УДК 004.94
DOI: 10.26102/2310-6018/2021.35.4.011

Метод автоматизированного контроля скрытой информации в изображении

О.И. Маслова✉, А.А. Жарких, Г.В. Шагрова, В.Г. Струкова

Северо-Кавказский федеральный университет,
Ставрополь, Российская Федерация
oksmaslova@inbox.ru✉

Резюме: Актуальность исследования обусловлена тем, что защита ценных документов от несанкционированного копирования и фальсификации является важной задачей в современном мире. В связи с этим в статье предложен вычислительный метод визуализации скрытой в изображении информации, основанный на модификации известного метода выявления и контроля скрытых изображений, элементы которых выделены алгоритмами вариации направления линий и вейвлет-преобразования файла документа. Отличие разработанного метода заключается в предварительном определении вида анализируемого изображения с внедренным скрытым сообщением, на основе перцептивных хэш-функций. В зависимости от вида скрытой информации и выполняется соответствующее преобразование изображения с помощью ранее определенного вейвлета, характерного для данного вида. Такой подход позволяет сократить время визуализации в 3 раза. Проведен эксперимент с целью проверки предложенного метода, в ходе которого произведено сравнение визуализации цифровых изображений известным методом и разработанным модифицированным с заранее определенным видом изображения. В результате эксперимента установлено, что вычислительный метод позволяет сократить временные затраты в 3 раза. Однако это не окончательный результат, из теоретической модели следует, что вычислительный метод контроля скрытой информации в изображении позволяет сократить временные затраты до 6 раз. Данное утверждение планируется подтвердить экспериментально, используя большее количество видов цифровых изображений.

Ключевые слова: скрытое изображение, латентное изображение, вейвлет-анализ, метод контроля скрытой информации, распознавание скрытых изображений.

Для цитирования: Маслова О.И., Жарких А.А, Шагрова Г.В., Струкова В.Г. Метод автоматизированного контроля скрытой информации в изображении. *Моделирование, оптимизация и информационные технологии.* 2021;9(4). Доступно по: https://moitvivt.ru/ru/journal/pdf?id=1013 DOI: 10.26102/2310-6018/2021.35.4.011

Method for automated control of hidden information in an image

O.I. Maslova✉, A.A. Zharkih, G.V. Shagrova, V.G. Strukova

North-Caucasus Federal University, Stavropol, Russian Federation
oksmaslova@inbox.ru✉

Abstract: The relevance of the study is due to the fact that protecting valuable documents from unauthorized copying and falsification is a critical task in the modern world. In this regard, this article proposes a computational method for visualizing information hidden in an image, based on a modification of the known method for detecting and controlling latent images, the elements of which are highlighted by algorithms for varying the direction of lines and wavelet transformation of the document file. The difference between the developed method lies in the preliminary determination of the type of the analyzed image with an embedded hidden message based on perceptual hash functions. Depending on the type of hidden information, the corresponding transformation of the image is performed using a previously defined wavelet characteristic of this type. This approach reduces

rendering time by three times. An experiment was carried out to test the proposed method. During the test, a comparison was made of the visualization of digital images by the known method and the developed modified one with a predetermined type of image. It was found that the computational method can reduce time costs by three times as a result of the experiment. However, this is not the final result; from the theoretical model, it follows that the computational method for controlling concealed information in the image can reduce the time spent up to six times. This statement is planned to be confirmed experimentally using more types of digital images.

Keywords: hidden image, latent image, wavelet analysis, hidden information control method, hidden image recognition

For citation: Maslova O.I., Zharkih A.A., Shagrova G.V., Strukova V.G. Method for automated control of hidden information in an image. *Modeling, Optimization and Information Technology*. 2021;9(4). Available from: https://moitvivt.ru/ru/journal/pdf?id=1013 DOI: 10.26102/2310-6018/2021.35.4.011 (In Russ).

Введение

Актуальность работы обусловлена тем, что проблема защиты ценных документов, денежных знаков и иной ценной полиграфической продукции стоит очень остро.

Одним из распространенных на сегодняшний день способов защиты ценных документов, денежных знаков и т. д. от несанкционированного копирования и фальсификации является использование скрытых изображений [1-3, 9-10], встраиваемых в защищаемые документы и полиграфическую продукцию (ГОСТ Р 54109 – 2010).

Для защиты путем встраивания скрытых изображений используются специальные способы и приемы печати [9, 10], в том числе методы термохромных, фотохромных УФ красок, методы, основанные на различной вариации параметров [5, 6, 7]. Контроль таких изображений осуществляется разными методами как визуальными, так и автоматизированными.

Для правильного понимания дальнейшей информации следует уточнить, что подразумевается под типом и видом изображений. Изображения делятся на типы в зависимости от метода внедрения в них скрытой информации, а типы, в свою очередь, подразделяются на виды. Например, одним из типов защищаемой полиграфической продукции являются денежные знаки, которые делятся на виды, такие как российские рубли, белорусские рубли, азербайджанские манаты и другие.

Целью данной работы является сокращение времени контроля скрытых изображений за счет модификации известного метода.

Материалы и методы (Materials and Methods)

Рассмотрим известный численный метод, представленный в работе [8]. Данный метод позволяет автоматизировать процесс выявления и контроля скрытых изображений, элементы которого получены методами вариации направлений линий. В основе этого метода лежит вейвлет-преобразование файла документа, защищенного скрытым изображением и сравнение полученных результатов с контрольными. На подготовительном этапе формируется база контрольных изображений, представленных в виде хэшей B. Данную базу формируют с помощью перцептивного хэш-алгоритма. Хэш B, полученный из изображения, соотносится с определенным видом изображения со скрытой информацией $L(x, y)$, зависящим от метода ее внедрения:

$$B[i_{(x,y)}] = \begin{cases} 1, \text{при } S^*(x,y) \geq t, \\ 0, \text{при } S^*(x,y) < t \end{cases} \quad (1)$$

где $S^*(x,y)$ – приведенное к размеру 8x8 выявленное путем вейвлет-преобразования скрытое изображение; x, y – координаты матрицы яркостей изображения; $i_{(x,y)}$ – позиционный элемент хэша для каждого элемента (x,y) контрольного изображения; t – адаптивный порог бинаризации.

Процесс контроля на основе данного метода заключается в следующем: выполняют шесть последовательных вейвлет-преобразований изображения со скрытой информацией, приведенного к оттенкам серого или его повернутой на 30° копии, при условии, что после первых трех преобразований не удалось визуализировать скрытую информацию (2):

$$\begin{cases} L_{Grey}(x,y) = 0.299\,L_R(x,y) + 0.587\,L_G(x,y) + 0.114\,L_B(x,y) \\ L_{Rot30}(x,y) = L_{Grey}\left(\frac{\sqrt{3}}{2}x_i + \frac{1}{2}x_j, -\frac{1}{2}x_i - \frac{\sqrt{3}}{2}x_j\right)\Big|_{i\geq 0,\, j\geq 0} \\ \begin{cases} Conv_R = h_\psi(-n) * L_{Grey}(x,y)\big|_{n=2k,k\geq 0} \\ W_1(1,m,n) = h_\psi(-m) * Conv_R\big|_{m=2k,k\geq 0} \end{cases} \\ \begin{cases} Conv_R = h_\varphi(-n) * L_{Grey}(x,y)\big|_{n=2k,k\geq 0} \\ W_2(1,m,n) = h_\psi(-m) * Conv_R\big|_{m=2k,k\geq 0} \end{cases} \\ \begin{cases} Conv_R = h_\psi(-n) * L_{Grey}(x,y)\big|_{n=2k,k\geq 0} \\ W_3(1,m,n) = h_\varphi(-m) * Conv_R\big|_{m=2k,k\geq 0} \end{cases} \\ \begin{cases} Conv_R = h_\psi(-n) * L_{Rot30}(x,y)\big|_{n=2k,k\geq 0} \\ W_4(1,m,n) = h_\psi(-m) * Conv_R\big|_{m=2k,k\geq 0} \end{cases} \\ \begin{cases} Conv_R = h_\varphi(-n) * L_{Rot30}(x,y)\big|_{n=2k,k\geq 0} \\ W_5(1,m,n) = h_\psi(-m) * Conv_R\big|_{m=2k,k\geq 0} \end{cases} \\ \begin{cases} Conv_R = h_\psi(-n) * L_{Rot30}(x,y)\big|_{n=2k,k\geq 0} \\ W_6(1,m,n) = h_\varphi(-m) * Conv_R\big|_{m=2k,k\geq 0} \end{cases} \\ E(x,y) = W_a(1,m,n)\big|_{1\leq a\leq 6} \end{cases} \quad (2)$$

где $L(x,y,z)$ – изображение со скрытой информацией; $L_{Grey}(x,y)$ – изображение со скрытой информацией, преобразованное к оттенкам серого; $L_{Rot30}(x,y)$ – изображение со скрытой информацией в оттенках серого, повернутое на 30°; $Conv_R$ – свертка вейвлет функции по строкам изображения; $W_a(1,m,n)$ – детализирующие вейвлет-коэффициенты; $E(x,y)$ – визуализированное скрытое изображение; x, y, z – координаты цветовых компонент в системе RGB.

Для установки факта визуализации скрытой информации после каждого преобразования полученный бинаризированный результат, представленный в виде хэша B'(3), сравнивается с одним из хэшей B (1) в базе контрольных изображений (4).

Вычисление хэша B′ преобразованного изображения E(x,y) производится по формуле 3:

$$B'[i_{(x,y)}] = \begin{cases} 1, \text{при } E^*(x,y) \geq t, \\ 0, \text{при } E^*(x,y) < t \end{cases} \quad (3)$$

где $E^*(x,y)$ – приведенное к размеру 8x8 преобразованное изображение.

Сравнение хэшей производится путем вычисления расстояния Хэмминга хэшей $d(B,B')$и сравнением его с заданным порогом точности T:

$$\begin{cases} d(B,B') = \sum_{k=1}^{64} |B_i - B'_i| \\ \begin{cases} B = B', & \text{при } d(B,B') \leq T \\ B \neq B', & \text{при } d(B,B') > T \end{cases} \\ T = 64 * k, \quad 0{,}8 \leq k \leq 1 \end{cases} \quad (4)$$

где B – хэш скрытого изображения из базы контрольных изображений; B' – хэш преобразованного изображения; T – заданный порог точности; k – экспериментально подобранный коэффициент, обеспечивающий минимальное количество ложных результатов.

В случае равенства хэшей считается, что визуализировано скрытое изображение, и устанавливается, к какому виду оно относится.

К числу недостатков данного метода можно отнести: необходимость выполнения шести последовательных вейвлет-преобразований, каждое из которых требует существенных временных затрат; невозможность по визуализированной скрытой информации точно определить вид изображения при ее внедрении в композиционно разные исходные изображения и, как следствие, достоверно определить подлинность анализируемого изображения.

Результаты (Results)

В данной работе предложена модификация существующего метода, позволяющая сократить время контроля, за счет применения конкретного вейвлет-преобразования, соответствующего виду анализируемого изображения. Таким образом, первоначально определяется, к какому виду относится анализируемое изображение, содержащее скрытую информацию, а затем уже выполняется вейвлет-преобразование. Причем выполняется только одно предварительно определенное для данного вида преобразование.

Сущность предлагаемого метода состоит в том, что на подготовительном этапе проводится анализ эталонного изображения со скрытой информацией $L(x,y)$ путем его шести вейвлет-преобразований в соответствии с системой уравнений (2) и определяется, какое одно из вейвлет преобразований позволяет визуализировать скрытую информацию $S(x,y)$, записываемую в базу контрольных изображений в виде хэша. Таким образом, определяется:

1. Хэш эталонного изображения со скрытой информацией A.
2. Хэш скрытого изображения B.
3. Номер преобразования P, с помощью которого анализируемое изображение $L(x,y)$ приводится к виду $S(x,y)$.
4. Буквенное обозначение вида изображения $type$.

$$\text{id}=\begin{cases} A_{id}[i_{(x,y)}]=\begin{cases}1, \text{при } L^*(x,y)\geq t,\\ 0, \text{при } L^*(x,y)<t\end{cases}\\ B_{id}[i_{(x,y)}]=\begin{cases}1, \text{при } S^*(x,y)\geq t,\\ 0, \text{при } S^*(x,y)<t\end{cases}\\ P_{id}\in\{1,2,3,4,5,6\}\\ type_{id}\end{cases} \quad (5)$$

где id – номер записи в базе контрольных изображений, соответствующий виду изображения;$L^*(x,y)$ – приведенное к размеру 8x8 изображение со скрытой информацией; $S^*(x,y)$ – приведенное к размеру 8x8 выявленное путем вейвлет-преобразования скрытое изображение; x,y – координаты матрицы яркостей изображения; $i_{(x,y)}$ – позиционный элемент хэша для каждого элемента (x,y) контрольного изображения; t – адаптивный порог бинаризации.

На основе предложенного метода разработан модифицированный численный метод, который заключается в следующем:

изображение со скрытой информацией $L(x,y,z)$ преобразуется к оттенкам серого $L_{Grey}(x,y)$:

$$L_{Grey}(x,y)=0.299L_R(x,y)+0.587L_G(x,y)+0.114L_B(x,y) \quad (6)$$

Определяется вид изображения $type_{L(x,y)}$ и необходимое для выявления преобразование $P_{L(x,y)}$, путем сравнения хэшей анализируемого изображения A' с хэшами A_{id} базы контрольных изображений.

$$\begin{cases} A'[i_{(x,y)}]=\begin{cases}1, \text{при } L^*(x,y)\geq t,\\ 0, \text{при } L^*(x,y)<t\end{cases}\\ d(A_{id},A')|_{id=1}^{N}=\sum_{k=1}^{64}\left|A_{(id,i)}-A'_i\right|\\ \begin{pmatrix} A_{id}=A'\\ type_{L(x,y)}=type_{id}\\ P_{L(x,y)}=P_{id}\end{pmatrix}, \text{при } d(A,A')\leq T_A\\ A_{id}\neq A', \text{ при } d(A,A')>T_A\end{cases}\Bigg|_{id=1}^{N} \quad (7)$$

где $d(A,A')$ – разница хэшей A и A'; id – номер записи в базе контрольных изображений вид изображения; A – хэш скрытого изображения из базы контрольных изображений; A' – хэш преобразованного изображения; N – число записей в базе контрольных изображений; T_A – заданный порог точности при сравнении хэшей A и A'.

Осуществляется преобразование $W_{P_{L(x,y)}}(1,m,n)$ с использованием биортогонального вейвлета с базисом 2.8 путем вейвлет-преобразования изображения $L_{Grey}(x,y)$ или повернутого на 30 градусов изображения $L_{Rot30}(x,y)$. Визуализированные вейвлет-коэффициенты образуют изображение $E(x,y)$:

$$\begin{cases} h_\psi(t) = \{\{0.0,0.0,0.0,0.0,0.0,0.0,0.0,0.3535533905932738, \\ -0.7071067811865476,0.3535533905932738,0.0,0.0,0.0,0.0,0.0,0.0,0.0,0.0\} \\ h_\varphi = \{\{0.0,0.0015105430506304422,-0.0030210861012608843, \\ -0.012947511862546647, \\ 0.02891610982635418,0.052998481890690945,-0.13491307360773608, \\ -0.16382918343409025,0.4625714404759166,0.9516421218971786, \\ 0.4625714404759166,-0.16382918343409025,-0.13491307360773608, \\ 0.052998481890690945,0.02891610982635418,-0.012947511862546647, \\ -0.0030210861012608843,0.0015105430506304422\} \\ \begin{cases} \begin{cases} Conv_R = h_\psi(-n) * L_{Grey}(x,y)\big|_{n=2k,k\geq 0} \\ E(x,y) = h_\psi(-m) * Conv_R|_{m=2k,k\geq 0} \end{cases}, \text{ при } P_{L(x,y)} = 1 \\ \begin{cases} Conv_R = h_\varphi(-n) * L_{Grey}(x,y)\big|_{n=2k,k\geq 0} \\ E(x,y) = h_\psi(-m) * Conv_R|_{m=2k,k\geq 0} \end{cases}, \text{ при } P_{L(x,y)} = 2 \\ \begin{cases} Conv_R = h_\psi(-n) * L_{Grey}(x,y)\big|_{n=2k,k\geq 0} \\ E(x,y) = h_\varphi(-m) * Conv_R|_{m=2k,k\geq 0} \end{cases}, \text{ при } P_{L(x,y)} = 3 \\ \begin{cases} Conv_R = h_\psi(-n) * L_{Rot30}(x,y)|_{n=2k,k\geq 0} \\ E(x,y) = h_\psi(-m) * Conv_R|_{m=2k,k\geq 0} \end{cases}, \text{ при } P_{L(x,y)} = 4 \\ \begin{cases} Conv_R = h_\varphi(-n) * L_{Rot30}(x,y)|_{n=2k,k\geq 0} \\ Conv_R = h_\psi(-n) * L_{Rot30}(x,y)|_{n=2k,k\geq 0} \end{cases}, \text{ при } P_{L(x,y)} = 5 \\ \begin{cases} Conv_R = h_\psi(-n) * L_{Rot30}(x,y)|_{n=2k,k\geq 0} \\ Conv_R = h_\varphi(-n) * L_{Rot30}(x,y)|_{n=2k,k\geq 0} \end{cases}, \text{ при } P_{L(x,y)} = 6 \end{cases} \end{cases} \quad (8)$$

Определяется хэш контролируемого изображения B′ по формуле 3. Устанавливается наличие скрытой информации в изображении. Сравнение хэшей выполняется по аналогии с известным методом.

Обсуждение (Discussion)

Для проверки предложенного метода проведен эксперимент. В качестве исследуемых образцов использовали изображения 4-х видов (отсканированные деньги): Белорусские рубли, Азербайджанские манаты, Российские рубли, паспорта РФ. Все исследуемые цифровые изображения вышеуказанных видов цветные в формате jpg. На первом этапе изображения сначала визуализировали известным методом без определения вида их заранее. На втором этапе проводили визуализацию тех же цифровых изображений модифицированным методом, т. е. заранее определяли их вид. На третьем этапе время визуализации, полученное вышеуказанными методами, сравнили и определили, какой из методов позволяет сократить временные затраты.

В ходе эксперимента удалось установить, что модифицированный метод позволяет сократить время контроля в 3 раза (Таблица 1). Осуществляется это за счет того, что изначально определяется вид анализируемого изображения и, в зависимости от данного вида, используется определенная последовательность вейвлет-преобразований.

Таблица 1 – Результаты эксперимента
Table 1 – Experiment results

Вид цифрового изображения	Среднее время визуализации известным методом (без заранее определенного типа ЦИ) сек.	Среднее время визуализации модифицированным методом (с заранее определенным типом ЦИ) сек.	Сокращение временных трудозатрат (количество раз)
Белорусские рубли	45	28	1,6
Азербайджанский манат	38	12	3,2
Российские рубли	22	17	1,3
Паспорт РФ	12	11	1,1

Утверждать, что любое изображение независимо от вида удастся распознать быстрее в 6 раз, нельзя, т. к. один вид изображений для контроля требует только одно вейвлет-преобразование, а для контроля изображения другого вида может потребоваться несколько вейвлет преобразований и за счет этого время контроля изображений будет разным. Относительно исследованных видов изображений временные затраты сократились в 3 раза.

Заключение

В работе предложен модифицированный численный метод автоматизированного контроля скрытой информации в изображении, позволяющий уменьшить временные затраты за счет изменения существующего алгоритма. Сокращение времени удалось достичь за счет определения вида исследуемого изображения до выполнения вейвлет-преобразований, т. е. на подготовительном этапе, и далее, в зависимости от вида изображения, производить определенное для данного вида преобразование. Таким образом, временные затраты сократились в 3 раза.

СПИСОК ИСТОЧНИКОВ

1. Шевелев А.А. Создание латентных изображений с использованием стохастических растровых структур. *Технологія і техніка друкарства*. 2009;1-2(23-24):226–233.
2. Маккарти Л.Д., Свиджерс Г.Ф. Способ формирования латентного изображения: патент на изобретение RUS 2337403: G 06 T 5 00,G 06 K 9 00. Правообладатель: *Коммонвелс сайнтифик энд индастриал рисеч организейшен;* дата регистрации 04.06.2004.
3. Goryaev M.A. Two models of the latent image formation. *IS and T's 52nd Annual Conference. Savannah, GA.* 1999;52:11–13.
4. Mowry W. Protected document bearing watermark and method of making, U.S. Patent 4,210,346. Burroughs Corporation; 1977.
5. Hutton R.G. Documents of value including intaglio printed transitory images, U.S. Patent 4,033,059. American Banknote Company, New York; 1977.
6. Koltai F. Anti-counterfeiting method and apparatus using digital screening. U.S. Patent 6,104,812. Juratrade Limited; 1998.

7. Koltai F. Enhanced optical security by using information carrier digital screening. *SPIE Conference on Optical Security and Counterfeit Deterrence Techniques V*. 2004;5:160–169.
8. Жарких А.А. Математическое моделирование формирования и контроля латентных изображений: диссертация кандидата технических наук. Северо-Кавказский федеральный университет, Ставрополь; 2017.
9. Maslova O.I, Shagrova G.V. An algorithm for implementation and recognition of hidden images based on discrete waves of transformation and singular decomposition of matrices. *Студенческая наука для развития информационного общества*. *X Всероссийская науч.-техн. Конференция с международным участием*. *Изд-во СКФУ*. 2019;2:444–452.
10. Жарких А.А., Шагрова Г.В., Маслова О.И. Пакетное вейвлет-разложение и анализ латентного изображения, полученного методом вариации направления линий. *Современная наука и инновации*. 2018;24(4):11–19.

REFERENCES

1. Shevelev A.A. Sozdanie latentnykh izobrazhenii s ispol'zovaniem stokhasticheskikh rastrovykh struktur. *Tekhnologiya i tekhnika drukarstva*. 2009;1-2(23-24):226–233. (In Russ.)
2. Makkarti L.D., Svidzhers G.F. Sposob formirovaniya latentnogo izobrazheniya: patent na izobretenie RUS 2337403: G 06 T 5 00, G 06 K 9 00. Pravoobladatel': *Kommonvels saintifik end indastrial risech organizeishen;* data registratsii 04.06.2004. (In Russ.)
3. Goryaev M.A. Two models of the latent image formation. *IS and T's 52nd Annual Conference. Savannah, GA*. 1999;52:11–13.
4. Mowry W. Protected document bearing watermark and method of making, U.S. Patent 4,210,346. Burroughs Corporation; 1977.
5. Hutton R.G. Documents of value including intaglio printed transitory images, U.S. Patent 4,033,059. American Banknote Company, New York; 1977.
6. Koltai F. Anti-counterfeiting method and apparatus using digital screening. U.S. Patent 6,104,812. Juratrade Limited; 1998.
7. Koltai F. Enhanced optical security by using information carrier digital screening. *SPIE Conference on Optical Security and Counterfeit Deterrence Techniques V*. 2004;5:160–169.
8. Zharkih A.A. Matematicheskoe modelirovanie formirovaniya i kontrolya latentnykh izobrazhenii: dissertatsiya kandidata tekhnicheskikh nauk. Severo-Kavkazskii federal'nyi universitet, Stavropol'; 2017. (In Russ.)
9. Maslova O.I, Shagrova G.V. An algorithm for implementation and recognition of hidden images based on discrete waves of transformation and singular decomposition of matrices. *Student science for the development of the information society. X All-Russian scientific and technical. Conference with international participation. Publishing house of NCFU*. 2019;2:444–452. (In Russ.)
10. Zharkih A.A., Shagrova G.V., Maslova O.I. Paketnoe veivlet-razlozhenie i analiz latentnogo izobrazheniya, poluchennogo metodom variatsii napravleniya linii. *Sovremennaya nauka i innovatsii*. 2018;24(4):11–19. (In Russ.)

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Маслова Оксана Игоревна, программист кафедры информационных систем и технологий института цифрового развития, Северо-Кавказский федеральный университет (СКФУ). Ставрополь, Российская Федерация.
e-mail: oksmaslova@inbox.ru
ORCID: 0000-0002-9972-5735

Maslova Oksana, programmer of the Department of Information Systems and Technologies, Institute Digital Development, North Caucasian Federal University (NCFU). Stavropol, Russian Federation.

Жарких Андрей Анатольевич, кандидат технических наук, доцент кафедры информационных систем и технологий института цифрового развития, Северо-Кавказский федеральный университет (СКФУ) Ставрополь, Российская Федерация
e-mail:azh89@mail.ru

Zharkih Andrey, Candidate of Technical Sciences, Associate Professor of chair Information Systems and Technologies, Institute Digital Development, North Caucasus Federal University (NCFU) Stavropol, Russian Federation

Шагрова Галина Вячеславовна, доктор физико-математических наук, профессор кафедры информационных систем и технологий института цифрового развития, Северо-Кавказский федеральный университет (СКФУ), Ставрополь, Российская Федерация.
e-mail: g_shagrova@mail.ru

Shagrova Galina, Doctor of Physico-Mathematical Sciences, Professor of chair Information systems and technologies, Institute Digital Development, North Caucasian Federal University (NCFU), Stavropol, Russian Federation.

Струкова Виктория Геннадьевна, аспирант третьего года обучения, спец. 09.06.01 «Информатика и вычислительная техника», кафедра», кафедра информационных систем и технологий института цифрового развития, Северо-Кавказский федеральный университет (СКФУ). Ставрополь, Российская Федерация.
e-mail: vivata.21@mail.ru
ORCID: 0000-0002-1689-784X

Strukova Viktoria, post-graduate student of the third year of study, special. 09.06.01 Informatics and Computer Engineering, Department of Information Systems and Technologies, Institute of Digital Development, North Caucasus Federal University (NCFU). Stavropol, Russian Federation.

Статья поступила в редакцию 25.06.2021; одобрена после рецензирования 05.10.2021; принята к публикации 21.10.2021.

The article was submitted 25.06.2021; approved after reviewing 05.10.2021; accepted for publication 21.10.2021.