Ключові слова: *текстон, зміна текстури, хаотичний динамічний режим, ентропія подібності, часові ряди, значення субзображень*

Цель. Благодаря своему разнообразию, текстон сварочного изображения мало заметен, и дефекты сварки трудно обнаружить автоматически. Цель данной работы заключается в определении текстурных изменений изображения сварного шва для обнаружения дефектов сварки и определении оптимального числа элементов, в частности, в хаотичном динамическом режиме.

Методика. Текстура характеризуется энтропией подобия, которая рассчитывается в фазовом пространстве. Временные ряды реконструируются с энтропией значений субизображений для выбора из соответствующих параметров текстуры. Применяя хаотическую теорию, мы предложили метод поиска зоны резких текстурных изменений.

Результаты. Сначала мы получаем энтропию подобия в фазовом пространстве, а затем, с помощью метода поиска зоны изменений текстуры неровностей, мы находим область изменения соответствующей текстуры.

Научная новизна. Нами проведено исследование области резких текстурных изменений. Рассмотрена реконструкция принципа временных рядов, энтропия подобия определения порога мутации.

Практическая значимость. На практике, возможно реконструировать временные ряды с энтропией значений субизображений на первом этапе, эти результаты намного более точны в зоне резких текстурных изменений.

Ключевые слова: *текстон, изменение текстуры, хаотический динамический режим, энтропия подобия, временные ряды, значения субизображений*

Рекомендовано до публікації докт. техн. наук В. В. Гнатушенком. Дата надходження рукопису 25.10.15.

Changjiu Pu,
Fei Hu,
Jie Long

Chongqing University of Education, Chongqing, China

AN IMAGE COPYRIGHT PROTECTION AND TAMPERING DETECTION SCHEME BASED ON DEEP LEARNING AND MEMRISTOR

Чанцзю Пу,
Фей Ху,
Цзе Лун

Чунчинський університет освіти, Чунцин, Китай

СХЕМА ЗАХИСТУ АВТОРСЬКИХ ПРАВ І ВИЯВЛЕННЯ ФАЛЬСИФІКАЦІЇ ЗОБРАЖЕНЬ НА ОСНОВІ ГЛИБИННОГО НАВЧАННЯ ТА МЕМРИСТОРА

Purpose. In order to improve the effect of image copyright protection and detect whether an image is tampered illegally, we introduce an image copyright protection and tampering detection scheme of ROI (Region of interest) image based on image feature sequence in NROI (Non Region of interest) image. We have evaluated this scheme with some performance measures and the results show it is effective.

Methodology. We formulate the scheme using the copyright watermarking and the fragile watermarking. With the deep learning, memristor chaos, Arnold transform and extend zigzag transform, the watermarkings are generated and embedded into ROI image in DCT (Discrete cosine transform) domain using the feature sequence of NROI image.

Findings. We first completed the division of ROI and NROI image and get the feature sequence of NROI image using deep learning and memristor chaos. Then by using the sequence and some methods such as Arnold transform, we obtained the scrambling copyright watermarking and the new fragile watermarking of each image grouping and embedded them into ROI image.

Originality. We realize the extraction of image feature sequence in NROI image using deep learning and memristor chaos. It is applied to generate and embed the scrambling copyright watermarking and the new fragile watermarking into ROI image. The research on this aspect has not been found at present.

Practical value. We have completed some validation experiments with some performance measures. The results show it can completely satisfy the need of secure transmission. This scheme features strong robustness and security.

Keywords: *image feature, image protection, tampering detection, copyright, memristor, deep learning*

Introduction. With the development of information technology, the application and development of computer network has brought great convenience to the transmission of image. As a result, the secure transmission of image over the internet has become a common interest in the fields of research and application. The traditional solution is to use image encryption, but the effect of protection disappears after receiving and decrypting. And image encryption is not conducive to communication and displaying. It also cannot solve the problems of piracy, infringement and arbitrary tampering [1].

In order to solve these problems, digital watermarking technology has been widely used for copyright protection [2] and tampering detection [3–4], which plays a certain role in ensuring the security of the image. Furthermore, there are many research findings with the architecture of combining copyright protection and tampering detection [4]. The general deficiencies or flaws of these algorithms are summarized as follows:

1. The key for watermarking is independent of the image. The addition of image feature can greatly improve the security of the algorithm, but many algorithms do not use the image feature. Since the principle of the algorithm is to embed copyright watermarking or fragile watermarking into the image, the required original image feature may be damaged by the new information. In order not to harm the required original image feature information, the selected feature of some algorithms may be less important or representative.

2. Some algorithm can be further optimized in the protection region. If the information content of a picture is relatively large, the processing of the entire image is bound to consume amount of computer resources and time. However, not every place is important in reality and people only need to focus on ROI image [5–6] in some industries and fields. For instance, if the ROI image may be modified or copyright of image is broken, it must be retrieved and not used any longer. But the image is available when the watermarking of ROI image is correct. So image protection is the focus of copyright protection and tampering detection of ROI image.

According to the analysis and research, the paper introduces an image copyright protection and tampering detection scheme of ROI image based on image feature sequence in NROI image. The scheme extracts feature sequence from the NROI image using deep learning and memristor chaos, the feature is used for image copyright protection and tampering detection in ROI image. This scheme can not only combine copyright protection and tampering detection using feature sequence, but also has the advantages of easy implementation, high security and high sensitivity.

Related working. ***Deep learning.*** In 2006, Hinton proposed the concept of deep learning, which successfully solves time consuming problem for large scale data computation and has high precision. The deep learning has been successfully applied to a variety of problems in artificial intelligence research, especially in image processing, voice recognition and analysis of intelligent network [7].

Deep learning can be used for image feature and the purpose of deep learning is just the feature learning. In order to discover the distributed feature of data, the abstract high-level features can be obtained from the low level features using deep learning to construct a machine learning model with many hidden layers. So, the deep learning algorithm is very suitable to extract feature sequence of the NROI image in this paper.

Deep learning has a lot of algorithm models，such as RBM (Restricted Boltzmann Machine) and DBN (Deep Belief Network) [8]. The basic equations of RBM are shown as equations (1–4).

$$E(v,h) = -\sum_{i\in \text{visivle}} a_i v_i - \sum_{j\in \text{hidden}} b_j h_j - \sum_{i,j} v_i h_j w_{i,j}. \quad (1)$$

Where $w_{i,j}$ are the connection weights between visible layer node v_i and hidden layer node h_j, a_i and b_j respectively are the bias value for v_i and h_j. The joint probability between v and h is shown as follows

$$p(v,h) = \frac{1}{Z} e^{-E(v,h)}, \quad (2)$$

where Z is a normalization factor and the value is obtained as follows

$$Z = \sum_{v,h} e^{-E(v,h)}, \quad (3)$$

where probability distribution function of v is obtained as follows

$$P(v) = \sum_{h} P(v,h) = \sum_{h} \frac{e^{-E(v,h)}}{Z}. \quad (4)$$

RBM is not the best way to capture image features. DBN is usually composed of multiple RBM overlays; it adopts unsupervised training method and has better performance of reduction dimension than RBM. DBN uses the way of training by layer by layer. DBN and RBM can both be used for image feature sequence extraction. In this paper, the DBN is used to extract feature sequence form the NROI image, which has a better feature extraction capability than a single hidden layer.

Memristor. The memristor is a kind of variable resistor with memory function, which can be controlled by the external voltage. The memristor chaos is different from general chaos. It can not only change with the parameters, but also depends on the initial value. Starting from 1971, Leon 0 Chua, who is a nonlinear circuit expert in University of California, Berkeley, first proposed and studied the memristor form in the paper "Memristor – The Missing Circuit Element". It attracts more and more attention of researchers. Since the chaotic equation of the memristor can be obtained

by different memristor elements or changing circuit, many research findings in Memristor chaos based on different memristor elements or changing circuit have been constantly emerging [9–10].

The most important characteristic of the memristor chaos is nonlinearity, which is very easy to produce a chaotic oscillation signal. The memristor chaos also has other characteristics, such as randomness and sensitivity, so it is suitable to use in image copyright protection and tampering detection. The selected circuit of memristor is shown as follows (Fig. 1)

According to the volt ampere characteristics of resistance, capacitance and inductance components, the differential equations of three state variables can be obtained using Kirchhoff voltage and current law

$$\begin{cases} \dfrac{dv_{c1}}{dt} = \dfrac{v_{c1}}{RC_1} + \dfrac{v_{c2}}{RC_1} - \dfrac{f(v_{c1})}{C_1} \\ \dfrac{dv_{c2}}{dt} = \dfrac{v_{c1}}{RC_2} + \dfrac{v_{c2}}{RC_2} - \dfrac{i_L}{C_2} \\ \dfrac{di_L}{dt} = -\dfrac{v_{c2}}{L} + \dfrac{ri_L}{L} \end{cases}, \quad (5)$$

where v_{c1} and v_{c2} respectively are the voltage of capacitance C_1 and C_2, i_L is the current of inductance L.

According to the method of memristor chaos described in above, the sequence $P\{P_1, P_2, ..., P_i, ...\}$ is generated by using initial values and parameters in this paper.

Algorithm. ***Division in nroi and roi image.*** In the scheme, image feature sequence of NROI image is needed to use in image copyright protection and tampering detection scheme. It is important to divide the image into NROI and ROI because different divisions will bring about different results. In order to protect ROI image safety and integrity, it may be necessary to enlarge ROI image. The main method of division is described as follows (Assume the size of image is $M \times N$):

1. Consider whether the ROI image meets the requirements, because ROI image can be of any shape and it will be grouped in the later operation. So it is necessary to make sure whether the ROI image meets rule of grouping. If the original ROI image is not rectangle, the new ROI image will become the smallest rectangle including the original ROI image. Then it is necessary to test whether the length and width are all divisible by 8. If it is satisfy, the next step is to go to (4), otherwise go to (2).

2. Adjust the ROI image. It must satisfy that ROI image is rectangle and the length and width are also divisible by 8. So the new ROI image is established as follows: Assume that the coordinates of the 4 points of the rectangle respectively are $A_1(x_1, y_1)$, $A_2(x_1, y_2)$, $A_3(x_2, y_1)$, $A_4(x_2, y_2)$, and the distances to the image edge respectively are a, b, c and d. It is shown in Fig. 2.

3. Generate a_1, b_1, c_1 and d_1 (They are positive integer and less than 6, which cannot exceed the edge of the image) using memristor chaos. Then adjust the values to satisfy the following equations

$$\begin{cases} \text{mod}((x_2 - x_1 + 1), 8) = 0 \\ \text{mod}((y_2 - y_1 + 1), 8) = 0 \end{cases}. \quad (6)$$

If the first equation of (6) is not satisfactory, the position of X coordinates A_1 and A_3 may respectively change to $x_1 - b_1$ and $x_2 + d_1$, The method is shown as follows:

$$\begin{aligned} &b_1 = 0;\ d_1 = \text{ob\_}mivalue();\\ &\text{while } (\text{mod}((x_2 + d_1 - x_1 + 1), 8) <> 0 \,\&\&\\ &((x_2 + d_1) < M))\\ &\{d_1 = d_1 + 1;\}\\ &b_1 = \text{ob\_}mivalue();\\ &\text{while } (\text{mod}((x_2 + d_1 - (x_1 - b_1) + 1), 8) <> 0 \,\&\&\\ &((x_2 + d_1) == M))\\ &\{b_1 = b_1 - 1;\}, \end{aligned}$$

where the function of ob_*mivalue*(...) is obtaining the value b_1 according the memristor chaos and requirement. In the same way, if the second equation of (6) is not satisfy, position of Y coordinates A_1 and A_2 may respectively change to $y_1 - a_1$ and $y_2 + c_1$. So

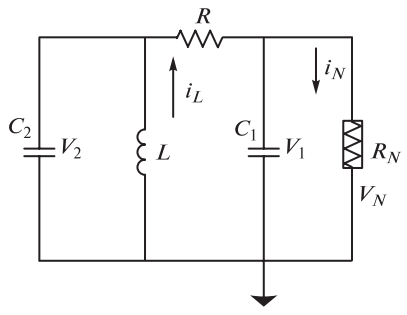

Fig. 1. The circuit of memristor

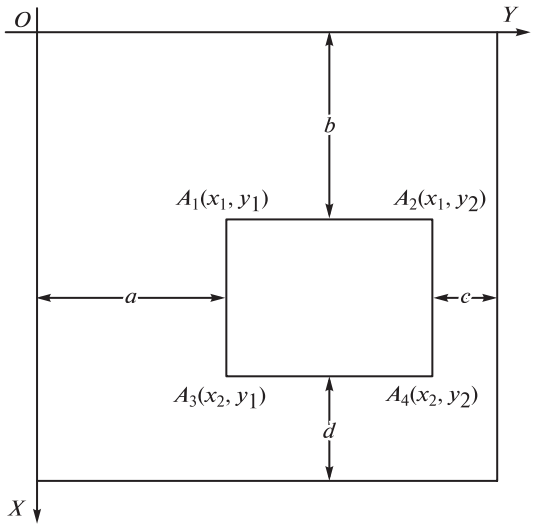

Fig. 2. Division in NROI and ROI Image

the new edge coordinates are $A_1'(x_1 - b_1, y_1 - a_1)$, $A_2'(x_1 - b_1, y_2 + c_1)$, $A_3'(x_2 + d_1, y_1 - a_1)$ and $A_4'(x_2 + d_1, y_2 + c_1)$.

4. Obtain the new ROI image A''.

Image feature sequence. Image information is abundant and image feature has no uniform or precise definition, so there are many feature types such as color feature, texture feature, shape feature, and spatial relation. In order to improve the security of scheme, each image need have different keys, so it is necessary to extract image feature as the keys. Because part of feature may affect the effect of the image copyright protection and tampering detection, some algorithms extract a less significant feature in some papers.

However the original image is divided into two parts (NROI and ROI) in this paper. Any feature, which is extracted from NROI image, has no effect on image copyright protection and tampering detection of ROI image. So this paper does not use single image feature.

In this paper, the NROI image is trained using a deep learning model to generate the weight values of NROI image, the weight values and the sequence of memristor chaos are combined to the sequence as image feature sequence. The detailed process is described as follows:

1. Determine the number and the order of the NROI image. The NROI image may be divided into several pictures in some cases such as the image is cut to two pieces by the ROI image, and then the order of NROI image is needed to arrange into the deep learning.

2. Initialize the number of layers and neurons in each layer. And weight values between neurons from adjacent layers are initialized according to the initial key (the decimal portion of partial sequence of $P\{P_1, P_2, ..., P_i, ...\}$).

3. The NROI image (One or more images) is used to train this model, and the sequence $L\{L_1, L_2, ..., L_i, ...\}$ is generated by weight values from deep learning which may be selected and sorted using memristor sequence.

4. In order to ensure the randomness of the middle weight values, the new sequence $L'\{L_1', L_2', \cdots, L_3', \cdots\}$ can be obtained by using $P\{P_1, P_2, ..., P_i, ...\}$ and $L\{L_1, L_2, ..., L_i, ...\}$ according to Equation (7)

$$L_i' = \mathrm{mod}((P_i + L_i), 10). \quad (7)$$

Watermarking. The copyright watermarking. Image copyright watermarking is relatively simple (0-1 sequence). In order to improve safety and robustness of copyright watermarking, the watermarking needs to be pre-processed before using it. According to Arnold transform, matrix transform, the sequence $L'\{L_1', L_2', \cdots, L_i', \cdots\}$ described in section 3.2 and input parameters, the new watermarking sequence is generated as follows:

1. Input the watermarking image $B(m \times m)$, $s1$(The starting position of the sequence $L'\{L_1', L_2', \cdots, L_i', \cdots\}$), a and b(a and b are parameters of Arnold transform).

2. Initialize the Arnold transform and complete the first Arnold transform to generate the new copyright watermarking B', the number of Arnold transform is $time1$

$$\begin{cases} time1 = \mathrm{mod}(round(L_{s1}' \times 10^{10}), (cts - 3)) \\ time2 = \mathrm{mod}(round(L_{s1+1}' \times 10^{10}), (cts - 3)) \end{cases}, \quad (8)$$

where cts is the cyclic periodic of Arnold transform when the size of image is $m \times m$. Arnold transform has periodicity and the time Arnold transform needs to avoid the cycle number, so $time1 \in [3, cts - 3]$. If $time1$ is less than 3, $time1$ is equal to 3. The requirements of $time1$ and $time2$ are the same.

3. Generate the new watermarking C from B' using image grouping and exchange. The method is as follows: The image is divided into 4 parts (B_{11}', B_{12}', B_{21}' and B_{22}'), the number of exchange is 24. But it only has 4 choices in this paper: Non-exchange, horizontal-exchange, vertical-exchange and diagonal-exchange. So according to the input parameter, the new watermarking C is generated by image exchange.

4. Complete the second Arnold transform to generate the new watermarking image D according to $time2$.

5. Transform D to a one-dimensional sequence $D'\{D_1', D_2', ..., D_{m \times n}'\}$ using matrix transform.

The fragile watermarking. The tampering detection of image is mainly achieved by the fragile watermarking, which is very sensitive in contrast to the copyright watermarking. It is mainly used to ensure the integrity of the image. When authenticating each image grouping of the ROI image integrity, the embedded fragile watermarking is extracted from the next image grouping for comparison with the generation watermarking to identify whether the image grouping has been tampered. So the generating procedure of the fragile watermarking is important. The detail is shown as follows:

1. Input the ROI image A'' and the parameter km.

2. The image A'' is divided into sub grouping according to the size of . The DCT coefficient matrix of each image grouping can respectively be obtained after the DCT transform and quantization.

3. According to DCT coefficient matrix, the fragile watermarking of each grouping image can be generated by some low frequency coefficient. The process of obtaining is shown as follows.

First, according to the sequence value, h_{s+m} can be obtained using the Equation (9). Then the zigzag traversal method of the frequency coefficient is solved by the value of h_{s+m}.

$$h_{s+m} = \mathrm{mod}(round(L_{km+m}' \times 10^{10} + P_m), 4), \quad (9)$$

where m is the m-th image grouping. P_m is the m-th value of sequence $P\{P_1, P_2, ..., P_i, ...\}$.

Second, according to zigzag traversal method, the fragile watermarking of $A''(m)$ is obtained as follows

$$\begin{cases} block.A''_{\inf}(m) = \mathrm{mod}((m+ \\ +round(A''_m(1,1)/Q(1,1))+ \\ +round(A''_m(2,1)/Q(2,1))- \\ -round(A''_m(1,2)/Q(1,2))+\cdots+ \\ +P_m)*10^5,256) \\ block.A''_{\inf}(m) = \mathrm{mod}((m+ \\ +round(A''_m(1,1)/Q(1,1))+ \\ +round(A''_m(1,2)/Q(1,2))- \\ -round(A''_m(2,1)/Q(2,1))+\cdots+ \\ +P_m)*10^5,256) \end{cases}, \quad (10)$$

where $block.A''_{\inf}(m)$ is the fragile watermarking of m-th image grouping, $Q(i, j)$ is quantization step, $A''(i, j)$ is the low frequency coefficient according to zigzag traversal method. The number of $A''(i, j)$ is 5 to 10, which is solved by the following equation

$$count_{h_{s+m}} = 5 + \mathrm{mod}(round(L'_{km+m} \times 10^{10}),6). \quad (11)$$

Accord to Equation (10), the bit of the fragile watermarking is 8. But too much information is easy to reduce the resolution ratio of ROI image, so the bits of fragile watermarking $block.A''_{\inf}(m)$ are reduced to 4 bits using the following Equation (12)

$$bit.A''_{\inf}(m) = bitxor(bitand(7, block.A''_{\inf}(m)), \\ bitshift(bitand(240, block.A''_{\inf}(m)), -4)). \quad (12)$$

The procedure of algorithm.

1. Input the original image A, the copyright watermarking B and the parameters.

2. Divide entire image into NROI and ROI image and scan NROI image to obtain image feature sequence $L'\{L'_1, L'_2, ..., L'_i, ...\}$ using deep learning and memristor chaos according to the methods described in section 3.1 and 3.2.

3. Generate copyright watermarking sequence $D'\{D'_1, D'_2, ..., D'_{m \times m}\}$ according to the method described in section 3.3.1.

4. Divide the ROI image into sub grouping according to the size of . The DCT coefficient matrix of each image grouping can respectively be obtained after the DCT transform and quantization.

5. Generate the fragile watermarking according to the method described in section 3.3.2 and together with the copyright watermarking sequence $D'\{D'_1, D'_2, ..., D'_{m \times m}\}$ to embed into the intermediate and high frequency coefficient of the DCT matrix of the next grouping. The method is shown as follows.

First, it is necessary to decide whether the copyright watermarking is embedded into the next ROI image grouping. There is no more than 1 bit embedded into the next ROI image grouping, but not each grouping needs the copyright watermarking, which can be determined by the value of $int\_L''_g$.

```
if (strcmp((int_L'_g(3:4)),'01')‖
(!strcmp((int_L'_g(3:4)),'01')&&
(!strcmp((int_L'_{g-1}(3:4)),'01'))))
insert_wking(blo_img(g), bit.A''_inf(g-1), D'(i));
g = g+1;      i = i+1;
else
insert_wking(blo_img(g), bit.A''_inf(g-1));
g = g+1;
end,
```

where value of $int\_L'_g$ is from the Equation (13), L'_g is the g-th value of sequence $L'\{L'_1, L'_2, ..., L'_i, ...\}$ and g is the integer, the function of *insert_wking*() is embedding the fragile watermarking and copyright watermarking (If there is not copyright watermarking $D'(i)$ in the parameters, 1 bit of copyright watermarking is not embedded into the image grouping.) into image grouping of ROI image, $blo\_img(g)$ is the g-th image grouping of ROI image, $bit.A''_{\inf}(g-1)$ is the $(g-1)$-th fragile watermarking described in section 3.3.2 and $D'(i)$ is i-th one-dimensional sequence $D'\{D'_1, D'_2, ..., D'_{m \times m}\}$.

$$int\_L'_g = dec2bin(\mathrm{mod}(((L'_g - \\ - round(L'_g)) * 10^{10}), 256)). \quad (13)$$

So, there is 4- or 5-bit watermarking (the 4 bits fragile watermarking and 0 or 1 bit copyright watermarking) in each block of ROI image.

Second, it is needed to decide the embedded position of the next image grouping of ROI image. According to the zigzag traversal method described in section 3.3.2, the embedding coefficient position is eleventh to thirty-sixth values, which is intermediate and high frequency coefficient in each image grouping. Selection method is adopted by Equation (14)

$$pos_i = (\mathrm{mod}(round(L'_{g+i} \times 10^{10}), 26) + 11), \quad (14)$$

where pos_i is a coefficient position of embedded watermarking according the zigzag traversal method and $i \le 5$.

Finally, according the value of watermarking and the embedded position, the watermarking is embedded into the image grouping.

6. Complete the IDCT transform in the image grouping, and the new ROI image, which has the copyright watermarking and the fragile watermarking is generated, is obtained.

Experiments and analysis. In order to check the effect of image copyright protection and tampering detection, some experiments have been done. The experimental platform is windows 7 and Matlab R2014a. The original image used in the experiment is shown in Fig. 3, *a* (Barbara, the size is 512 × 512) and the watermarking is shown in Fig. 3, *b* (the size is 32 × 32). The image copyright protection and tampering detection scheme is described in this paper.

a

b

c

Fig. 3. The original image:

a — the original image; b — the copyright watermarking; c — the ROI image

1. Experimental result.

The initial keys of memristor chaos are chosen randomly between –1 and 1, so the sequence $P\{P_1, P_2, ..., P_i, ...\}$ is obtained by function *ode*45() of runge-kutta method. In the experiment, the starting position of each sequence could be adjusted especially for the feature sequence $L(L_1, L_2, ..., L_i, ...)$, the sequence of the memristor $P\{P_1, P_2, ..., P_i, ...\}$ and sequence $L'\{L'_1, L'_2, ..., L'_i, ...\}$ which is generated by describing in section 3.2.

The original ROI image of Fig. 3, *a* is thought in the upper right corner, which is a triangle with length 256 px and height 256 px. So the new ROI image is a square 256 px long and high after the division of region, which is shown in Fig. 3, *c*. The PSNR of Fig. 3, *c* is 27.3620 according to the equations of PSNR as following

a

b

Fig. 4. The scrambling watermarking (a); the ROI image after embedding the watermarking (b)

a

b

Fig. 5. Sensitivity test:

a — the image after embedding the watermarking; b — the another ROI image after adding the watermarking

$$PSNR = 10 \times \log_{10}\left(\frac{(2^n - 1)^2}{MSE}\right); \quad (15)$$

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\|I(i,j) - K(i,j)\|^2. \quad (16)$$

The NROI image of Fig. 3, *a* was inputted into the deep learning algorithm, and the watermarking was changed into Fig. 4, *a* after the Arnold transform and matrix transform.

Finally, the new ROI image after embedding the copyright watermarking and the fragile watermarking is shown in Fig. 4, *b* (PSNR = 26.4157) and the entire new image is Fig. 5, *a*. Compared to the original image Fig. 3, *a*, the quality of Fig. 5, *a* has declined in the ROI image. But with the naked eye the effect of the entire image is almost of no influence.

1. Sensitivity testing.

In another experiment, parts of parameters are modified such as the position of watermarking, the other new ROI image after embedding the copyright watermarking and the fragile watermarking is shown in Fig. 5, *b* (PSNR = 26.9195). Compared to Fig. 3, *c,* Fig. 4, *b* and Fig. 5, *b*, the PSNR respectively are 27.3620, 26.4157and 26.9195. So the scheme will have different effects on the ROI image using different parameters for the watermarking.

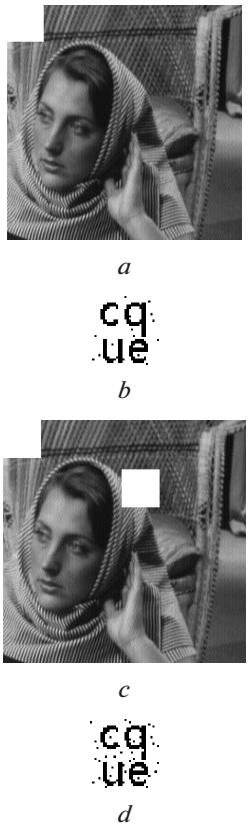

Fig. 6. Shear test:

a — shear ROI image; b — the recovering watermarking of (a); c — another shear ROI image; d — the recovering watermarking of (c)

2. Shear effect.

In order to check the effect of the watermarking, the copyright watermarking and fragile watermarking are tested separately. After the experiment of copyright watermarking extraction, it is confirmed that there is no difference between the original copyright watermarking and the extracted copyright watermarking in Fig. 4, *b* or Fig. 5, *b*. In another experiment, the recovery effect of copyright watermarking is also tested using the sheared ROI image after embedding the copyright watermarking, the effect of shear is shown in Fig. 6, *a* and Fig. 6, *c,* the recovery effects of copyright watermarking are respectively Fig. 6, *b* and Fig. 6, *d*. According to the experimental results, the shear has certain influence on extraction of copyright watermarking, but copyright information can still be identified. So the copyright watermarking in the scheme has strong robustness.

The fragile watermarking can also be detected according to the location where it is modified. And the modification part can be replaced with another mark. The effect of mark is consistent with the sheared part, so it gives unnecessary details no longer. It is worth mentioning that, if some value is modified in the ROI image grouping, the scheme will also mark itself entire grouping according to division of image grouping.

3. Key space analysis.

In the scheme, there are many steps to complete the algorithm, such as the generation of chaotic sequence, feature extraction, image division, generation and embedding of watermarking. In each step, there are one or more arguments or parameters and some of them have a large range. So, the scheme has huge key space and has high security.

Conclusions. A novel ROI image copyright protection and tampering detection scheme based on DCT and image feature has been obtained by deep learning and memristor chaos. The scheme could achieve satisfactory results in image copyright protection and detect whether an image is tampered illegally, and has the advantages of easy implementation, high security and high sensitivity. It is practicable and reliable to be applied to the application in copyright protection and tampering detection.

Acknowledgements. This work was supported by Scientific and Technological Research Program of Chongqing Municipal Education Commission (Grant No. KJ1501409, No. KJ1501405 and No. KJ1501412), Scientific Research Program of Chongqing University of Education (No. KY201520B and No. KY201522B), Natural Science Foundation of China (No. 61403050).

References/Список літератури

1. Umaamaheshvari, A. and Thanushkodi, K., 2014. Image Security Through Watermarking. *Journal of Medical Imaging and Health Informatic*, Vol. 4, No. 2, pp. 277–284.

2. Mettripun Narong, Amornraksa Thumrongrat and Delp Edward J., 2013. Robust image watermarking based on luminance modification. *Journal of Electronic Imaging*, Vol. 22, No. 3, pp. 1090–1098.

3. Masoodhu Banu, N. M. and Sujatha, S., 2015. Improved Tampering Detection for Image Authentication Based on Image Partitioning. *Wireless Personal Communications*, Vol. 84, No. 1, pp. 69–85.

4. Lyu Wan-Li, Chang Chin-Chen, and Chou Yeh-Chieh, 2015. Hybrid color image steganography method used for copyright protection and content authentication. *Journal of Information Hiding and Multimedia Signal Processing*, Vol. 6, No. 4, pp. 686–696.

5. Yu Hongyang, Yang Gongping, Wang Zhuoyi and Lin Zhang, 2015. A New Finger-Knuckle-Print ROI Extraction Method Based on Two-Stage Center Point Detection. *International Journal of Signal Processing, Image Processing and Pattern Recognition*, Vol. 8, No. 2, pp. 185–200.

6. Göpfert, F., Schmidt, R., Wulff, J. and Zink, K., 2015. Effect of ROI filtering in 3D cone-beam rotational angiography on organ dose and effective dose in cerebral investigations. *Journal of Applied Clinical Medical Physics*, Vol. 16, No. 2, pp. 229–249.

7. S Bu, Z Liu, J Han, et al., 2014. Learning High-Level Feature by Deep Belief Networks for 3-D Model Retrieval and Recognition», *IEEE Transactions on Multimedia*, Vol. 16, No. 8, pp. 2154–2167.

8. Yushi Chen, Xing Zhao and Xiuping Jia, 2015. Spectral-Spatial Classification of Hyperspectral Data Based on Deep Belief Network. *IEEE Journal of Se-*

lected Topics in Applied Earth Observations and Remote Sensing, Vol. 8, No. 6, pp. 1939–1404.
9. Rakkiyappan, R., Sivasamy, R. and Li Xiaodi, 2015. Synchronization of Identical and Nonidentical Memristor-based Chaotic Systems Via Active Backstepping Control Technique. *Circuits, Systems, and Signal Processing*, Vol. 34, No. 3, pp. 763–778.
10. Mo Chen, Mengyuan Li, Qing Yu, Bocheng Bao, Quan Xu and Jiang Wang, 2015. Dynamics of self-excited attractors and hidden attractors in generalized memristor-based Chua's circuit. *Nonlinear Dynamics*, Vol. 81, No. 1, pp. 215–226.

Мета. Для покращення результату захисту авторських прав на зображення та визначення, чи є зображення незаконно сфальсифіковано, ми пропонуємо відповідну схему виявлення ROI (області інтересу) зображення на основі послідовності ознак в NROI (не області інтересу) зображення. Ми оцінили цю схему за декількома критеріями, а результати підтвердили її ефективність.

Методика. Запропонована схема, що використовує для захисту авторських прав водяний знак і крихкий водяний знак. За допомогою глибинного навчання, мемристорного хаосу, перетворення Арнольда та розширеного зигзаг-перетворення, водяні знаки генеруються й вбудовуються в область інтересу зображення у DCT (дискретне косинус-перетворення) домен з використанням послідовності особливостей області зображення, що не цікавить.

Результати. Спочатку здійснюємо розділення ROI та NROI зображення й отримуємо послідовність ознак NROI зображення, використовуючи глибинне навчання та мемристорний хаос. Потім за допомогою послідовності й деяких методів, таких як перетворення Арнольда, ми отримуємо скрембльовані водяні знаки захисту авторського права та нові крихкі водяні знаки кожної групи зображень і впроваджуємо їх у ROI зображення.

Наукова новизна. Запропоноване витягання послідовності ознак зображень у NROI зображення, використовуючи глибинне навчання та мемристорний хаос. Він застосовується для генерації та впровадження скрембльованих водяних знаків захисту авторського права та нових крихких водяних знаків у ROI зображення.

Практична значимість. Проведені експерименти з перевіркою показників ефективності показують, що потреба безпечної передачі може бути повністю задоволена. Ця схема має високу надійність і безпеку.

Ключові слова: *ознака зображення, захист зображень, виявлення фальсифікації, авторське право, мемристор, глибинне навчання*

Цель. Для улучшения результата защиты авторских прав на изображение и определения, является ли изображение незаконно фальсифицировано, мы предлагаем соответствующую схему обнаружения ROI (области интереса) изображения на основе последовательности признаков в NROI (не области интереса) изображения. Мы оценили эту схему по нескольким критериям, и результаты подтвердили её эффективность.

Методика. Предложена схема, использующая для защиты авторских прав водяной знак и хрупкий водяной знак. С помощью глубинного обучения, мемристорного хаоса, преобразования Арнольда и расширенного зигзаг-преобразования, водяные знаки генерируются и встраиваются в область интереса изображения в DCT (дискретное косинус-преобразование) домен с использованием последовательности особенностей не интересующей области изображения.

Результаты. Сначала осуществляем разделение ROI и NROI изображения и получаем последовательность признаков NROI изображения, используя глубинное обучение и мемристорный хаос. Затем с помощью последовательности и некоторых методов, таких как преобразование Арнольда, мы получаем скремблированные водяные знаки защиты авторского права и новые хрупкие водяные знаки каждой группы изображений и внедряем их в ROI изображения.

Научная новизна. Предложено извлечение последовательности признаков изображений в NROI изображения, используя глубинное обучение и мемристорный хаос. Он применяется для генерации и внедрения скремблированных водяных знаков защиты авторского права и новых хрупких водяных знаков в ROI изображения.

Практическая значимость. Проведенные эксперименты с проверкой показателей эффективности показывают, что потребность безопасной передачи может быть полностью удовлетворена. Эта схема обладает высокой надежностью и безопасностью.

Ключевые слова: *признак изображения, защита изображений, обнаружение фальсификации, авторское право, мемристор, глубинное обучение*

Рекомендовано до публікації докт. техн. наук В. В. Гнатушенком. Дата надходження рукопису 12.10.15.