Computing and Informatics, Vol. 42, 2023, 591–614, doi: 10.31577/cai_2023_3_591

STEGANOGRAPHY APPROACH TO IMAGE AUTHENTICATION USING PULSE COUPLED NEURAL NETWORK

Radoslav Forgáč, Miloš Očkay

Institute of Informatics
Slovak Academy of Sciences
Dúbravská cesta 9
845 07 Bratislava, Slovakia
e-mail: {radoslav.forgac, milos.ockay}@savba.sk

Martin Javurek, Bianca Badidová

Department of Informatics
Armed Forces Academy of gen. M. R. Štefánik
Demänová 393
031 01 Liptovský Mikuláš, Slovakia
e-mail: {martin.javurek, bianca.badidova}@aos.sk

Abstract. This paper introduces a model for the authentication of large-scale images. The crucial element of the proposed model is the optimized Pulse Coupled Neural Network. This neural network generates position matrices based on which the embedding of authentication data into cover images is applied. Emphasis is placed on the minimalization of the stego image entropy change. Stego image entropy is consequently compared with the reference entropy of the cover image. The security of the suggested solution is granted by the neural network weights initialized with a steganographic key and by the encryption of accompanying steganographic data using the AES-256 algorithm. The integrity of the images is verified through the SHA-256 hash function. The integration of the accompanying and authentication data directly into the stego image and the authentication of the large images are the main contributions of the work.

Keywords: Image steganography, pulse coupled neural network, position matrix, image authentication

1 INTRODUCTION

Digital images are predominantly processed and transmitted in environments that allow for their modification. There is a growing need to develop procedures and methods that allow the integrity and authenticity of the image to be verified. Current examples mainly include industry, healthcare, military and many others. Image processing is greatly simplified by high-performance computing and specialized systems. Image modification is sophisticated and is used for a variety of purposes. An example is the misuse of artificial intelligence (AI) to generate fake images to commit fraud. Images generated by AI are so convincing that they can be difficult to distinguish from real images. The negative impacts of such manipulations might have far-reaching consequences on individuals or society. Copyright infringement or influencing public opinion can be mentioned, just to list a few examples. One of the possible solutions for authenticating images is to use steganographic methods. The term 'steganography' is derived from the Greek words 'steganos' (meaning hidden or concealed) and 'graphein' (meaning writing). Steganography proposes methods of data transmission using a carrier medium (cover media). The data transmission is implemented in such a way that it is not suspected that the information not directly related to the medium is being transmitted within the carrier medium. Suitable carrier media may be, for example, text, image, sound, video, etc. Analogously, any type of digital content, such as text, image, sound, video or binary code can be hidden using steganography. In order to extract the hidden information, the other party needs to know the steganographic method used to embed the message. It also concerns the accompanying data which are the parameters of the method used. Similar to cryptography, it is considered that the method for the embedding and extraction of the hidden message should be publicly available in order to verify the security of the method. The assurance of the untraceability of the hidden message in the cover medium should be a steganographic key, so-called stego key. Only knowledge of the stego key should lead to a successful extraction of the hidden content. Encryption is very often used to maximize the security of hidden content. In case of breaking the steganographic method, encryption is thus the final protection against the content being compromised.

This paper presents a steganographic method using position matrix generation by the Optimized Model of Pulse Coupled Neural Network (OM-PCNN). The position matrix can be considered as a prescription or template for embedding the hidden content into the carrier image. Due to the best setting of the position matrix, positions with high entropy are identified in the cover image. This is a prerequisite to eliminate the risk of detecting the positions of the hidden data in the cover image by the visual inspection. The security of the presented steganographic method is based on the secret stego key, the openness of the embedding algorithm and the extraction of the hidden message without the need to transmit the accompanying steganographic data by independent channel.

The rest of this paper is structured as follows. The second part describes related work on image authentication and steganography. In the third part, the theoretical background of the proposed model is described. The fourth part describes and evaluates the proposed authenticity verification model. The final part concludes the paper.

2 RELATED WORK

In recent years, there has been a rapid growth of research in the area of image data authentication [1, 2, 3]. There are two basic approaches for authentication: encryption-based approaches, i.e., cryptography and steganography-based approaches.

Another aspect of image authentication is the level of image modification. The first group consists of strict authentication methods which evaluate any image modification as inadmissible. Methods based on standard cryptography have been applied in this group [4]. Fragile watermarking-based methods have also been applied in this group, such as the method proposed based on the Frei-Chen edge mask [5], which provides excellent image quality with watermarking and clearly reveals tampered regions. Another example of a fragile watermarking-based method is a method combining discrete wavelet transform (DWT), singular value decomposition (SVD) and discrete cosine transform (DCT) [6]. The results showed that the method achieved high detection accuracy for various forms of modifications while maintaining high visual quality. The second group consists of selective authentication methods which tolerate selected operations on images, such as compression, various filtering algorithms, or the application of geometric transformations to images. Within the second group, semi-fragile watermarking methods have been applied, such as the Inner-Outer Block-Based method [7] which splits the image into an inner and an outer part. This division has the purpose of copyright protection in addition to authentication. The method has increased robustness to compression and common image operations such as gamma corrections, intensity adjustments and histogram equalization. Other methods for selective authentication include those using robust watermarking [8].

2.1 Cryptography-Based Image Authentication

Hashing functions are a key element of image authentication. A method to authenticate images using hashes with Multi-Attack Reference Generation and Adaptive Thresholding was proposed by [9]. The proposed method is based on clustering. A perceptual hashing algorithm was applied to the reference image to obtain the hash codes required for authentication. Adaptive thresholding was taken to account for variations in the hashing distance. The method showed a high performance but was rather time-consuming.

Tamper detection and localization in the images are still a subject of research. An approach was proposed by [10] in which the authors used hashes in combination

with fragile watermarks to authenticate and localize the tamper. In the presented approach, the original cover image is divided into non-overlapping blocks on which a DCT is performed. This operation extracts the coefficients to which the SHA-256 hash function is subsequently applied. After the hash is obtained, the original cover image is split into blocks by the Arnold transform using a key. A 16-bit hash is inserted into each block to obtain the watermarked image. The embedded hash function helps with tamper detection and image localization. The proposed approach was compared with several existing approaches, resulting in an improvement in peak signal-to-noise ratio (PSNR). Another study [11] also addressed image data authentication using hash functions, but the authors chose a neural network-based approach. A convolutional stacked denoising autoencoder was used for both authentication and tamper localization. The proposed autoencoder maps high-dimensional input data to hash codes. Then, the tamper localization is performed by comparing the decoder output of the tampered image with the hash of the real image. The authors used the F1-score metric and receiver operating characteristic (ROC) for evaluation. Results show better performance compared to other existing approaches.

Hashing as a stand-alone authentication tool is insufficient. Its primary function is to verify data integrity, i.e., that the data has not been modified in any way. Digital signatures [12, 13, 14] and Keyed-Hash Message Authentication Code [15, 16] are most commonly used to authenticate images.

Digital signature-based authentication has been addressed by [17] who proposed a novel image secret sharing (ISS) scheme. They introduced a two-way shadow image authentication method based on public key. The shadow image can be authenticated with the distributor's secret key in addition to the participants' private key. The proposed ISS scheme can decode secret images losslessly with bidirectional shadow image authentication without pixel expansion. The study in [18] proposed an asymmetric two-level phase generation image encryption scheme that uses a nonlinear decryption key generation process. The nonlinear encryption process provides a high level of resistance to the existing attacks. The use of a digital signature verifies the identity of the sender and no information is revealed without the use of the correct keys. An image encryption algorithm that hides a secret image and a digital signature that provides authenticity and confidentiality was proposed in [19]. The solution uses the Least Significant Bit (LSB) method to embed the digital signature and the Lifting Wavelet Transform (LWT) method to generate a meaningful encrypted image. Experimental results show that the proposed scheme has high key sensitivity. Based on the histogram analysis, it is found that the original carrier image and the final visual image are very similar.

Hash-based message authentication code (HMAC) was addressed in [20], in which the authors focused on the authentication of images from the healthcare domain. They proposed an optical algorithm that ensures the efficiency and security of medical image transmission. The proposed algorithm accomplished authentication and integrity by computing and verifying HMAC values. At the same time, confidentiality of medical images was achieved by using Rubik's cube encryption. The

effectiveness of the proposed algorithm has been thoroughly evaluated using various visual, qualitative, statistical and complex metrics. The security was evaluated by examining the key sensitivity and the robustness of the algorithm to different types of noise and attacks. Authentication using HMAC was also addressed by [21]. Their algorithm uses DCT combined with LSB. To verify the origin of the message, the HMAC of the transformed image is also embedded in the cover image. The proposed algorithm can identify data changes in the transmission channel but does not deal with the reconstruction of clipped or noisy images.

2.2 Authentication of Images Based on Data Hiding

Data hiding image authentication methods are based on digital steganography [22, 23, 24] or digital watermarking [25, 26, 27]. Currently, research in both sub-areas is also exploring the use of neural networks [28, 29, 30].

Digital watermarks are an ideal tool for verifying copyrighted images. A study in [31] proposes a blind dual watermarking scheme where the embedding of an invisible, robust watermark serves to protect the copyright and the embedding of a fragile watermark authenticates the image. The method in [32] focused on the use of blockchain to address the problem of trusted third parties protecting image copyrights. They tried to address the incompatibility between traditional digital watermarking technology and blockchain. They proposed a framework combining the zero-watermarking algorithm, the distributed storage system IPFS and the Ethereum blockchain. The proposed scheme has good robustness to noise filtering and moderate rotations.

Watermarks can be classified into several classes in terms of the monitored parameters. In terms of visual detection, we divide watermarks into visible [33, 34] and invisible [35, 36] watermarks. In terms of robustness to image transformations, we distinguish fragile watermarks, semi-fragile watermarks and robust watermarks. Fragile digital watermarks, like digital fingerprints, are very sensitive to virtually any transformations in the image, which is the main intention. A study in [37] used a dual fragile watermarking scheme to verify the integrity and localization of the tampered area. The results showed that the proposed scheme enhances the security of fragile watermarking and is robust to selected attacks. Semi-fragile watermarks are resilient to benign image operations but cannot handle significant operations. They are commonly used to detect significant image operations. A study in [38] used semi-fragile watermarks for authentication and tamper detection in the form of JPEG2000 compression. The proposed watermark generation process guides the system to verify the integrity of the image without the need for any other file except the watermarked image. Experimental results show that the proposed approach not only has extremely high tamper detection accuracy, but also has relatively high robustness to JPEG2000 compression. The last group is robust watermarking, which can withstand even significant image operations. Robust watermarks, in most cases, use frequency domain images for embedding. A study in [39] proposed an improved robust watermarking algorithm using discrete Fourier

transform (DFT) via spread spectrum that optimizes the number of bands and frequency coefficients, as well as the watermark strength factor using particle swarm optimization in conjunction with visual information fidelity and bit correct rate criteria. Experimental results show increased robustness to conventional signal processing and geometric distortions while maintaining the high visual quality of color images.

Steganography protects the hidden data in the cover image from detection [40, 41, 42]. Image steganography can be applied either directly in the spatial domain of images or in the frequency domain. Applications of steganography in the spatial domain have been addressed by [43]. The authors proposed a scheme using genetic algorithms to find optimal solutions. They used the LSB method for data embedding. To find the appropriate bits to hide the data, they used new concepts of shifting in vertical and horizontal directions, pixel scanning direction, secret image transposition, flipping of secret bits and using the XOR operation. The proposed scheme achieves high embedding capacity and reaches the desired imperceptibility of the stego image. Another study that addressed steganography in the spatial domain is [44], which proposed a multiple embedding scheme based on genetic algorithms for reversible data hiding based on histogram shifting. Compared with the previous approaches, experimental results show that the proposed scheme is superior in terms of embedding capacity and stego image quality. A study in [45] proposed a scheme using the integer wavelet transform (IWT) with improved embedding capacity. They used the coefficient value differencing (CVD) technique. The results showed that the eight-way CVD technique improves coefficient utilization, which helps to improve embedding capacity. Only high-frequency coefficients are used for embedding secret data because the distortion of high-frequency coefficients is less perceptible to the human eye than that of low-frequency coefficients. To enhance the security of the system, the secret data is embedded in horizontal and vertical subbands in a non-sequential manner. The proposed technique successfully resists both statistical and steganalysis attacks.

Steganography in the frequency domain was the subject of a study by [46]. The author used a secure medical data transmission mechanism based on a bit mask oriented genetic algorithm (BMOGA). The encrypted data is embedded in the medical images through 1-level and 2-level DWT. To extract the secret message from the encrypted one, the inverse process of BMOGA is implemented. The results show that the proposed algorithm is capable of secure data transmission. A study in [47] addressed the data hiding technique with enhanced embedding capacity using a combination of optimal pixel selection and LSB quantized DCT coefficients. It works with image partitioning into non-overlapping blocks of 8×8 pixels. The proposed scheme achieves high image quality because it selects the optimal pixels of a block. The performance of the proposed technique is evaluated using a standard dataset and compared with other state-of-the-art techniques. The proposed algorithm shows that the embedding capacity, stego image quality and processing time are better than other existing techniques.

3 THEORETICAL BACKGROUND OF PROPOSED MODEL

Our research in PCNNs began with the design of an optimized OM-PCNN model for reducing the dimension of the classification space. The OM-PCNN architecture is based on the original PCNN architecture with a modified feeding input [48, 49]. The optimization achieved a reduction in the number of parameters, furthermore, a mechanism for setting the initialization values of key parameters as well as an algorithm for generating features with a minimized number of iterations of the neural network were proposed [50, 51, 52, 53]. The structure of the original PCNN model and the OM-PCNN model itself are practically the same. It is a single-layer neural network. If we consider the input image as a 2D matrix, then the neural network matrix has the same structure as the image matrix. Each neuron has two defined inputs: a feeding input and a linking input (Figure 1).

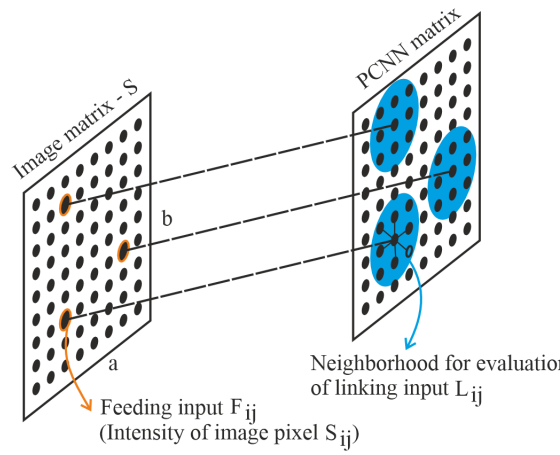


Figure 1. Structure of OM-PCNN neural network

The feeding input F_{ij} of each neuron is represented by one image pixel with intensity S_{ij} that corresponds positionally to the neuron in the neural network matrix. Linking input L_{ij} of each neuron depends on the number of active neurons in the linking neighborhood. Central neuron of each linking neighborhood will be reffered to as centroid. The size of the linking neighborhood, i.e., the OM-PCNN kernel matrix, depends on the linking radius r_o and the type of the neuron's linking neighborhood, which can be circular or square, depending on the used metric. Among the available metrics, the Chebyshev metric (C_D), Euclidean metric (E_D)

or Manhattan metric (M_D) are commonly applied:

$$C_D(x_i, x_j) = \max_k(|x_{ik} - x_{jk}|), \tag{1}$$

$$E_D(x_i, x_j) = \sqrt{\sum_{k=1}^{d}(x_{ik} - x_{jk})^2}, \tag{2}$$

$$M_D(x_i, x_j) = \sum_{k=1}^{d}|x_{ik} - x_{jk}|, \tag{3}$$

where d is the dimension of the feature space, x_i represents the centroid, and x_j is the neighborhood neuron.

The mathematical model of the OM-PCNN neuron (Figure 2) can be divided into three parts. The first part consists of the feeding and the linking input. The second part of the neuron contains the linking unit, in which the feeding and linking inputs are combined. The third part of the neuron is represented by a pulse generator and a threshold generator.

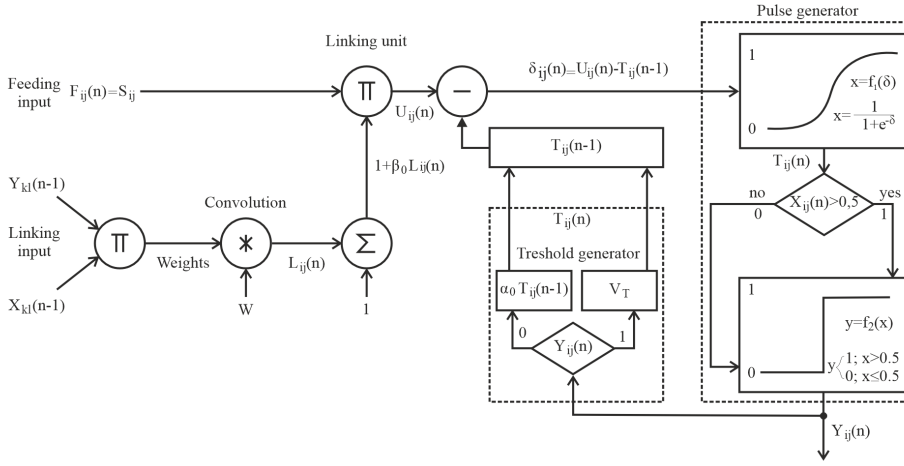


Figure 2. Mathematical model of the OM-PCNN neuron

The feeding input F_{ij} of centroid (i, j) in iteration n is represented by the following equation:

$$F_{ij}(n) = S_{ij}. \tag{4}$$

The linking input $L_{ij}(n)$ is given by the convolution of the weight matrix W and the product of the output matrices $X(n-1) \cdot Y(n-1)$ from the previous iteration $n-1$. The convolution is computed only for neurons that belong to the linking

neighborhood of the centroid (i, j):

$$L_{ij}(n) = [W * (X(n-1) \cdot Y(n-1))]_{ij}, \tag{5}$$

where the symbol "$*$" is the convolution operator and the symbol "$\cdot$" is the multiplication operator of the output matrices $X(n-1)$ and $Y(n-1)$. The elements of the matrix $X(n-1)$ represent the output activation quantities of the corresponding neurons based on the sigmoidal activation function (8) from the previous iteration $n-1$. The elements of the matrix $Y(n-1)$ represent the output activation quantities based on the step activation function (9) from the previous iteration $n-1$. Each element of the kernel matrix W represents the connection weight between the centroid and the neighborhood neuron. The elements of the kernel matrix W, i.e., the values of the weight coefficients, depend on the link radius r_o and the implemented kernel of the neural network. The most commonly used kernels for PCNNs are the kernel based on the Gaussian distribution or the $1/r$, $1/r^2$ kernels. In the case of using OM-PCNN for steganography, the kernel is generated using a stego key.

In the linking part of the neuron, occurs the modulation of the feeding input S_{ij} with the linking element $(1 + \beta_o \cdot L_{ij}(n))$. The modulation result is the input potential of the neuron $U_{ij}(n)$, which can be characterized by the formula:

$$U_{ij}(n) = S_{ij} \cdot [1 + \beta_0 \cdot L_{ij}(n)], \tag{6}$$

where β_o is the linking coefficient, which determines the degree of modulation of the feeding and linking inputs.

The level of the neuron's action potential $\delta_{ij}(n)$ has a profound effect on the neuron's pulsation. Pulsation is the output effect of each neuron in the OM-PCNN representing a series of active and inactive states of the neuron in a time sequence. The action potential $\delta_{ij}(n)$ is given by the difference of the neuron's current input potential $U_{ij}(n)$ and the threshold potential $T_{ij}(n-1)$ from the previous iteration of the OM-PCNN. $U_{ij}(n)$ has activating effect, while $T_{ij}(n-1)$ has inhibitory effect on neuron activity:

$$\delta_{ij}(n) = U_{ij}(n) - T_{ij}(n-1). \tag{7}$$

In the third part of the OM-PCNN neuron, it is decided whether the neuron will be activated or not. The third part of the neuron is made of a pulse generator and a threshold generator. In the pulse generator, a sigmoidal activation function evaluates the first neuron's output $X_{ij}(n)$, which determines the degree of activation of the neuron:

$$X_{ij}(n) = \frac{1}{1 + e^{-\delta_{ij}(n)}}. \tag{8}$$

The values of $X_{ij}(n)$ are in the interval $\langle 0, 1 \rangle$. The second neuron's output $Y_{ij}(n)$ depends on $X_{ij}(n)$ and determines whether the neuron in iteration n is active. The

output $Y_{ij}(n)$ is based on the step activation function:

$$Y_{ij}(n) = \begin{cases} 1, & \text{if } X_{ij}(n) > 0.5, \\ 0, & \text{else.} \end{cases} \tag{9}$$

The step activation function normalizes the output of each neuron to the binary values 0 (neuron activation is suppressed) and 1 (neuron is activated). This is the basic principle of generating binary images using OM-PCNN in each iteration step n. Based on the value of $Y_{ij}(n)$, the threshold potential of the neuron $T_{ij}(n)$ is then calculated:

$$T_{ij}(n) = \begin{cases} V_T, & \text{if } Y_{ij}(n) = 1, \\ \alpha_o \cdot T_{ij}(n-1), & \text{if } Y_{ij}(n) = 0, \end{cases} \tag{10}$$

where the parameter α_o is the threshold decay coefficient and the parameter V_T is the threshold potential coefficient. Formulas (4), (5), (6), (7), (8), (9) and (10) represent one iteration of the neuron. The number of iterations N, in most cases, is given by a qualified guess. In the case of OM-PCNN for steganographic purposes, it is in the interval $\langle 1, 5 \rangle$.

It has been shown that OM-PCNN has a potential in the field of image steganography, mainly due to its robustness to noise [54]. OM-PCNN generates a series of temporary binary images that represent the current state of the neurons in a given iteration (Figure 3). These binary images are the candidate position matrices for embedding.

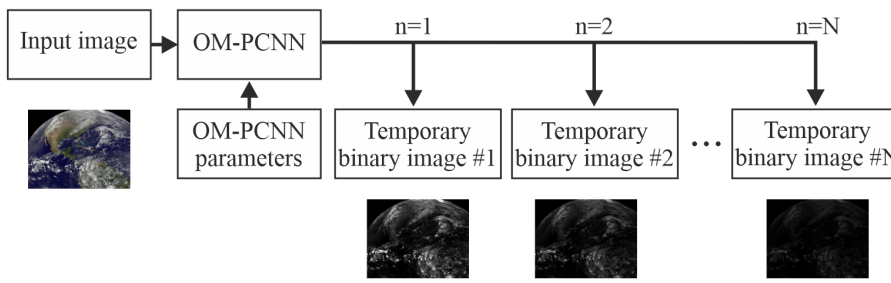


Figure 3. A series of binary images generated using OM-PCNN

The position matrices serve as templates for embedding messages into the cover images. The individual bits of the hidden message will be inserted into the cover image according to selected position matrix. Each binary image generated by the OM-PCNN within the n^{th} iteration can be considered a position matrix for the placement of the hidden message if it satisfies two basic criteria. The first criterion is the complete matching of the binary matrices of the cover image and the stego image. The second criterion is the capacity of the position matrix, which must be at least equal to the size of the hidden message. The selection of binary image matrices

within the first iteration, i.e., $n = 1$, is not recommended due to the initialization of the OM-PCNN. The embedding itself is performed using the LSB method, which is one of the most commonly used methods in the spatial domain of images. The principle of embedding the hidden message into the image itself is based on the LSB method (Figure 4). The bits of the hidden message are inserted only in those image points of the cover image that correspond to the unit elements of the position matrix:

$$y_i = \begin{cases} x_i + 1, \\ x_i - 1, \\ x_i, \end{cases} \tag{11}$$

where x_i is the original pixel value and y_i is the modified pixel value after LSB substitution. OM-PCNN-based steganography has two major advantages, namely the generation of a position matrix for message embedding and the invariance of OM-PCNN to noise.

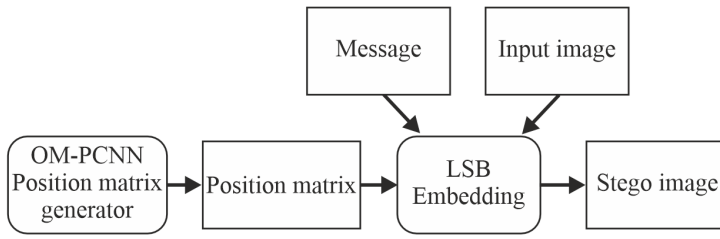


Figure 4. The embedding principle using OM-PCNN and LSB

4 AUTHENTICITY VERIFICATION MODEL

Our image authentication approach is based on a combination of cryptography (hashing and symmetric encryption), steganography and OM-PCNN neural network. The main goal was to design an offline solution where there is no need to store the accompanying steganographic data in secure repositories. The presented method is based on a unique stego key. The description of the detailed protocol for generating the different elements (stego key, random number, kernel, etc.) and the procedures in the authentication process is beyond the scope of this paper. Based on the description of the proposed method, one can proceed with the actual protocol specification, e.g., selection of the hashing method, random number generator, encryption algorithm, generation of starting positions, etc.

The testing set consisted of 500 gray satellite images with 8 bit depth without compression. The resolution $(x \times y)$ of those images was $1\,000 \times 1\,000$, $2\,000 \times 2\,000$ and $3\,000 \times 3\,000$. All experiments were realized within the inner matrix (IM) with the resolution $(a \times b)$ of 500×500 pixels (Figure 5).

Our authenticity verification concept consists of a proposed model baseline, cover image protection and the final stego image authenticity verification.

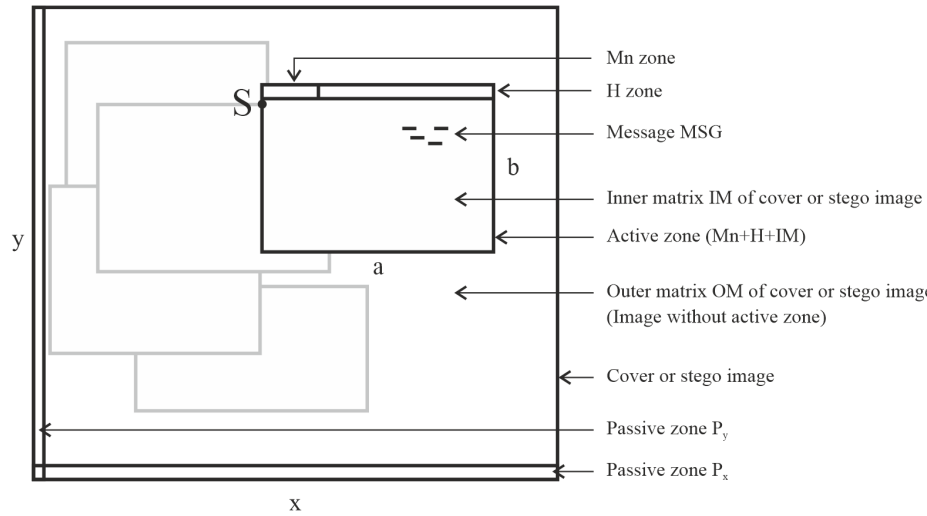


Figure 5. Cover or stego image with embedding zones

4.1 Baseline of the Proposed Model

For descriptive purposes, we have named the entity to insert the message into the cover image "Publisher" and the entity to extract the message from the cover image "Recipient". The success of the proposed steganographic method is dependent on several factors. OM-PCNN is the key factor of the proposed model. The optimal parameter setting allows to generate identical position matrices from both the cover image and the stego image. This means that the same position matrix is used for message embedding into the cover image at the Publisher side and for extracting the message from the stego image at the Recipient side. Message embedding and extraction are two independent processes. In [55] the influence of OM-PCNN parameters on the generation of position matrices is described. Namely, linking coefficient – β_o, linking radius – r_o, Type of OM-PCNN kernel – K, threshold decay coefficient – α_o, threshold potential coefficient – V_T, initialization value of threshold potential – $T(0)$, the number of iterations per cycle – N and type of activation function are explained. In the interval of 2 to 5 iterations, for which the OM-PCNN is optimized, the key influence of the parameter pair α_o and $T(0)$ has been demonstrated. In [56], two approaches for evaluating the quality of stego images based on entropy were compared. The first approach is based on the OM-PCNN position matrix. The second approach was based on generating random positions for embedding. Experiments

showed that embedding using a position matrix is a more efficient method compared to random embedding. OM-PCNN allows to locate regions with higher entropy in the images, thus minimizing the probability of embedding detection.

A proposed method to authenticate large images is based on the work of [57]. Experiments with cover images with a resolution of 500×500 pixels evoked the idea of applying "window" steganography. The baseline of this method is a window selection from the original large cover image, in which operations are performed to ensure the authenticity of the whole image. Compared to the original model, all the accompanying data required for message extraction at the Receiver side is part of the stego image. The principle of output parameter minimization applies, i.e., using only the necessary parameters to extract the hidden messages from the stego images.

In the preparatory phase, the necessary operations for the authentication process need to be carried out:

1. Generating stego key. The stego key is generated from the password using the SHA-256 hash function. The stego key is distributed between the Publisher and the Recipient only.
2. Unique number (UN) generation. This number is unique for each cover image. Our protocol uses a string length of 256 bits.
3. Generation of the start positions of the OM-PCNN key-parameter interval searches – α_o, $T(0)$. These positions are computed by combining the stego key and the pixel values of the passive zone P_x and P_y.
4. OM-PCNN kernel generation. The kernel represents the weight matrix of the neural network, which is computed by combining the stego key and the pixel values of the passive zone P_x and P_y.
5. Symmetric encryption key generation is optional to make the contents of sensitive data inaccessible in case of breaking the steganographic method. Our protocol uses AES-256 with a key equal to stego key.

4.2 Cover Image Protection

In this work, the term "cover image protection" refers to the creation of a stego image with implemented protection mechanisms. The pseudo-algorithm on the Publisher side can be described as follows:

1. The Publisher generates a 256-bit hash code from the outer cover image matrix. The hash is concatenated with the UN to produce a message of length 512 bits (MSG). The reason for combining the hash and the UN is to reduce the dependency of the MSG solely on the image data.
2. The Publisher generates the position of the inner image matrix (IM) based on the stego key and the passive zone P_x for x-axis, P_y for y-axis of the cover image (P_x + stego key, P_y + stego key). This means that the IM position will

be different for each image. The IM must not interfere with the passive zone. This is due to the possible overwriting of some bits in the passive zone caused by MSG embedding.

3. For the adaptation of the key parameters of the OM-PCNN, we seek a combination of parameters in such a way that the neural network generates the same position matrix for both the cover image and the stego image. The number of cycles M completed to find a suitable combination and the iteration number n within the final cycle are part of the accompanying data, which we insert into the Mn zone after AES-256 encryption with stego key. Using the values of M and n, we can compute the key parameters α_o, $T(0)$ to generate the position matrix. During adaptation, at each cycle and iteration, the candidate position matrix of the cover image is compared with the corresponding candidate stego image. If the position matrix candidates match, the position matrix and also the key parameters α_o, $T(0)$ have been found. The starting position of the MSG embedding is given by the centroid of the position matrix.
4. The Publisher inserts the MSG using the position matrix from point 3 into the IM. The result represents the inner stego image.
5. The Publisher adds a UN to the end of the inner stego image matrix and generates a 256-bit hash. The hash is inserted into the H zone. The generation of the stego image of the original cover image is complete.
6. The original cover image is deleted or stored in a protected location by the Publisher so that the cover image and stego image matrices cannot be compared. The stego image is considered to be the original.

4.3 Stego Image Authenticity Verification

The pseudo-algorithm corresponds to the process of extracting the MSG from the stego image on the Recipient side:

1. The Receiver calculates the IM position in the stego image. It decrypts the values of M and n from the Mn zone using AES-256 with stego key. In case of a decryption error, the authenticity of the stego image can be violated. After successful decryption, the starting position of the parameters α_o, $T(0)$ is determined using the stego key and the passive zone of the stego image. The values of the parameters α_o, $T(0)$ are calculated using M.
2. The Receiver generates the OM-PCNN kernel using stego key and the pixel values of the passive zone P_x and P_y. The IM is fed to the input of the OM-PCNN and the position matrix for the n^{th} iteration is generated. The centroid position of the position matrix is computed and the MSG is extracted.
3. The Receiver generates and compares the OM hash with the hash from the MSG. If the hashes match, the outer image matrix is authentic.

4. The Receiver adds a UN from MSG to the end of the IM and generates a 256-bit hash. If the generated hash matches the hash in the H zone, the stego image is authentic.

4.4 Evaluation of the Model

It is well known that PCNNs, due to their iterative nature are more time-consuming to process images. The random starting position of scanning the intervals of key parameters of OM-PCNNs can speed up the parameter adaptation significantly, but on the contrary, it can also slow it down. Parameter adaptation with step 0.01 requires about 1 500 cycles for a complete search of the redefined ranges of the two key parameters, which in the presented model represents up to 7 500 iterations for a single image in the worst case. The situation worsened with the increasing size of the images. For example, the processing of a 500×500 resolution image is about 3.6 times slower than a 200×200 resolution image. The idea of implementing steganography in a predefined cover image cutout unifies the computational complexity of generating position matrices for any large image solely based on the size of the image matrix of that cutout. The question is whether the limited size of the image matrix for embedding will be capaciously sufficient for authentication purposes. The experimental results clearly demonstrated that for a test set of images with a resolution of 500×500, a minimum embedding capacity of 723 bytes and a maximum capacity of up to 31 237 bytes were achieved (Figure 6). This is the capacity at which OM-PCNN can generate identical position matrices for both the cover image and the stego image, which is a prerequisite for the successful deployment of the presented method. This means that even images with minimal embedding capacity offer about three times more space than required by the authenticity itself, including the accompanying data.

The quality of the steganographic method can be determined by the change in the entropy of the image after the message is embedded. The entropy calculation is given by the formula

$$H(x) = -\sum_{i \in 0}^{255} p_i \log_2 p_i, \tag{12}$$

where i is the pixel intensity value and p_i is the probability of these pixel values occurring in the image. The maximum achievable entropy for images with a bit depth of 8 bits per pixel is 8. The entropy change after OM-PCNN based embedding and random MSG distribution in the image has been tested. The reference value is the entropy of the cover image. The images were divided into five groups according to the maximum embedding capacity (Figure 7). The results show that the lowest entropy change was achieved within each group using OM-PCNN based embedding (Table 1).

Despite the positive results achieved above, the presented model also has weaknesses. The problem is the embedding of the accompanying data (see Section 4.2, No. 3) in the Mn zone and the hashes (see Section 4.2, No. 5) in the H zone. These

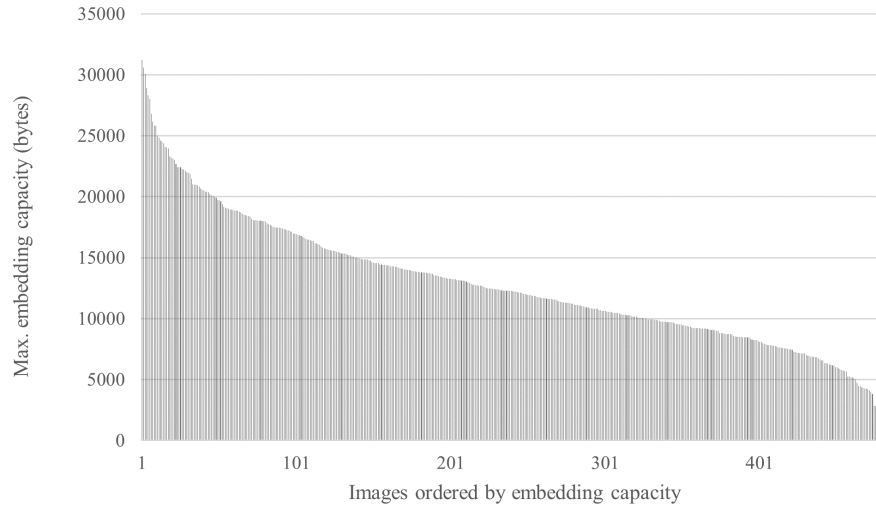


Figure 6. Overview of the maximum embedding capacity achieved for a group of 500 images with a resolution of 500×500

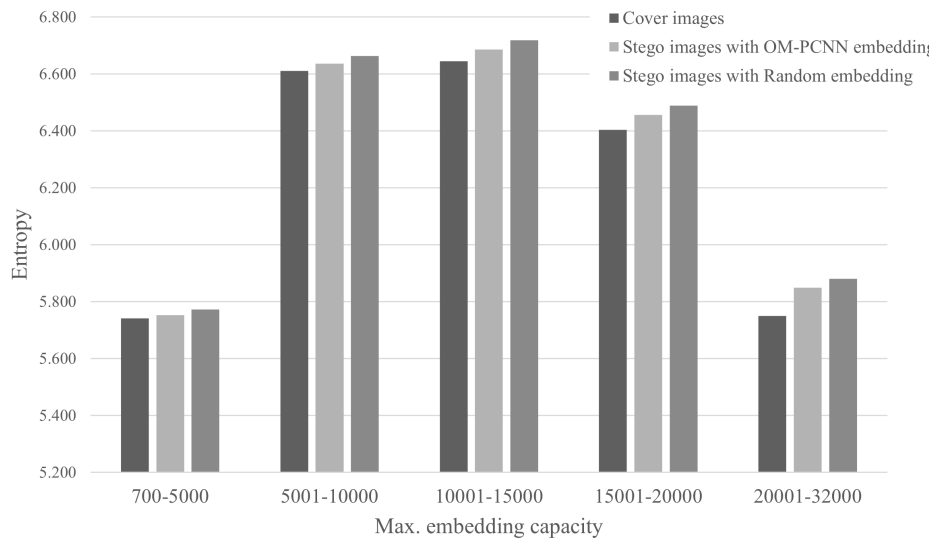


Figure 7. Overview of entropy values for five groups of images according to the maximum achieved embedding capacity

Maximum Embedding Capacity Range (Bytes)	Entropy of Cover Images	Entropy Change (%)	
		OM-PCNN Approach	Random Embedding
700–5 000	5.740	0.20	0.55
5 001–10 000	6.610	0.38	0.80
10 001–15 000	6.645	0.60	1.11
15 001–20 000	6.403	0.82	1.33
20 001–32 000	5.749	1.73	2.28

Table 1. Change of entropy by maximum embedding

are about 450 bits that are stored sequentially over the IM matrix, which may increase the probability of detectability of the embedded data. Since the security measure of the steganographic method is of primary importance in authentication, i.e., the unbreakability of the data embedding and extraction algorithms, the risk of steganography detection can be acceptable. This means that despite the detection of the embedding positions and the subsequent modification attempt in the Mn zone, the encrypted accompanying data will be degraded, which is evaluated by the system as an authenticity violation. Similarly, any modification in the H zone will trigger a hash mismatch on the Receiver side. Moreover, the position of the IM image matrix is different for each image as it depends on the stego key, the passive zone of the cover and the stego image, respectively. There may be other hidden risks that could be revealed by detailed steganalysis.

5 CONCLUSIONS

The main goal of any steganographic method is to minimize the probability of detecting or suspecting the existence of a hidden message in the stego image. In the case of authentication by steganography, however, this is not always a requirement. Our proposed model provides an efficient way to ensure the integrity and authenticity of high-resolution gray images relatively quickly. To minimize the processing time of large images, steganography has been proposed only in the inner image matrix, which is a subset of the original cover image. The presented OM-PCNN based method embeds the required data in the regions of high entropy. The entropy change after message embedding is lower compared to random embedding. The above attributes reduce the detection probability of embedded authentication data and accompanying data. Another advantage of the presented solution is the extension of the embedded data types. In addition to authentication data, other data related to a particular image can be embedded. For example, this can be personal data, access permissions, identifiers, passwords, or even data used to annotate the images, which can be used to search and sort the images according to different criteria. The advantage of the steganographic approach is that the data is an integral part of the subject image and is only accessible based on knowledge of the stego key.

The proposed steganography model belongs to the category of strict image authentication methods. It can effectively determine whether an image has been altered, even if it is a single pixel modification. Although the model does not allow the change to be localized, this is not a necessary requirement in the case of authentication. The presented model is not suitable for the authentication of images for which geometric transformations or conversion to another image format must be performed. These operations are evaluated by the model as modifications that corrupt the integrity of the image data. The strictness of the method can also be an issue for non-substantial image modifications, such as bitwise modifications in non-validated transmission protocols or automatic modification of image resolution during transmission using some communication applications. Model security requires detailed steganalysis. In the case of avoiding steganalytic detection and hidden message extraction, the option to encrypt all embedded data is still available.

In conclusion, the presented model based on the steganographic method using the OM-PCNN neural network has wide implementation possibilities. In the near future, it is planned to be included in a system for anomaly detection in distributed systems as well as for annotation of image data in order to determine the prevailing visibility.

Acknowledgement

This work was supported by the Slovak Research and Development Agency under the Contract No. APVV-20-0571 (ICONTROL) and by the Slovak Scientific Grant Agency VEGA 2/0131/23.

REFERENCES

[1] Shaik, A. S.—Karsh, R. K.—Islam, M.—Laskar, R. H.: A Review of Hashing Based Image Authentication Techniques. Multimedia Tools and Applications, Vol. 81, 2022, No. 2, pp. 2489–2516, doi: 10.1007/s11042-021-11649-7.

[2] Raj, N. R. N.—Shreelekshmi, R.: A Survey on Fragile Watermarking Based Image Authentication Schemes. Multimedia Tools and Applications, Vol. 80, 2021, No. 13, pp. 19307–19333, doi: 10.1007/s11042-021-10664-y.

[3] Chennamma, H. R.—Madhushree, B.: A Comprehensive Survey on Image Authentication for Tamper Detection with Localization. Multimedia Tools and Applications, Vol. 82, 2022, No. 2, doi: 10.1007/s11042-022-13312-1.

[4] Du, L.—Ho, A. T. S.—Cong, R.: Perceptual Hashing for Image Authentication: A Survey. Signal Processing: Image Communication, Vol. 81, 2020, Art. No. 115713, doi: 10.1016/j.image.2019.115713.

[5] Renklier, A.—Öztürk, S.: A Novel Frei-Chen Based Fragile Watermarking Method for Authentication of an Image. Concurrency and Computation: Practice and Experience, Vol. 34, 2022, No. 22, Art. No. e6897, doi: 10.1002/cpe.6897.

[6] Nguyen, T. S.: Fragile Watermarking for Image Authentication Based on DWT-SVD-DCT Techniques. Multimedia Tools and Applications, Vol. 80, 2021, No. 16, pp. 25107–25119, doi: 10.1007/s11042-021-10879-z.

[7] Senol, A.—Elbasi, E.—Topcu, A. E.—Mostafa, N.: A Semi-Fragile, Inner-Outer Block-Based Watermarking Method Using Scrambling and Frequency Domain Algorithms. Electronics, Vol. 12, 2023, No. 4, Art. No. 1065, doi: 10.3390/electronics12041065.

[8] Kadian, P.—Arora, S. M.—Arora, N.: Robust Digital Watermarking Techniques for Copyright Protection of Digital Data: A Survey. Wireless Personal Communications, Vol. 118, 2021, No. 4, pp. 3225–3249, doi: 10.1007/s11277-021-08177-w.

[9] Du, L.—He, Z.—Wang, Y.—Wang, X.—Ho, A. T. S.: An Image Hashing Algorithm for Authentication with Multi-Attack Reference Generation and Adaptive Thresholding. Algorithms, Vol. 13, 2020, No. 9, Art. No. 227, doi: 10.3390/a13090227.

[10] Hussan, M.—Parah, S. A.—Jan, A.—Qureshi, G. J.: Hash-Based Image Watermarking Technique for Tamper Detection and Localization. Health and Technology, Vol. 12, 2022, No. 2, pp. 385–400, doi: 10.1007/s12553-021-00632-9.

[11] Shaik, A. S.—Karsh, R. K.—Islam, M.—Singh, S. P.: A Secure and Robust Autoencoder-Based Perceptual Image Hashing for Image Authentication. Wireless Communications and Mobile Computing, Vol. 2022, 2022, Art. No. 1645658, doi: 10.1155/2022/1645658.

[12] Gafsi, M.—Amdouni, R.—Hajjaji, M. A.—Malek, J.—Mtibaa, A.: Improved Chaos-RSA-Based Hybrid Cryptosystem for Image Encryption and Authentication. Concurrency and Computation: Practice and Experience, Vol. 34, 2022, No. 23, Art. No. e7187, doi: 10.1002/cpe.7187.

[13] Jasra, B.—Moon, A. H.: Color Image Encryption and Authentication Using Dynamic DNA Encoding and Hyper Chaotic System. Expert Systems with Applications, Vol. 206, 2022, Art. No. 117861, doi: 10.1016/j.eswa.2022.117861.

[14] Parida, P.—Pradhan, C.—Gao, X. Z.—Roy, D. S.—Barik, R. K.: Image Encryption and Authentication with Elliptic Curve Cryptography and Multidimensional Chaotic Maps. IEEE Access, Vol. 9, 2021, pp. 76191–76204, doi: 10.1109/ACCESS.2021.3072075.

[15] Wu, X.—Yang, C. N.—Yang, Y. Y.: Sharing and Hiding a Secret Image in Color Palette Images with Authentication. Multimedia Tools and Applications, Vol. 79, 2020, No. 35-36, pp. 25657–25677, doi: 10.1007/s11042-020-09253-2.

[16] Hlaing, A. T.—Thant, K. M.: Color Image Steganography Using Cryptography and Magic LSB Substitution Method (M-LSB-SM). 2018 Joint International Conference on Science, Technology and Innovation, IEEE, 2019.

[17] Yan, X.—Li, L.—Chen, J.—Sun, L.: Public Key Based Bidirectional Shadow Image Authentication Without Pixel Expansion in Image Secret Sharing. Frontiers of Information Technology and Electronic Engineering, Vol. 24, 2023, No. 1, pp. 88–103, doi: 10.1631/FITEE.2200118.

[18] Khurana, M.—Singh, H.: Two Level Phase Retrieval in Fractional Hartley Domain for Secure Image Encryption and Authentication Using Digital Signatures. Multimedia Tools and Applications, Vol. 79, 2020, No. 19, pp. 13967–13986, doi:

10.1007/s11042-020-08658-3.

[19] Huang, X.—Dong, Y.—Ye, G.—Yap, W. S.—Goi, B. M.: Visually Meaningful Image Encryption Algorithm Based on Digital Signature. Digital Communications and Networks, Vol. 9, 2023, No. 1, pp. 159–165, doi: 10.1016/j.dcan.2022.04.028.

[20] El-Shafai, W.—Almomani, I.—Ara, A.—Alkhayer, A.: An Optical-Based Encryption and Authentication Algorithm for Color and Grayscale Medical Images. Multimedia Tools and Applications, Vol. 82, 2023, No. 15, pp. 23735–23770, doi: 10.1007/s11042-022-14093-3.

[21] Sheidaee, A.—Farzinvash, L.: A Novel Image Steganography Method Based on DCT and LSB. 2017 9th International Conference on Information and Knowledge Technology (IKT), Tehran, Iran, 2017, pp. 116–123, doi: 10.1109/IKT.2017.8258628.

[22] Muhammad, K.—Ahmad, J.—Rho, S.—Baik, S. W.: Image Steganography for Authenticity of Visual Contents in Social Networks. Multimedia Tools and Applications, Vol. 76, 2017, No. 18, pp. 18985–19004, doi: 10.1007/s11042-017-4420-8.

[23] Alarood, A.—Ababneh, N.—Al-Khasawneh, M.—Rawashdeh, M.—Al-Omari, M.: IoTSteg: Ensuring Privacy and Authenticity in Internet of Things Networks Using Weighted Pixels Classification Based Image Steganography. Cluster Computing, Vol. 25, 2022, No. 3, pp. 1607–1618, doi: 10.1007/s10586-021-03383-4.

[24] Gutub, A.—Al-Ghamdi, M.: Hiding Shares by Multimedia Image Steganography for Optimized Counting-Based Secret Sharing. Multimedia Tools and Applications, Vol. 79, 2020, No. 11, pp. 7951–7985, doi: 10.1007/s11042-019-08427-x.

[25] Sharma, S.—Zou, J. J.—Fang, G.: A Single Watermark Based Scheme for Both Protection and Authentication of Identities. IET Image Processing, Vol. 16, 2022, No. 12, pp. 3113–3132, doi: 10.1049/ipr2.12542.

[26] Sanivarapu, P. V.—Rajesh, K. N. V. P. S.—Hosny, K. M.—Fouda, M. M.: Digital Watermarking System for Copyright Protection and Authentication of Images Using Cryptographic Techniques. Applied Sciences, Vol. 12, 2022, No. 17, Art. No. 8724, doi: 10.3390/app12178724.

[27] Wang, Y.—Li, Z.—Gong, D.—Lu, H.—Liu, F.: Image Fragile Watermarking Algorithm Based on Deneighbourhood Mapping. IET Image Processing, Vol. 16, 2022, No. 10, pp. 2652–2664, doi: 10.1049/ipr2.12515.

[28] Jarusek, R.—Volna, E.—Kotyrba, M.: Photomontage Detection Using Steganography Technique Based on a Neural Network. Neural Networks, Vol. 116, 2019, pp. 150–165, doi: 10.1016/j.neunet.2019.03.015.

[29] Zhang, S.—Su, S.—Li, L.—Lu, J.—Zhou, Q.—Chang, C. C.: CSST-Net: An Arbitrary Image Style Transfer Network of Coverless Steganography. The Visual Computer, Vol. 38, 2022, No. 6, pp. 2125–2137, doi: 10.1007/s00371-021-02272-6.

[30] Hussain, S.—Sheybani, N.—Neekhara, P.—Zhang, X.—Duarte, J.—Koushanfar, F.: FastStamp: Accelerating Neural Steganography and Digital Watermarking of Images on FPGAs. Proceedings of the 41st IEEE/ACM International Conference on Computer-Aided Design (ICCAD '22), ACM, 2022, Art. No. 41, doi: 10.1145/3508352.3549357.

[31] Ahmadi, S. B. B.—Zhang, G.—Rabbani, M.—Boukela, L.—Jelodar, H.: An Intelligent and Blind Dual Color Image Watermarking for Authentication and

Copyright Protection. Applied Intelligence, Vol. 51, 2021, No. 3, pp. 1701–1732, doi: 10.1007/s10489-020-01903-0.

[32] Wang, B.—Jiawei, S.—Wang, W.—Zhao, P.: Image Copyright Protection Based on Blockchain and Zero-Watermark. IEEE Transactions on Network Science and Engineering, Vol. 9, 2022, No. 4, pp. 2188–2199, doi: 10.1109/TNSE.2022.3157867.

[33] Fragoso-Navarro, E.—Rangel-Espinoza, K.—Nakano-Miyatake, M.—Cedillo-Hernandez, M.—Perez-Meana, H.: Seam Carving Based Visible Watermarking Robust to Removal Attacks. Journal of King Saud University – Computer and Information Sciences, Vol. 34, 2022, No. 7, pp. 4499–4513, doi: 10.1016/j.jksuci.2021.03.010.

[34] Qi, W.—Liu, Y.—Guo, S.—Wang, X.—Guo, Z.: An Adaptive Visible Watermark Embedding Method Based on Region Selection. Security and Communication Networks, Vol. 2021, 2021, Art. No. 6693343, doi: 10.1155/2021/6693343.

[35] Liu, C.—Zhong, D.—Shao, H.: Data Protection in Palmprint Recognition via Dynamic Random Invisible Watermark Embedding. IEEE Transactions on Circuits and Systems for Video Technology, Vol. 32, 2022, No. 10, pp. 6927–6940, doi: 10.1109/TCSVT.2022.3174582.

[36] Liang, J.—Feng, Z.—Chen, R.—Liu, X.: BHI: Embedded Invisible Watermark as Adversarial Example Based on Basin-Hopping Improvement. Information Sciences, Vol. 640, 2023, Art. No. 119037, doi: 10.1016/j.ins.2023.119037.

[37] Gong, X.—Chen, L.—Yu, F.Zhao, X.—Wang, S.: A Secure Image Authentication Scheme Based on Dual Fragile Watermark. Multimedia Tools and Applications, Vol. 79, 2020, No. 25, pp. 18071–18088, doi: 10.1007/s11042-019-08594-x.

[38] Rhayma, H.—Makhloufi, A.—Hamam, H.—Hamida, A. B.: Semi-Fragile Watermarking Scheme Based on Perceptual Hash Function (PHF) for Image Tampering Detection. Multimedia Tools and Applications, Vol. 80, 2021, No. 17, pp. 26813–26832, doi: 10.1007/s11042-021-10886-0.

[39] Cedillo-Hernandez, M.—Cedillo-Hernandez, A.—Garcia-Ugalde, F. J.: Improving DFT-Based Image Watermarking Using Particle Swarm Optimization Algorithm. Mathematics, Vol. 9, 2021, No. 15, Art. No. 1795, doi: 10.3390/math9151795.

[40] Li, G.—Feng, B.—He, M.—Weng, J.—Lu, W.: High-Capacity Coverless Image Steganographic Scheme Based on Image Synthesis. Signal Processing: Image Communication, Vol. 111, 2023, Art. No. 116894, doi: 10.1016/j.image.2022.116894.

[41] Gao, K.—Chang, C. C.—Horng, J. H.—Echizen, I.: Steganographic Secret Sharing via AI-Generated Photorealistic Images. EURASIP Journal on Wireless Communications and Networking, Vol. 2022, 2022, Art. No. 119, doi: 10.1186/s13638-022-02190-8.

[42] Chowdhuri, P.—Pal, P.—Si, T.: A Novel Steganographic Technique for Medical Image Using SVM and IWT. Multimedia Tools and Applications, Vol. 82, 2023, No. 13, pp. 20497–20516, doi: 10.1007/s11042-022-14301-0.

[43] Wazirali, R.—Alasmary, W.—Mahmoud, M. M. E. A.—Alhindi, A.: An Optimized Steganography Hiding Capacity and Imperceptibly Using Genetic Al-

gorithms. IEEE Access, Vol. 7, 2019, pp. 133496–133508, doi: 10.1109/ACCESS.2019.2941440.

[44] Wang, J.—Ni, J.—Zhang, X.—Shi, Y. Q.: Rate and Distortion Optimization for Reversible Data Hiding Using Multiple Histogram Shifting. IEEE Transactions on Cybernetics, Vol. 47, 2017, No. 2, pp. 315–326, doi: 10.1109/TCYB.2015.2514110.

[45] Mandal, P. C.—Mukherjee, I.—Chatterji, B. N.: High Capacity Steganography Based on IWT Using Eight-Way CVD and n-LSB Ensuring Secure Communication. Optik, Volume 247, 2021, Art. No. 167804, doi: 10.1016/j.ijleo.2021.167804.

[46] Pandey, H. M.: Secure Medical Data Transmission Using a Fusion of Bit Mask Oriented Genetic Algorithm, Encryption and Steganography. Future Generation Computer Systems, Vol. 111, 2020, pp. 213–225, doi: 10.1016/j.future.2020.04.034.

[47] Roselin Kiruba, R.—Sree Sharmila, T.: Secure Data Hiding by Fruit Fly Optimization Improved Hybridized Seeker Algorithm. Multidimensional Systems and Signal Processing, Vol. 32, 2021, No. 2, pp. 405–430, doi: 10.1007/s11045-019-00697-w.

[48] Ranganath, H. S.—Kuntimad, G.: Image Segmentation Using Pulse Coupled Neural Networks. Proceedings of 1994 IEEE International Conference on Neural Networks (ICNN '94), Vol. 2, 1994, pp. 1285–1290, doi: 10.1109/ICNN.1994.374369.

[49] Ranganath, H. S.—Kuntimad, G.—Johnson, J. L.: Pulse Coupled Neural Networks for Image Processing. Proceedings IEEE Southeastcon '95: Visualize the Future, 1995, pp. 37–43, doi: 10.1109/SECON.1995.513053.

[50] Forgac, R.—Mokris, I.: Linking and Activation Potential Optimization in the Pulse Coupled Neural Network. 2008 IEEE International Conference on Computational Cybernetics, Stara Lesna, Slovakia, 2008, pp. 85–88, doi: 10.1109/ICCCYB.2008.4721384.

[51] Forgac, R.—Mokris, I.: Feature Generation Improving by Optimized PCNN. 2008 6th International Symposium on Applied Machine Intelligence and Informatics, Herlany, Slovakia, 2008, pp. 203–207, doi: 10.1109/SAMI.2008.4469166.

[52] Forgac, R.—Mokris, I.: Threshold Potential Optimization in the Pulse Coupled Neural Network. 2008 6th International Symposium on Intelligent Systems and Informatics, Subotica, Serbia, 2008, pp. 1–4, doi: 10.1109/SISY.2008.4664914.

[53] Forgáč, R.—Mokriš, I.: Algorithm for Pulse Coupled Neural Network Parameters Estimation. 2009 IEEE International Conference on Computational Cybernetics (ICCC), Palma de Mallorca, Spain, 2009, pp. 147–151, doi: 10.1109/ICCCYB.2009.5393944.

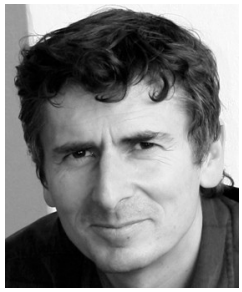
[54] Forgáč, R.—Krakovský, R.: Contribution to Image Steganography Using Pulse Coupled Neural Networks. 2017 Communication and Information Technologies (KIT), Vysoke Tatry, Slovakia, 2017, pp. 1–6, doi: 10.23919/KIT.2017.8109445.

[55] Forgáč, R.—Očkay, M.—Krakovský, R.: Impact of Pulse Coupled Neural Network Parameters on Image Steganography. 2019 Communication and Information Technologies (KIT), Vysoke Tatry, Slovakia, 2019, pp. 1–6, doi: 10.23919/KIT.2019.8883304.

[56] Forgáč, R.—Očkay, M.—Krakovský, R.: Entropy Based Image Quality Assessment of Stego Images Created by Pulse Coupled Neural Network. 2020 New

Trends in Signal Processing (NTSP), Demanovska dolina, Slovakia, 2020, pp. 1–5, doi: 10.1109/NTSP49686.2020.9229546.

[57] Forgáč, R.—Očkay, M.—Javurek, M.: Steganography Based Approach to Image Authentication. 2021 Communication and Information Technologies (KIT), Vysoke Tatry, Slovakia, 2021, pp. 1–6, doi: 10.1109/KIT52904.2021.9583618.



Radoslav Forgáč is a researcher at the Institute of Informatics, Slovak Academy of Sciences. He graduated from the Armed Forces Academy in Liptovský Mikuláš in 1993. He received his Ph.D. in artificial intelligence in 2006 from the Technical University of Košice. His research is focusing on machine learning, especially neural networks for classification, regression and clustering.

Miloš Očkay is a researcher at the Institute of Informatics, Slovak Academy of Sciences and Associate Professor at the Department of Informatics at the Armed Forces Academy in Liptovský Mikuláš. He holds his Ph.D. degree in the field of informatics, received in 2012 from the Technical University of Košice. His research is focusing on parallel computing, neural networks.

Martin Javurek is an Assistant Professor at the Department of Informatics at the Armed Forces Academy in Liptovský Mikuláš and a researcher at the Institute of Informatics, Slovak Academy of Sciences. He holds his Ph.D. degree in the field of informatics, received in 2017 from the Armed Forces Academy in Liptovský Mikuláš. His research focuses on neural networks, cybersecurity and cryptography.

Bianca Badidová is a Ph.D. candidate at the Department of Informatics at the Armed Forces Academy of Liptovský Mikuláš. Her research focuses on data analysis, cybersecurity and neural networks.