. Используя инструмент MATLAB "char", приемник может преобразовать этот вектор цифр обратно в текст. Предположим, что мы хотим передать сообщение, являющееся звуковым сигналом, как показано на рисунке 3. Шифрованное сообщение показано на рисунке 4, и видно, что оно надежно зашифровано. Расшифрованное сообщение показано на рисунке 5. Ошибка $S(t) - S_d(t)$ между переданным звуковым сигналом и восстановленным сигналом показана на рисунке 6. Из рисунке 6 можно наблюдать, что исходный волновой сигнал точно восстановлен.

6. Однопараметрическая модуляция и хаотическая маскировка для шифрования обычного текста

Теперь рассмотрим второе сообщение $S(t)$, представленное в виде обычного текста, который может содержать буквы алфавита, символы, цифры и пробелы. Предположим, что мы хотим передать небольшую часть текста, как показано на рисунке 7. Шифрованное сообщение показано на рисуноке 8, и видно, что оно надежно зашифровано. Расшифрованное сообщение показано на рисуноке 9, и оно идентично оригинальному содержимому. Логика шифрования текста, аналогична рассмотренному выше примеру, функции шифрования и дешифрования выбираются аналогично как и для случая хаотической маскировки звукового сигнала.

Для того, чтобы прочитать зашифрованную информацию, принимающей стороне необходимы ключ и дешифратор (устройство, реализующее алгоритм расшифровывания). Идея шифрования состоит в том, что злоумышленник, перехватив зашифрованные данные и не имея к ним ключа, не может ни прочитать, ни изменить передаваемую информацию. Кроме того, в современных криптосистемах (с открытым ключом) для шифрования, расшифрования данных могут использоваться разные ключи. Однако, с развитием криптоанализа, появились методики, позволяющие дешифровать закрытый текст без ключа. Они основаны на математическом анализе переданных данных.

Рис. 7: Оригинальный текст.

sFOE7tiTOu6e74iOMt3EyfSNZbV07ky2h2yCZDqv/7Pq3k+F8vIplGE2GyF6SkBiGBGXu7lE/h
xhIDRA9lZLaARivzta/8ycBOM1M3UBZ7L8PpT54ck4TmnISLVFMPp5AvNdtwntiaaLT3WmJ
eqZntqziZJyWYSVH3Ec1L6Yr5u/HffHmKyz0vRmO+xoDOKd2AxSLT3E7M1BsesSpFl3xCc98
zP9kSql6tU8+eM4edyN0/g+53VSdjYlfG1OSpfZAYmv6Nr7+0ozeovvfWAfJbfuHM5+XPX+E
tdlbAJ8XIgsFyX23OHEvqbciHt3KyjbKmyddlyGMaa6AO5IVS/9buKNZfgayY8GZTBOj4EAJeR
nvjN8Ozxmq8uQ7EAwVV+QHjW8juIqfVkpF7yqTvtUFK2+kCJC/8opDjKRVEVJsS/0cLiRy4yN
XwgCUO3mAvIIKcJK4tAjM7xfSxKrZGIeAuJFIsZOZgiu9GUtIU3oCporR+keHw/tH4RNVBh0e
ygE2AOMDq2cbjcgSxVsMObXYl29lo3zVcTlSsf48WhetWRTAtJnwOoosSqaWtnfFJJm4FDrg
qPSVaNx7+uhIDw7Fl7tpplCX9YjGpDY=

Рис. 8: Зашифрованный текст.

Для того, чтобы прочитать зашифрованную информацию, принимающей стороне необходимы ключ и дешифратор (устройство, реализующее алгоритм расшифровывания). Идея шифрования состоит в том, что злоумышленник, перехватив зашифрованные данные и не имея к ним ключа, не может ни прочитать, ни изменить передаваемую информацию. Кроме того, в современных криптосистемах (с открытым ключом) для шифрования, расшифрования данных могут использоваться разные ключи. Однако, с развитием криптоанализа, появились методики, позволяющие дешифровать закрытый текст без ключа. Они основаны на математическом анализе переданных данных.

Рис. 9: Расшифрованный текст.

7. Однопараметрическая модуляция и хаотическая маскировка для изображения в градациях серого

Следущее сообщение $S(t)$ является изображением в градации серого (City.tif) размером 256×256. Это изображение может быть преобразовано в матрицу пикселей размером $m \times n$ следующим образом:

$$S = \begin{pmatrix} s_{11} & s_{12} & \dots & s_{1n} \\ s_{21} & s_{22} & \dots & s_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ s_{m1} & s_{m2} & \dots & s_{mn} \end{pmatrix}, \tag{20}$$

где s_{kl} обозначает значение изображения в пикселе в позиции (k, l), где $k = 1, 2, \dots, m, l = 1, 2, \dots, n$. Матрица пикселей преобразуется в одномерный вектор целых чисел от 0 до 255. Пусть $S = [s_{11}, s_{21}, \dots, s_{m1}, s_{12}, s_{22}, \dots, s_{m2}, s_{1n}, s_{2n}, \dots, s_{mn}] = [s_1, s_2, \dots, s_{mn}]$. Последний вектор делится на два вектора $S_1 = [s_1, s_2, \dots, s_k]$ и $S_2 = [s_{k+1}, s_{k+2}, \dots, s_{mn}]$. Первый вектор вводится в параметры передающей системы, а второй - в ее хаотические состояния. Для модуляции параметров, хаотической маскировки и расшифровки используются те же функции, что и в рассмотренных выше примерах с шифрованием звукового сигнала и текста. Переданные и восстановленные серые изображения показаны на рисунках 10 и 12. Гистограммы, показывающие распределения интенсивностей для оригинального и расшифрованного изображений, приведены на рисунках 13 и 15, соответственно. На рисунках 11 и 14 показаны зашифрованное изображение и его гистограмма. Сравнивая рисунки 12 и 15 с рисунками 10 и 13 соответственно, видно, что расшифрованнное изображение идентично оригинальному.

Рис. 10: Оригинальное изображение.

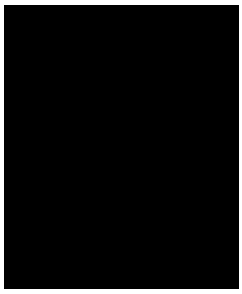

Рис. 11: Зашифрованное изображение.

Рис. 12: Расшифрованное изображение.

Чтобы продемонстрировать надежность стратегии безопасной связи для шифрования изображений добавляется аддитивный белый гауссовский шум (АБГШ) с различными масштабами

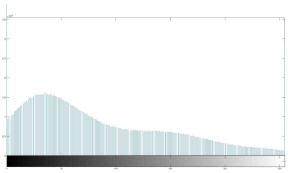

Рис. 13: Гистограмма оригинального изображения.

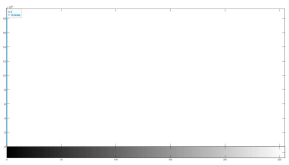

Рис. 14: Гистограмма зашифрованного изображения.

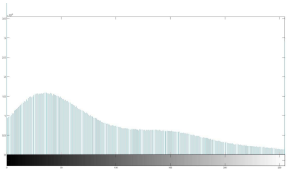

Рис. 15: Гистограмма расшифрованного изображения.

[28]. Оригинальные изображения с шумом представлены на рисунках 16-18, зашифрованные изображения аналогичны рисунку 11, расшифрованные изображения представлены на рисунках 19-21. Для измерения качества восстановленного изображения используются следущие тесты: пиковое отношение сигнал/шум (PSNR) и индекс структурного сходства изображения (SSIM) [30]. Как видно из таблицы 1, изображения точно рассшифрованы.

Рис. 16: Оригинальное изображение с шумом 0.05.

Рис. 17: Оригинальное изображение с шумом 0.2.

Рис. 18: Оригинальное изображение с шумом 0.5.

Рис. 19: Расшифрованное изображение с шумом 0.05.

Рис. 20: Расшифрованное изображение с шумом 0.2.

Рис. 21: Расшифрованное изображение с шумом 0.5.

8. Анализ отношения пикового уровня сигнала к шуму

Для анализа распределения пикселей восстановленного сообщения по отношению к оригинальному применяется пиковое отношение сигнал/шум (PSNR). PSNR можно определить следующим образом [13; 29]:

$$PSNR(S, S_d) = 10 \lg \frac{255^2}{MSE(S, S_d)}, \tag{21}$$

где MSE - среднеквадратичная ошибка, которая определяется следующим образом:

$$MSE(S, S_d) = \frac{1}{m \times n} \sum_{k=1}^{m} \sum_{l=1}^{n} (s_d(k,l) - s(k,l))^2. \tag{22}$$

Здесь S и S_d означают оригинальное и восстановленное изображение, соответственно. Отметим, что высокое значение PSNR означает близкое сходство между расшифрованным сообщением и оригиналом.

9. Индекс структурного сходства изображения

Второй тест, используемый для измерения и анализа сходства между оригиналом и найденным изображением - это индекс структурного сходства изображения (SSIM), определяемый в следующей форме [30]:

$$SSIM(S, S_d) = \frac{(2\mu_S\mu_{S_d} + C_1)(2\sigma_{SS_d} + C_2)}{(\mu_S^2 + \mu_{S_d}^2 + C_1)(\sigma_S^2 + \sigma_{S_d}^2 + C_2)} \tag{23}$$

где μ_S и μ_{S_d} - среднее значение яркости оригинального изображения S и расшифрованного изображения S_d, соответственно, σ_S и σ_{S_d} - стандартные вариации S и S_d, соответственно, σ_{SS_d} - ковариация между S и S_d, C_1 и C_2 - небольшие фиксированные положительные константы, чтобы знаменатель не был равен нулю. Оценка SSIM всегда находится в диапазоне $[-1, 1]$, и самая сильная оценка 1 реализуется, если $S = S_d$.

Серое изображение	PSNR	SSIM
City АБГШ 0.05	99.999999999985574	0.999999999993749
City АБГШ 0.2	98.343454354614656	0.999999999845454
City АБГШ 0.5	96.712344545296567	0.999999995675675

Таблица 1: Оценка PSNR и SSIM для изображения в градации серого

10. Заключение

Хаотические системы играют важную роль в системах защищенной связи из-за их сложного поведения и чувствительности к начальным условиям. В литературе предложено множество схем хаотических (гиперхаотических) защищенных систем связи. В этой работе применена схема защищенной коммуникации, основанная на адаптивной синхронизации между парой идентичных мегастабильных систем с 2-D полосой скрытых хаотических аттракторов. Схема предназначена для разделения сообщения и распределения его между двумя независимыми каналами связи, что приводит к повышению уровня защищенности предложенной схемы и усложняет задачу дешифровки злоумышленником. Информационный битовый поток поступает в шифратор, где разделяется на два шифрованных потока, первый вводится в параметры модуляции и передается по одному из двух каналов связи, а второй вводится в состояния передатчика и передается по второму каналу. На стороне приемника сообщение может быть точно извлечено с помощью адаптивных методов и функции дешифрования. В случае, если передаваемое по каналу связи сообщение $S(t)$, является видеосигналом для его маскировки используется симбиоз техник, описанных в разделах 5 и 7 [28]. Исходный видеосигнал разделяется на аудиосигнал и последовательность картинок. Далее каждому кадру сопоставляется звуковая дорожка, длительность которой варьируется сменой кадров в видео ряде. После чего отдельно шифруется последовательность кадров-изображений и соответствующих им звуковых сигналов. После дешифрования происходит “склейка”, последовательности изображений и наложение соответствующих им звуковых сигналов. В результате получается видео файл, аналогичный оригинальному. Предложенная схема надежна к различным масштабам аддитивного белого гауссовского шума.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Arecchi F. T , Meucci R., Puccioni G., Tredicce J. Experimental evidence of subharmonic bifurcations-multistability and turbulence in a Q-switched gas laser // Phys. Rev. Lett. 1982. Vol. 49(17):1217.

2. Laurent M., Kellershohn N. Multistability: a major means of differentiation and evolution in biological systems // Trends Biochem Sci. 1999. Vol. 24(11). P. 418–422.

3. Komarov A., Leblond H., Sanchez F. Multistability and hysteresis phenomena in passively mode-locked fiber lasers // Phys. Rev. A. 2005. Vol. 71(5):053809.

4. Zeng Z., Huang T., Zheng W. Multistability of recurrent neural networks with time-varying delays and the piecewise linear activation function // IEEE Trans Neural Netw. 2010. Vol. 21(8). P. 1371–1377.

5. Ying L., Huang D., Lai Y. C. Multistability, chaos, and random signal generation in semiconductor superlattices // Phys. Rev. E. 2016. Vol. 93(6):062204.

6. Pecora L. M., Carroll T. L. Synchronization in chaotic systems // Physical review letters. 1990. Vol. 64, № 8. P. 821-824.

7. Shoreh A. A.-H., Kuznetsov N. V., Mokaev T. N., Tavazoei M. S. Synchronization of hidden hyperchaotic attractors in fractional Order complex-valued systems with application to secure communications // 2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus). IEEE. 2021. P. 62—67

8. Tavazoei M. S., Haeri M. Synchronization of chaotic fractional-order systems via active sliding mode controller // Physica A: Statistical Mechanics and its Applications. 2008. Vol. 387, № 1. P. 57—70.

9. Zhang H., Ma X.-K. Synchronization of uncertain chaotic systems with parameters perturbation via active control // Chaos, Solitons & Fractals. 2004. Vol. 21, № 1. P. 39—47.

10. Shoreh A. A.-H., Kuznetsov N. V., Mokaev T. N. Lag synchronization for complex-valued Rabinovich system with application to encryption techniques // 2020 16th International Computer Engineering Conference (ICENCO). IEEE. 2020. P. 11—16.

11. Du H., Zeng Q., Lu N. A general method for modified function projective lag synchronization in chaotic systems // Physics Letters A. 2010. Vol. 374, № 13/14. P. 1493—1496.

12. Mahmoud G. M., Mahmoud E. E. Lag synchronization of hyperchaotic complex nonlinear systems // Nonlinear Dynamics. 2012. Vol. 67, № 2. P. 1613—1622.

13. Tang Z., Park J. H., Feng J. Novel approaches to pin cluster synchronization on complex dynamical networks in Lur'e forms // Communications in Nonlinear Science and Numerical Simulation. 2018. Vol. 57. P. 422—438.

14. Mahmoud G. M. Farghaly A. A., Abed-Elhameed T. M., Darwish M. M. Adaptive dual synchronization of chaotic (hyperchaotic) complex systems with uncertain parameters and its application in image encryption // Acta Phys. Pol. B. 2018. Vol. 49, № 11. P. 1923-1939.

15. He H., Tu J., Xiong P. Lr-synchronization and adaptive synchronization of a class of chaotic Lurie systems under perturbations // Journal of the Franklin Institute. 2011. Vol. 348, № 9. P. 2257—2269.

16. Xu Y., Zhou W., Sun W. Adaptive synchronization of uncertain chaotic systems with adaptive scaling function // Journal of the Franklin Institute. 2011. Vol. 348, № 9. P. 2406—2416.

17. Shoreh A.-H., Kuznetsov N., Mokaev T. New adaptive synchronization algorithm for a general class of complex hyperchaotic systems with unknown parameters and its application to secure communication // Physica A: Statistical Mechanics and its Applications. 2021. DOI:10.1016/j.physa.2021.126466.

18. Kolumban G., Kennedy M. P., Chua L. O. The role of synchronization in digital communications using chaos. I. Fundamentals of digital communications // IEEE Transactions on circuits and systems I: Fundamental theory and applications. 1997. Vol. 44, № 10. P. 927—936.

19. Kolumban G., Kennedy M. P., Chua L. O. The role of synchronization in digital communications using chaos. II. Chaotic modulation and chaotic synchronization // IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications. 1998. Vol. 45, № 11. P. 1129—1140.

20. Guan Z. H., Huang F., Guan W. Chaos-based image encryption algorithm // Phys. Lett. A. 2005. Vol. 346, №1-3. P. 153-157.

21. Gao T., Chen Z. A new image encryption algorithm based on hyper-chaos // Phys. Lett. A. 2008. Vol. 372, №4. P. 394-400.

22. Xie E. Y., Li C., Yu S, Lü J. On the cryptanalysis of Fridrich's chaotic image encryption scheme // Signal processing. 2017. Vol.132. P. 150-154.

23. Wang S., Kuang J., Li J., Luo Y., Lu H., Hu G. Chaos-based secure communications in a large community // Phys. Rev. E. 2012. Vol. 66, Art. no. 065202R.

24. Chen G. R., Mao Y. B., Chui C. K. A symmetric image encryption scheme based on 3D chaotic cat maps // Chaos Solitons & Fractals. 2004. Vol. 21, №3. P. 749–761.

25. Pareek N. K., Patidar V., Sud, K. K. Image Encryption Using Chaotic Logistic Map // Image and Vision Computing. 2006. Vol. 24. P. 926-934.

26. Yen J.-I., Guo J.-C. Efficient hierarchical chaotic image encryption algorithm and its VLSI realisation // IEE Proc - Vision, Image, Sign Proc. 2000. Vol. 147, № 2. P. 167-175.

27. Буркин И. М., Кузнецова О. И. Новая мегастабильная система с 2-D полосой скрытых аттракторов и аналитическими решениями // Чебышевский сборник. 2021. Т. 22, Вып. 4. С. 360–368.

28. Кузнецова О. И. Программа для шифрования информации с использованием мегастабильной системы с 2-D полосой скрытых аттракторов // Свидетельство о государственной регистрации программы для ЭВМ №2022666310. 30.08.22. 1 с.

29. Wang Z., Bovik A. C., Sheikh H. R., Simoncelli E. P. . Image quality assessment: from error visibility to structural similarity // IEEE transactions on image processing. 2004. Vol. 13, № 4. P. 600—612.

30. Wang Z., Bovik A. C. A universal image quality index // IEEE signal processing letters. 2002. Vol. 9, № 3. P. 81—84.

REFERENCES

1. Arecchi, F. T., Meucci, R., Puccioni, G. & Tredicce, J. 1982, "Experimental evidence of subharmonic bifurcations-multistability and turbulence in a Q-switched gas laser", *Phys. Rev. Lett.*, vol. 49(17):1217.

2. Laurent, M. & Kellershohn, N. 1999, "Multistability: a major means of differentiation and evolution in biological systems", *Trends Biochem Sci.*, vol. 24(11), pp. 418–422.

3. Komarov, A., Leblond, H. & Sanchez, F. 2005, "Multistability and hysteresis phenomena in passively mode-locked fiber lasers", *Phys. Rev. A.*, vol. 71(5):053809.

4. Zeng, Z., Huang, T. & Zheng, W. 2010, "Multistability of recurrent neural networks with time-varying delays and the piecewise linear activation function", *IEEE Trans. Neural Netw.*, vol. 21(8), pp. 1371–1377

5. Ying, L., Huang, D. & Lai, Y. C. 2016, "Multistability, chaos, and random signal generation in semiconductor superlattices", *Phys. Rev. E.*, vol. 93(6):062204.

6. Pecora, L. M. & Carroll, T. L. 1990, "Synchronization in chaotic systems", *Physical review letters*, vol. 64, no. 8, pp. 821-824.

7. Shoreh, A. A.-H., Kuznetsov, N. V., Mokaev, T. N. & Tavazoei, M. S. 2021, "Synchronization of hidden hyperchaotic attractors in fractional Order complex-valued systems with application to secure communications", *2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus). IEEE*, pp. 62—67

8. Tavazoei, M. S. & Haeri, M. 2008, "Synchronization of chaotic fractional-order systems via active sliding mode controller", *Physica A: Statistical Mechanics and its Applications*, vol. 387, no. 1, pp. 57—70.

9. Zhang, H. & Ma, X.-K. 2004, "Synchronization of uncertain chaotic systems with parameters perturbation via active control", *Chaos, Solitons & Fractals*, vol. 21, no. 1, pp. 39—47.

10. Shoreh, A. A.-H., Kuznetsov, N. V. & Mokaev, T. N. 2020, "Lag synchronization for complex-valued Rabinovich system with application to encryption techniques", *2020 16th International Computer Engineering Conference (ICENCO). IEEE.*, pp. 11—16.

11. Du, H., Zeng Q.& Lu, N. 2010, "A general method for modified function projective lag synchronization in chaotic systems", *Physics Letters A.*, vol. 374, no. 13/14, pp. 1493—1496.

12. Mahmoud, G. M. & Mahmoud, E. E. 2012, "Lag synchronization of hyperchaotic complex nonlinear systems", *Nonlinear Dynamics*, vol. 67, no. 2, pp. 1613—1622.

13. Tang, Z., Park, J. H. & Feng, J. 2018.,"Novel approaches to pin cluster synchronization on complex dynamical networks in Lur'e forms", *Communications in Nonlinear Science and Numerical Simulation*, vol. 57, pp. 422—438.

14. Mahmoud, G. M. Farghaly, A. A., Abed-Elhameed, T. M. & Darwish, M. M. 2018, "Adaptive dual synchronization of chaotic (hyperchaotic) complex systems with uncertain parameters and its application in image encryption", *Acta Phys. Pol. B.*, vol. 49, no. 11, pp. 1923-1939.

15. He, H., Tu, J. & Xiong, P. 2011, "Lr-synchronization and adaptive synchronization of a class of chaotic Lurie systems under perturbations", *Journal of the Franklin Institute*, vol. 348, no. 9, pp. 2257—2269.

16. Xu, Y., Zhou, W. & Sun, W. 2011, "Adaptive synchronization of uncertain chaotic systems with adaptive scaling function", *Journal of the Franklin Institute*, vol. 348, no. 9, pp. 2406—2416.

17. Shoreh, A.-H., Kuznetsov, N. & Mokaev, T. 2021, "New adaptive synchronization algorithm for a general class of complex hyperchaotic systems with unknown parameters and its application to secure communication", *Physica A: Statistical Mechanics and its Applications*, DOI:10.1016/j.physa.2021.126466.

18. Kolumban, G., Kennedy, M. P. & Chua, L. O. 1997, "The role of synchronization in digital communications using chaos. I. Fundamentals of digital communications", *IEEE Transactions on circuits and systems I: Fundamental theory and applications*, vol. 44, no. 10, pp. 927—936.

19. Kolumban, G., Kennedy, M. P. & Chua, L. O. 1998, "The role of synchronization in digital communications using chaos. II. Chaotic modulation and chaotic synchronization", *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 45, no. 11, pp. 1129—1140.

20. Guan, Z. H., Huang, F. & Guan, W. 2005, "Chaos-based image encryption algorithm", *Phys. Lett. A.*, vol. 346, no. 1-3, pp.153-157.

21. Gao, T. & Chen, Z. 2008, "A new image encryption algorithm based on hyper-chaos", *Phys. Lett. A.*, vol. 372, no. 4, pp. 394-400.

22. Xie, E. Y., Li, C., Yu, S. & Lü, J. 2017, "On the cryptanalysis of Fridrich's chaotic image encryption scheme", *Signal processing*, vol.132, pp.150-154.

23. Wang, S., Kuang, J., Li, J., Luo, Y., Lu, H. & Hu, G. 2012, "Chaos-based secure communications in a large community", *Phys. Rev. E.*, vol. 66, Art. no. 065202R.

24. Chen, G. R., Mao, Y. B. & Chui, C. K. 2004, "A symmetric image encryption scheme based on 3D chaotic cat maps", *Chaos Solitons & Fractals*, vol. 21, no. 3. pp. 749–761.

25. Pareek, N.K., Patidar, V. & Sud, K. K. 2006, "Image Encryption Using Chaotic Logistic Map", *Image and Vision Computing*, vol. 24, pp. 926-934.

26. Yen, J.-I. & Guo, J.-C. 2000, "Efficient hierarchical chaotic image encryption algorithm and its VLSI realisation", *IEE Proc - Vision, Image, Sign Proc*, vol. 147, no. 2, pp. 167-175.

27. Burkin, I. M. & Kuznetsova, O. I. 2021, "New megastable system with 2-D strip of hidden attractors and analytical solutions" , Chebyshevskii sbornik, vol. 22, no. 4, pp. 360-368.

28. Kuznetsova, O. I., TSU, 2022, "Programma dlya shifrovaniya informatsii s ispolzovaniem megastabilnoy sistemy s 2-D polosoy skrytyh attractorov", *Svidetelstvo o gosudarstvennoy registracii programmy dlya EVM no. 2022666310*, 1 p.

29. Wang, Z., Bovik, A. C. Sheikh, H. R. & Simoncelli, E. P. 2004, "Image quality assessment: from error visibility to structural similarity", *IEEE transactions on image processing*, vol. 13, no. 4, pp. 600—612.

30. Wang, Z. & Bovik, A. C. 2002, "A universal image quality index", *IEEE signal processing letters*, vol. 9, no. 3, pp. 81—84.

Получено: 02.11.2022
Принято в печать: 24.04.2023