New Image Watermarking Algorithm Based on DWT and Pixel Movement Function PMF

Razika Souadék and Naceur-Eddine Boukezzoula
Department of Electronic, University of Setif 1, Republic Algeria

Abstract: In this paper, we propose a new algorithm of image watermarking based on Discrete Wavelet Transform (DWT) including a function for pixels movement. The proposed algorithm uses DWT of two levels in order to compact a higher energy in component LL1, and Contrast Sensitivity Function (CSF) to improve the invisibility and robustness, the new Function of Pixel Movement (PMF) is applied to increase the security properties. Pixel Movement Function (PMF) is a function of N iteration inside each block, this function required a changeable key K calculated in each iteration N for the position of each block. Numerical experiments are performed to demonstrate that the proposed method can improve watermarking quality in terms of imperceptibility of watermark, capacity of insertion and robustness against different attacks such as Joint Photographic Experts Group (JPEG) compression, noise addition and geometrical attacks.

Keywords: Wavelet transforms, image watermarking, image quality evaluation.

Received June 8, 2016; accepted May 7, 2018
https://doi.org/10.34028/iajit/17/1/1

1. Introduction
The huge evolution in field of electronics and data processing is accompanied by an hugely development in multimedia communication like video broadcasting, network and High Definition image (HD) image. The communications between people become in real time, and they can exchange multimedia produces easily in very short time, this is wonderful. However, this evolution brings a series of problems such as confidentiality and authors copyright in scientific area. Therefore, for security constrains and for rights of the authors protected, Researchers have created several techniques in different field to secure the information, among these techniques, the watermarking finds place.

In standard technique, the watermarking image is referring to the addition of a fixed number of pixels to the original image pixels, these pixels constitute the watermark image, the resulting image is the watermarked image [6, 5, 14, 22]. However, in the extraction process, watermark can be detected via the original and watermarked image with protection of this last.

The main objective of watermarking image is to secure the cover image through the watermark, and so yield to undetectable and non erasable via intentional or unintentional attacks [5].

Researchers define two domains of watermarking includes the insertion operation; a spatial domain is based on embedding in the pixels of cover image after changed the intensity and colour value, for example insertion in the Last Significant Bit (LSB) of image to acquire a good visual quality. However, this technique not robust against various attacks as noising, filtering and geometrical because after attacks the LSB turns over to zero according to [17].

An insertion in the frequency domain has given a very robust watermarking scheme against most attacks, because it uses various reversible transforms like the Discrete Cosine Transform (DCT) [10, 19, 21], Discrete Wavelet Transform (DWT) [4, 9, 16] and Discrete Fourier Transform (DFT) [13]. In this process, after calculating the transformation coefficients, the watermark is embed in weak weight coefficients the inverse transformation is required to obtain the watermarked image [18]. Additionally, the mathematics technique such as Singular Value Decomposition (SVD) is well known in watermarking image, for the advantage of invisibility and robustness of system against various attacks [8].

Lately, the researchers have combined the two transforms in one algorithm named a hybrid system like DCT-DWT [1], DWT-SVD [2, 7, 15] and DCT-SVD [3]; the hybrid system has added more security, robustness and invisibility.

In [12] the authors have proposed an algorithm of watermarking image based on Partial Pivoting Lower and Upper triangular (PPLU) decomposition and Differential Evolution (DE) using DWT transforms. The PPLU concerns only the low and the upper triangular matrix of watermark image, a permutation matrix $P_w$ it used as secret key. The SVD technique is involved to calculate $\Delta_w$ which present the multiplication of $U_w$ and $S_w$ and conserving the $V_w$ for the ownership, the $\Delta_w$ is add to the singular values of components $LL$ and $HH$ in order to obtain $S_w$ respectively, then also obtain the watermarked
This method is robust against multiple attacks such as geometric, filtering and noising. Note that, two watermark images embedding have raised the system robustness. The proposed method in [20] has confirmed the robustness by embedding two watermark images in different blocks, and has preserved the visual quality of watermarked image by using the Slant Let Transform matrix (SLT) before embedding the watermark.

In this paper, we present a watermarking algorithm based on pixels movement function applying before watermark insertion, the principle of this method is to change the site of the pixels of the original image blocks for ensuring security, so hackers can’t extract the watermark. Moreover, the addition of the transfer function, a modified Contrast Sensitivity Function to evaluate image degradation quality after watermark embedding allows reinforcing the algorithm against various attacks.

This paper is organized in five sections. After introducing the problem, we present the transform and tools in section two, watermarking algorithm is detailed in section three. Results and discussion are given in section four, and finished by a conclusion and perspective.

2. Transforms Domains and Tools
2.1. Discrete Wavelet Transform
Most researchers prefer to use the discrete wavelet transform for their positive influence of image quality and for many interesting proprieties. The DWT uses filter bank to decompose the input image into four sub-bands; LL, HL, LH, and The LL sub-band results from low-pass filtering of the time domain, it contains the major cover image information. Whereas, the HHSub-band component is the result of high pass filtering of the time domain, it contains the high frequency along diagonals. The HL and LH of image are the results of low pass filtering and high pass filtering vertical or horizontal in one direction, this last two sub-bands are demonstrated the details of the image [2] (Figure 1). We can apply the DWT for many times to multiple levels for the same image to get more exploitation of frequency characteristics of image.

The vertical shift of odd columns (Figure 2) is determined by the Equation (1).

\[ y_{i+1}(i, j) = y_{i}(i - 1, j) \]  

(1)

Where \( j=1, 2, \ldots, n \) and \( j \) are the odd number from 1 to \( n \).

The left shift of the odd lines (Figure 3) is determined by the Equation (2).

\[ x_{i+1}(i, j) = x_{i}(i, j - 1) \]  

(2)

Where \( j=1, 2, \ldots, n \) and \( i \) are the odd number from 1 to \( n \).

2.2. Pixel Movement Function PMF
The Pixels Movement Function (PMF) is implemented by shifting one pixel in both; odd columns and odd lines of the matrix for each \( N \) iteration.

2.3. Inverse Pixel Movement Function IPMF
This step define the operation to get back to the initial state used the opposite shifting on the odd lines and columns as shown in Equations (3) and (4).

\[ \tilde{x}_{i+1}(i, j) = x_{i+1}(i, j + 1) \]  

(3)

Where \( j=1, 2, \ldots, n \) and \( i \) are the odd number from 1 to \( n \).

\[ \tilde{y}_{i+1}(i, j) = y_{i+1}(i + 1, j) \]  

(4)

Where \( i=1, 2, \ldots, n \) and \( j \) are the odd number from 1 to \( n \).

2.4. Transfer Function TF
The Transfer Function (TF) is derived from Contrast Sensitivity Function of the Human Visual System (HVS) [11]. The transfer function is applying the sub-band LL1 as it given in Equation (5), the linear exponential decreases the values of the pixels in LL1 components, for this reason the extracted watermark not really affected by different attacks, so we can get better results for the watermarking. The transfer function is determined by the Equation (5).

\[ H = TF(LL1) = a(b + c \times LL1)e^{-\|c\|_p} \]  

(5)

Where \( a, b, c \) are randomly selected real numbers.

[Figure 1. The discrete wavelet transform (DWT).]

[Figure 2. Vertical shift of one pixel for \( j=1 \).]

[Figure 3. Left shift of one pixel for \( i=1 \).]
Where \( fe \) is a positive randomly selected real number.

Histograms in the Figure 4 demonstrate that before and after applying of the TF, pixels values have been reduced by three-quarter. In part (a) before applying the transfer function denote the pixel values converge to 900 and with transfer function the pixel values reduce to 250 shown in (b). To protect the information and augment the robustness against attacks.

3. Proposed Algorithm

The proposed Algorithm in this paper is characterized by embedding watermark in the LL1 sub-band after applied the TF and passed by our new function PMF. The diagram in Figures 5 and 6 are explaining step by step the insertion and extraction algorithms. To evaluate the performance of our algorithm we have to test it in terms of Peak Signal to Noise Ratio (PSNR) given in Equation 6 and by a factor of similarity Normalized Correlation (NC) Equation (7).

\[
PSNR = 10 \log_{10} \left( \frac{I_{\max}^2}{\frac{1}{(m \times n)} \sum_{i,j} (I(i,j) - \hat{I}(i,j))^2} \right) \tag{6}
\]

\[
NC = \frac{\sum \sum w(i,j) \hat{w}(i,j)}{\sqrt{\sum \sum w(i,j)^2} \sqrt{\sum \sum \hat{w}(i,j)^2}} \tag{7}
\]

Where \( I, \hat{I} \) are the original image test and the watermarked image respectively, and \( w, \hat{w} \) are the original watermark and the extracted watermark respectively.

3.1. Embedding Process

The different steps of the developed watermarking algorithm are explained below:

- Get the original image \( I \) of size 512×512 pixels, the discrete wavelet transform of two levels is applying for image test to get \( \{LL1, HL1, LH1, HH1, HL, LH, HH\} \), the sub-band \( LL1 \) is chosen for embedding the watermark, then apply the transfer function TF to the \( LL1 \) sub-band as follows: \( H = TF(LL1) \), after this step the mark is embedding according to the following method:

- Divide the component \( H \) to a sub-blocks \( B_H \) of size 8×8 pixels, then insert the watermark image \( w \) of size 72×70 pixels with split to sub-blocks \( B_w \), where each one contains 20 pixels.
- Calculate and arrange the averages of each sub-block \( B_w \) in a vector named \( M \).
- Convert the decimals numbers into binary numbers in the averages vector \( M \).
- Count the bits equal to 1 in each binary number and select the bit 1 beside the MSB bit.
- The emplacement of this bit 1determine a number of iteration \( N \).
• Make the movement of pixels by PMF of sub-blocks $B_H$ for $N$ iteration (each block has $N$ iteration different to the others), then embed the watermark image in the primary position of each block of component $H$ by a key $k$; the key $k$ is calculated as it given in Equation (8).

$$k = \sqrt{NB_{emb} + N}$$ \hspace{1cm} (8)

$NB_{emb}$: it is the position of sub-block $B_H$.

• For each sub-block $B_H$, the watermark is inserted as follows:

$$\overline{B}_{Hw} = PMF_N(B_H) + k \times B_w$$ \hspace{1cm} (9)

• After watermark insertion, the inverse pixels movement function is applied for each sub-block of each $\overline{B}_{Hw}$.

$$B_{Hw} = IPMF_N(\overline{B}_{Hw})$$ \hspace{1cm} (10)

• Rebuild the sub-blocks $B_{Hw}$ to restore the initial state of pixels in order to obtain the watermarked component $H_w$, then apply the inverse transfer function to $H_w$ as follows:

$$LL1_w = ITF(H_w)$$ \hspace{1cm} (11)

Finally, apply the inverse discrete wavelet transform of two level on the components $\{LL1_w, HL1, LH1, HH1, HL, LH, HH\}$ to find the watermarked image $I_w$.

3.2. Extraction Process

The extraction process of the watermark is defined in following step:

Firstly, get the test image $I$ of size 512×512 pixels, and the watermarked image $I_w$ of size 512×512 pixels.

• Apply the discrete wavelet transform of two (level) to the original and the watermarked image to obtain $\{LL1, HL1, LH1, HH1, HL, LH, HH\}$ and $\{LL1_w, HL1, LH1, HH1, HL, LH, HH\}$ respectively.

• Choose the components LL1 and LL1w for extracting the watermark.

• Apply the transfer function $TF$ to the LL1 and LL1w to get $H=TF(LL1)$ and $H_w=TF(LL1w)$.

• Make the movements of the sub-block $\hat{B}_H$ of component $\hat{H}$ and sub-block $\hat{B}_{Hw}$ of component $\hat{H}_w$ for $N$ iteration, by the pixels movement function $PMF$.

• Extract the watermark into the primary emplacement of each sub-blocks of the component $\hat{H}_w$ by a key $k$ as it given in Equation (12);

$$B_{wv} = \frac{PMF_N(\hat{B}_{Hw}) - PMF_N(\hat{B}_H)}{k}$$ \hspace{1cm} (12)

Rebuild the sub-blocks $B_{wv}$ to obtain the extracted watermark image.

4. Results and Discussion

The developed watermarking algorithm presented in this work is implemented in Matlab. We have calculated the qualities parameters of the algorithm as: peak signal to noise ratio and normalized correlation. The image selected for this work are the image Lena of size 512×512 pixels and the image Airplane of size 512×512 pixels as tests image, and the image of copyright size 72×70 pixels as watermark image (Figure 7).

Figure 7. The performance of the proposed algorithm.

Figure 8 present the histograms of originals and watermarked images of Lena and Airplane images, it’s showed clearly the difference between histograms in certain bands. In the bands from 200 to 220 pixels of Lena and Airplane for original and watermarked images, histograms present a noticeable change in pixels values. Using transfer function reduces noise in high frequency, which raises the watermarked image quality.

In case of the intentional attacks, the algorithm is testing where the key $k$ has a fixed value ($k=0.1$) for different iteration ($N=3$, $N=10$), the results are illustrated in Figure 9:

In Figure 8 we can see clearly the change in the histograms by using the transfer function.

Figure 9. The effect of the key and iteration $N$ on extracted watermark.
Number of iteration $N$ and the key $k$ have an important influence on the visual quality of the extracted watermark and in security proprieties too; without the key $k$ and the number of iteration $N$ which are secret ($N$ and $k$ attached to the watermark inserted) you can’t extract the watermark, when you don’t have the watermark, you can’t examine the key $k$ and the iteration $N$ in other side.

The attacks have erased the watermark completely so that has obliged to test the algorithm against the unintentional attacks. Hence, we signed to the watermarked images Lena and Airplane by (WIL) and (WIA), and for Extracted watermark by EW, the expression of attacks as follows:

To ensure the robustness against noising attacks, the algorithm is tested against Salt and Pepper noise with 0.001(SP) and Gaussian noise with 0.001 Gaussian Noise (GN). The examination against filtering attacks contain Median filter of 3x3 Median Filter (MF), Average filter of 3x3 Average Filter (AF), Sharpening Filter (SH), and Gaussian filter of 3x3 Gaussian Filter (GF). Next, the system has inspected for geometrical attacks such as rescaling 512 to 256 to 512 Rescaling of image (RS), in the end, we apply the attack of Joint Photographic Experts Group (JPEG) compression with 50%.

Subsequently, the Figure 10 present two images of tests Lena and Airplane with the different unintentional attacks, results notice a good quality of visibility of the extracted watermark with similarity factor approaches to 1 ($0.9000 \leq NC \leq 0.9999$).

The Figure 11 represents the values of Normalized Correlation between the extracted watermark image and original watermark image related to the coefficient of JPEG compression. Results demonstrate the good quality of extraction watermark.

The following figures present the values of normalized correlation in function of; percentage of Salt and Pepper noise (Figure 12), the dimension of Gaussian filter (Figure 13), as noticeable this algorithm is robust against major attacks.

The following table (Table 1) recapitulates the effect of the attacks for different degrees (degree of attacks) and their corresponding values of normalized correlation and peak signal to noise ratio for the extracted watermark. These results are used to confirm the robustness and perceive of our algorithm.

Compared to other algorithms, we note in the Figure 14 that the algorithm provided proved robustness against various attacks.
A new watermarking method has been presented in this paper, it based on pixel movement in each image test sub-blocks for ensuring the security. The watermark is embedding after pixels movement into sub-block for many iteration N, this last is derived from the average of watermark image sub-blocks, it uses to calculate the key k and it sub-block position. In terms of security, it would be impossible to detect the watermark without knowing the number of iteration N and the key k. The watermarking algorithm has provided 42.77 dB PSNR for Lena image it has given 0.9997 normalized correlation and 42.77 dB PSNR for Airplane image it has given 0.9998 normalized correlation. Intentional and unintentional attacks have demonstrated the robustness of our system, we have showed that note after different attacks our algorithm has resisted, it presented a NC higher than 0.9. This algorithm can also be applied to color images. As perspective, a Digital Signal Processor (DSP) implementation of our watermarking method is necessary to proof the precision and rapidity of system in real time.

**5. Conclusions**

Figure 14. NC values of comparison between algorithms to various attacks for lena and airplane images.

Table 1. NC and PSNR values after the various attacks for the images lena, airplane, pepper and sailboat.

| Attacks | Lena image | Airplane image | Pepper image | Sailboat image |
|---------|------------|----------------|--------------|----------------|
|         | NC  | PSNR | NC  | PSNR | NC  | PSNR | NC  | PSNR |
| SP   | 0.1% | 0.9953 | 40.70 | 0.9959 | 40.58 | 0.9956 | 40.62 | 0.9965 | 40.60 |
|      | 0.2% | 0.9905 | 39.70 | 0.9920 | 39.61 | 0.9928 | 39.80 | 0.9934 | 39.67 |
|      | 0.3% | 0.9866 | 38.89 | 0.9882 | 38.79 | 0.9900 | 39.06 | 0.9907 | 38.80 |
| GN   | 0.1% | 0.9797 | 38.68 | 0.9794 | 38.70 | 0.9781 | 38.71 | 0.9786 | 38.70 |
|      | 0.2% | 0.9702 | 37.38 | 0.9610 | 37.36 | 0.9583 | 37.38 | 0.9582 | 37.38 |
|      | 0.3% | 0.9446 | 36.54 | 0.9477 | 36.57 | 0.9410 | 36.57 | 0.9360 | 36.57 |
| MF   | 3x3  | 0.9846 | 41.19 | 0.9824 | 40.64 | 0.9858 | 41.57 | 0.9544 | 39.45 |
|      | 5x5  | 0.9320 | 39.55 | 0.9300 | 38.66 | 0.9294 | 40.34 | 0.8585 | 37.57 |
|      | 7x7  | 0.8504 | 38.53 | 0.8382 | 37.44 | 0.8269 | 39.38 | 0.7492 | 36.49 |
| AF   | 3x3  | 0.9729 | 40.71 | 0.9692 | 39.69 | 0.9726 | 40.29 | 0.9457 | 38.99 |
|      | 5x5  | 0.8994 | 38.85 | 0.8925 | 37.73 | 0.8880 | 38.75 | 0.8259 | 37.12 |
|      | 7x7  | 0.8245 | 37.83 | 0.8213 | 36.66 | 0.7806 | 37.79 | 0.7396 | 36.11 |
| SF   | 0.9  | 0.9703 | 35.86 | 0.9600 | 35.55 | 0.9750 | 36.44 | 0.9507 | 34.86 |
| GF   | 3x3  | 0.9811 | 41.22 | 0.9785 | 40.32 | 0.9817 | 40.86 | 0.9631 | 39.63 |
|      | 5x5  | 0.9640 | 40.55 | 0.9587 | 39.59 | 0.9627 | 40.33 | 0.9275 | 38.91 |
|      | 7x7  | 0.9611 | 40.48 | 0.9556 | 39.52 | 0.9595 | 40.28 | 0.9223 | 38.85 |
| RS   | To 256| 0.9919 | 40.72 | 0.9895 | 39.57 | 0.9916 | 39.95 | 0.9841 | 38.90 |
| JPE  | 30%  | 0.9819 | 40.72 | 0.9829 | 40.56 | 0.9791 | 40.34 | 0.9973 | 39.69 |
| G C  | 60%  | 0.9934 | 42.00 | 0.9913 | 41.93 | 0.9937 | 41.97 | 0.9938 | 41.39 |
|      | 90%  | 0.9988 | 42.71 | 0.9988 | 42.70 | 0.9988 | 42.71 | 0.9988 | 42.65 |
| Without attack | 0.9995 | 42.77 | 0.9995 | 42.77 | 0.9995 | 42.77 | 0.9995 | 42.77 |

**Reference**

[1] Al-Haj A., “Combined DWT-DCT Digital Image Watermarking,” *Journal of Computer Science*, vol. 3, no. 9, pp. 740-746, 2007.

[2] Ali M., Ahn C., and Pant M., “An Optimized Watermarking Technique Based on DE in DWT-SVD Domain,” in *Proceedings of IEEE Symposium on Differential Evolution*, Singapore, pp. 99-104, 2013.

[3] Ali M., Ahn C., and Pant M., “A Robust Image Watermarking Technique Using SVD and Differential Evolution In DCT Domain,” *Optik*, vol. 125, pp. 428-434, 2014.

[4] Dawei Z., Guanrong C., and Wenbo L., “A Chaos-Based Robust Wavelet-Domain Watermarking Algorithm,” *Chaos, Solitons and Fractals*, vol. 22, no. 1, pp. 47-54, 2004.

[5] Hernández J. and Pérez-González F., “Performance Analysis of a 2-D-Multipulse Amplitude Modulation Scheme for Data Hiding and Watermarking of Still Images,” *IEEE*
New Image Watermarking Algorithm Based on DWT and Pixel Movement Function PMF

Journal on Selected Areas in Communications, vol. 16, no. 4, pp. 510-524, 1998.

[6] Hussein J., “Spatial Domain Watermarking Scheme for Colored Images Based on Log-Average Luminance,” Journal of Computing, January, vol. 2, no. 1, pp. 100-103, 2010.

[7] Imran M., Ghafoor A., and Riaz M., “Adaptive Watermarking Technique Based on Human Visual System and Fuzzy Inference System,” in Proceedings of IEEE International Symposium on Circuits and Systems, Beijing, pp. 2816-2819, 2013.

[8] Li G. and Wang Y., “A Privacy-Preserving Classification Method Based on Singular Value Decomposition,” The International Arab Journal of Information Technology, vol. 9, no. 6, pp. 529-534, 2012.

[9] Li N., Zheng X., Zhao Y., Wu H., and Li S., “Robust Algorithm of Digital Image Watermarking Based on Discrete Wavelet Transform,” in Proceedings of International Symposium on Electronic Commerce and Security, Guangzhou City, pp. 942-945, 2008.

[10] Lin S., Shie S., and Guo J., “Improving the Robustness of DCT-based Image Watermarking Against JPEG Compression,” Computer Standards and Interfaces, vol. 32, no. 1-2, pp. 54-60, 2010.

[11] Mannos J. and Sakrison D., “The Effects of A Visual Fidelity Criterion on The Encoding of Images,” IEEE Transactions on Information Theory, vol. 20, no. 4, pp. 525-536, 1974.

[12] Muhammad N. and Bibi N., “Digital Image Watermarking Using Partial Pivoting Lower and Upper Triangular Decomposition into The Wavelet Domain,” IET Image Processing, vol. 9, no. 9, pp. 795-803, 2015.

[13] Qi X. and Qi J., “A Robust Content-Based Digital Image Watermarking Scheme,” Signal Processing, vol. 87, no. 6, pp. 1264-1280, 2007.

[14] Radharan S. and Valarmathi M., “A Study on Watermarking Schemes for Image Authentication,” International Journal of Computer Applications, vol. 2, no. 4, pp. 24-32, 2010.

[15] Rani A., Bhullar K., Dangwal D., and Kumar S., “A Zero-Watermarking Scheme using Discrete Wavelet Transform,” Procedia Computer Science, vol. 70, pp. 603-609, 2015.

[16] Reddy A. and Chatterji B., “A New Wavelet Based Logo-Watermarking Scheme,” Pattern Recognition Letters, vol. 26, pp. 1019-1027, 2005.

[17] Reddy P., Prasad M., and Rao D., “Robust Digital Watermarking of Images using Wavelets,” International Journal of Computer and Electrical Engineering, vol. 1, no. 2, pp. 111-116, 2009.

[18] Seddik H. and Gupta M., Watermarking, IntechOpen, 2012.

[19] Tewari T. and Saxena V., “An Improved and Robust DCT based Digital Image Watermarking Scheme,” International Journal of Computer Applications, vol. 3, no. 1, pp. 28-32, 2010.

[20] Thabit R. and Khoo B., “Capacity Improved Robust Lossless Image Watermarking,” IET Image Processing, vol. 8, no. 11, pp. 662-670, 2014.

[21] Xu Z., Wang Z., and Lu Q., “Research on Image Watermarking Algorithm based on DCT,” Procedia Environmental Sciences, vol. 10, pp. 1129-1135, 2011.

[22] Ye J. and Tan G., “An Improved Digital Watermarking Algorithm for Meaningful Image,” in Proceedings of International Conference on Computer Science and Software Engineering, Hubei, pp. 822-825, 2008.

Razika Souadek obtained licence degree in instramentation electronic, a master's degree in electronics embedded system and a PhD student in embedded system technology from Setif University Electronic Department. she teachers in university of setif in Sociology department to two years. Her principal researches are about image processing (Watermarking image). A member of scientific instrumentation Laboratory.

Naceur-Eddine Boukezzoula has got the Engineering degree in 1980 from University of Oran USTO (Algeria) in Electronics in 1980, then a magister degree in communication from Setif University (Algeria) in 1989, and a PHD degree from Setif University in 2006. He teachers in university of setif at Electronics Department since 1980. He is a member of the scientific institution of the faculty of Technology. His principal researches are about Neural Networks, image processing (Watermarking and Biometrics).