ROMANIAN JOURNAL OF INFORMATION SCIENCE AND TECHNOLOGY
Volume 26, Number 3–4, 2023, 339–350

A Data Hiding Approach for Secured Data Communication

T. T. MIRNALINEE[1], J. BHUVANA[1,*], and SB. VINODHINISRI[1]

[1]Department of CSE, Sri Sivasubramaniya Nadar College of Engineering, Chennai, Tamil Nadu, India
Email: mirnalineett@ssn.edu.in, bhuvanaj@ssn.edu.in, sbvinodhinisri@gmail.com
* Corresponding author

Abstract. In the digital era preserving the privacy of confidential information is the crucial issue in authentication and secret communication. Cryptography, steganography, data anonymization are few techniques used to preserve the information. Steganography is the process of hiding information into other non-secret sources of information like text, image or audio, so that secret information is not visible to the naked eye. This paper proposes a novel Prime Number Based Embedding (PNBE) approach for efficient data hiding to encode the data in images without any visual distortion. This approach proposes a novel scheme for identifying the embedding location of the data in the image and PNBE algorithm for the encoding and decoding of messages. The proposed approach is demonstrated with benchmark images. The data encoding capacity and quality are tested on different sized images. Experimental results show better hiding capacity in terms of bytes ranging from 6,327 to 12,448 based on the size of the image. The quality of the image is described as Peak to Signal Noise Ratio (PSNR), which computes the quality difference between original and compressed images. The efficiency of the proposed approach is demonstrated using PSNR with higher values. It is observed from the results that the proposed approach outperforms the existing ones in terms of embedding capacity and quality of the images.

Key-words: Embedding; encoding; data hiding; decoding; steganography.

1. Introduction

Image processing in the fields of electrical engineering and computer science and engineering is applied to perform specific operations on images in order to extract the information or to enhance the images. This is a kind of signal processing where the input is an image or set of images, such as a photograph or video frame, where the output can be either an image or a set of attributes retrieved from the input image. Images are used as carrier signal to carry the secret

information during transmission and storage. With the invent of networks and advanced data processing techniques, there are several ways of hiding information namely covert channels, hidden text within web pages, hiding files in plain sight, null ciphers [4]. Cryptography is the science of encoding the intelligent message into unintelligent and unreadable form. It offers the services necessary for secure communication namely privacy, confidentiality, key exchange, authentication, and non-repudiation [12]. But cryptography does not always ensure safe communication, since it reveals the presence of information to be secured.

Steganography is the science of hiding information. The objective of cryptography is to make data unreadable by scrambling it in order to secure it, whereas the purpose of steganography is to conceal the literal presence of the data from a third party. Steganography is an art where the receiver doubts the presence of the message since it is not revealed. The term steganography has the Greek origin and refers to "concealed writing", from the Greek words *steganos* referring "covered or protected", and *graphei* meaning "writing" [17]. The advantage of steganography over cryptography is that messages do not attract attention to others, since their presence is not known to the third party. There are different approaches available as steganographic techniques that enable us to hide the data. Some of the popular steganographic techniques are physical steganography, digital steganography, network steganography, printed steganography and text steganography [12]. In this context, the carrier is the image in which the data will be hidden via encoding resulting in a stego image. The resultant image will, of course be the same type of file as the carrier. The cover medium will usually be image or audio files.This paper focuses on images as carriers and hereafter will be referred to as cover image or stego image.

Authors' contribution towards the data hiding are:

1. Message to be communicated in a secret manner is embedded in a cover image such that no one, except the sender and intended receiver could see it.

2. A new Prime Number Based Embedding (PNBE) approach was designed to identify the location in the image to store the secret message and to retrieve it by the intended receiver. By this novel technique, the capacity of the encoded data in the image is enhanced without compromising the quality of the image.

3. Elaborate experiments were conducted to evaluate the performance of the proposed PNBE technique and whose performance was observed to be better than the existing work.

This paper is organized as follows: Section 2 discusses on various data hiding techniques with similar and relevant literature, Section 3 describes the proposed PNBE technique, Section 4 presents the experiments and results with the corresponding discussion, whereas Section 5 concludes the paper.

2. Literature Survey

The paper [1] divides the image into multiple hierarchies. The signatures at the lower levels of hierarchy guarantee the accuracy to tamper localization and signatures at higher level blocks offer higher resistance to vector quantization attacks. Using hierarchical scheme is more beneficial than the other schemes that use watermarking, since the entire image is used for computing the signature that handles the counterfeit attack.

Several approaches related to data modeling are used in several applications [21], [22]. One such work was reported in [23] using cognition process based on human knowledge. Pattern based and signature based approaches are used for the modelling.

A hybrid approach named multilevel reversible data hiding was proposed in [2], where the peak point of a difference image is integrated with a multilevel hiding strategy. The approach provides large data hiding capacity along with reversibility by finding a trade-off between data hiding capacity and image distortion. The authors reported that their scheme of data hiding had provided good hiding capacity by keeping the distortion low.

A data hiding scheme is proposed as lossless data hiding scheme in [3], where a message is encoded without losses into a cover image. As per this scheme, variations in the 3 consecutive pixels are computed for this purpose. When large number of pixel pairs are with variations, an absolute difference between a pair of pixels is chosen to encode the message in the cover image. To embed a binary bit "1" or "0", the chosen difference is incremented by 1 or remain unchanged. In addition, this approach was used on different smooth to complex images.

The LBP algorithm [4] is a texture classification pattern for transparently and securely hiding data. LBP was mostly used in applications such as texture classification, image retrieval, facial recognition etc. Local Binary Pattern (LBP) is a kind of feature used for classification where this method labels the pixels of an image by thresholding the surroundings of each pixel and computes a binary number. Then the binomial weights are computed by a XOR operation with the binary number to obtain the LBP operator value. The embeddable capacity is 38328 bits of data for 256*256 sized images.

In local edge sensing prediction [6], combinational weight factor has been used by predicting interpolation errors in the surrounding pixels. Better de-correlation is obtained through their approach that estimates the difference image. To minimize the cost function, the approach manipulates the surrounding samples and observed to provide better estimation even for a small disturbance.

An approach named high capacity reversible data hiding scheme was proposed in [7], to enhance the embedding capacity and uses multiple base lossless method using JPEG-LS pixel value prediction. This method reduces the distortion made by the secret data embedding. Usually, the prediction error value will be less in smooth areas when compared to be in boundaries, and hence when secret data embedded in smooth areas achieves better stego image quality. This approach can embed more secret data maintaining the quality of the stego image.

A steganalytic approach was used in reliable detection of LSB in [8], where the presence of the encoded messages is detected. The authors have also observed and reported the maximum size of the message that can be embedded in a cover image.

In data embedding, a scheme based on VQ joint neighboring coding [20] has offered a trade-off between the encoding message capacity and the final stegano image. The cover image is converted by VQ and becomes a VQ image. The message to be hidden is then embedded into the index table of VQ with respect to the index variations. The authors observed that their scheme has achieved higher PSNR and a higher capacity in data hiding.

An approach called Sample Pair Analysis [10] was used to identify (LSB) steganography in images. With relatively good accuracy, the size of the encoded message can be retrieved from the LSB of signal samples. This approach was built on statistical estimates of pairs which are sensitive to least significant bit schemes. Advanced LBP has been used in a similar approach reported in [11].

Without any distortion to the cover images, large capacity of data can be hidden by the scheme

reported as robust and secured image-adaptive data hiding [12]. This approach uses image adaptive energy thresholding technique to embed the data into the cover image, which has the ability to handle the attacks that are either intentional or unintentional namely filtering, compression and Additive White Gaussian Noise (AWGN). It was observed that their approach has given good quality of the stego image when compared to STOOL, COX, CDMA and SEC approaches.

A review of developments in data embedding and watermarking for audio, image, and video was reported [13]. Audio, video and image data-embedding techniques based on implicit and explicit masking were reviewed. The embedded data are basically inaudible or invisible to maintain the quality of the cover media.

The F5 algorithm [14] was introduced to handle the security problem when encoding data into a JPEG image. The F5 algorithm provides high steganographic capacity whose main advantage is it uses an approach based on matrix encoding to enhance the efficiency of encoding. But the F5 algorithm cannot preserve the shape of jpeg image where it can prevent both visual and statistical attacks. For an image sized 256*173 the embeddable capacity is 1855 bytes of data.

Gray scale images are found to be the suitable images to hide data for steganographic approaches [15] since they offer the better hiding capacity and good quality stego images. Non-malicious attacks are better handled by the approach used in lossless robust data hiding scheme.

A data hiding scheme based on Pattern Substitution (PS) was proposed in [17], where the method accumulates the occurrence frequency of various patterns and uses PS for data embedding. During the retrieving phase undistorted cover image is reconstructed by reversing the pixels. The PSNR remains at 40 dB irrespective of the size of the data hidden.

Histogram of the pixel differences was applied in Adjacent Pixel Difference (APD) in [18], based upon the differences in pixel and shifting pixel values. APD is observed to be easy to implement and offers better data hiding capacity without sacrificing quality of stego image and also reported with a PSNR of 48.13 dB.

Data embedding in JPEG images was proposed in [19] using a improved adaptive LSB steganography technique. The visual distortion of the stego image was reduced by shuffling the bit order of the data to be embedded. Logistic maps were used for the shuffling the bits of the data, the optimal parameters for the logistic maps are identified using Genetic algorithm. The major drawback reported was the poor security of the embedded message.

In compression and data lossless information hiding [20], it was attempted to bring the embedded image as close to the actual image so that the data hiding is not visible to naked eye. A balance is arrived between the code stream and capacity of data hidden. This approach excels other schemes in terms of data hiding capacity and bit rate.

One prominent drawback of all image data hiding methods is that the cover image is inevitably distorted, even by the presence of small quantity of noise due to data embedding. In the existing techniques surveyed it is observed that the embedding capacity and quality of the image shall be still more improved to encode data in the cover image. The motivation of the proposed work is to improve the capacity of data embedded in the image and to maintain the quality of the image for which a novel PNBE technique is proposed.

3. Proposed Methodology

An efficient system for data hiding to communicate the messages in a secured manner is proposed. The capacity of the data encoded in the image is enhanced without compromising

the quality of the image. The proposed data hiding scheme, namely Prime Number Based Embedding (PNBE), is comprised of encoding and decoding phases. During encoding, the secret message is encoded in an image and the intended receiver extracts the message using decoding algorithm.

3.1. Design strategy

Fig. 1 shows the proposed architecture of the PNBE approach. The stego image is generated by encoding the secret message into the carrier image. PNBE decoding algorithm extracts the hidden message from the stego image.

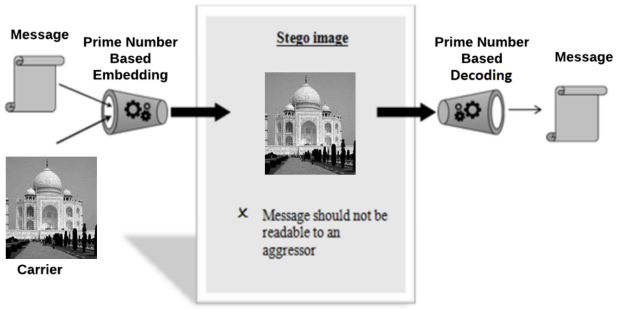

Fig. 1. Proposed architecture.

The carrier image is divided into 9 components as shown in Fig. 2. The center pixel is computed and the 8 neighbors of the center pixel of the carrier image are designated as Group G5 as shown in Figure 2. An embedding code that helps in encoding and decoding the secret message into the carrier image is used and stored in G5. The group G5 has 9 pixels which are referred to as G51, G52, G53,..., G59. The location G51 is having the embedding code for the group G1, group G52 will have the embedding code for G2 and so on (shown in blue arcs emerging out of G5 in Fig. 2).

The message is encoded as per the steps given in Algorithm 1 and the encoded message is stored in G1 to G9 except G5. During decoding the original message is extracted from the encoded message as described in Algorithm 2.

3.2. PNBE based message encoding

As specified in Algorithm 1, a matrix of embedding code is generated with prime numbers and stored in G5 part of the image. The secret message is converted into ASCII and then the same is converted into binary before it is to be encoded in the carrier image. If the embedding code from the matrix is say 2 and the binary digit of secret message is 1 then the pixel in the corresponding G is either incremented or decremented, so that the updated pixel value is divisible by the prime number 2. The binary bit to be embedded in the carrier image is 0 then repeat the same operation by incrementing or decrementing the pixel value so that the pixel value is not divisible by the prime number of the embedding matrix.

This process is repeated on all the groups of the carrier image and finally the image generated will be a stego image that is sent to the other end. Hence the proposed PNBE algorithm securely

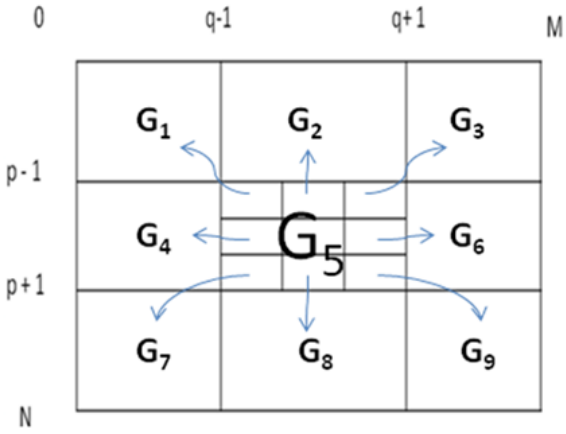

Fig. 2. Grouping of carrier image for efficient encoding.

hides the secret message into the carrier image before the data communication. The stego image generated after PNBE encoding could hide the message efficiently without compromising the quality.

3.3. PNBE decoding

The PNBE decoding algorithm for extracting data from the steganography image is given in Algorithm 2.

For the PNBE decoding, the stego image, StegImg received from the sender will serve as the input for the decoding algorithm from which the hidden message is extracted from this stego Image as described in Algorithm 2. The center of the received image is identified, which is surrounded by the embedding code as a matrix. The StegImg is now divided into 9 groups into G1 to G9 as in Fig. 2.

Binary bits from each group are taken and evaluated whether they are divisible by the embedding code corresponding to that group. If the pixel is divisible by the embedding code, then the binary bit of the secret message is 1 otherwise it is 0. This way the binary stream of secret message is extracted from the StegImg and are converted into ASCII code. The ASCII code is now converted into the secrete message.

Consider an image of size 332 * 300 as shown in Figure 3a, as the carrier image for embedding secret message. The center pixel of the image say (i, j) is chosen as the pivot. Here say, the center pixel location is (166, 150). The following embedding code

$$\begin{bmatrix} 2 & 3 & 2 \\ 2 & 3 & 2 \\ 2 & 2 & 3 \end{bmatrix}$$

is stored in the 3*3 matrix surrounding the center of the image (166,150). Then the image is divided into nine groups say the center G5 will be having the embedding code for the remain-

Algorithm 1 : PNBE encoding algorithm

Input: *Carrier Image: Img,* Message: M
Output: *Steganography image: StegImg*
Function `PNBE Encoding`**:**

```
C ← Center (Img)
G5 ← 3*3 Neighborhood matrix of C
Divide image into 9 different Groups (G1 to G9) as shown in Fig. 2.
Assign EmbeddingCode as prime numbers
for i ∈ [i-1, i, i+1] do
    for j ∈ [j-1, j, j+1] and G ∈ [G1 to G9] ∉ G5 do
        G5 (i, j)=EmbeddingCode(G)
ASCIICode_M ← Convert to ASCII (M)
BinaryCode_M ← Convert to Binary (ASCIIcode_M)
for G ∈ [G1 to G9] ∉ G5 do
    for E ∈ EmbeddingCode [ (2, 3, 5, 7, 9 ...) ] do
        if G (BinaryCode_M)== 1 then
            Increment or decrement G s.t {G % E =0} {G | G % E =0}
        else if G (BinaryCode_M) == 0 then
            Increment or Decrement G s.t {G % E ≠ 0}
```

Algorithm 2 : PNBE decoding algorithm

Input: *Steganography image: StegImg*
Output: *Extracted message: M*
Function `PNBE Decoding`**:**

```
C ← Center (StegImg)
G5 ← 3*3 Neighborhood matrix of C
Divide StegImg into 9 different Groups (G1 to G9) as shown in Figure 2.
Extract EmbeddingCode from G5
for i ∈ [i-1, i, i+1] do
    for j ∈ [j-1, j, j+1] and G ∈ [G1 to G9] ∉ G5 do
        EmbeddedCode (G) = G5 (i, j)
        if G % EmbeddedCode(G) == 0 then
            BinaryData = 1
        else
            BinaryData = 0
ASCIICode ← Convert to ASCII (BinaryData)
M ← Convert (ASCIICode)
```

ing eight groups. For instance, if the secret message is “FIND”, the ASCII value for the input message is ”70 73 78 68”. The ASCII is now represented as a 8 bit binary data, which will be ”1000110 1001001 1001110 1000100”. The binary data is next embedded into each group by using the embed code, in the 3*3 matrix as specified in the embedding algorithm. Then the stego image which contains the hidden message is obtained. The stego image with the hidden message is sent to the other end of communication. At the other end, the secret message ”FIND” is extracted from the received StegImg.

4. Results and Discussion

The efficiency of the proposed PNBE scheme is evaluated by applying the algorithm on different sized images and is compared with existing data hiding techniques. PNBE scheme is evaluated on two different criteria namely;

1. Data encoding capacity
2. Peak-signal-to-noise-ratio (PSNR)

Data encoding capacity of the proposed PNBE scheme for an M * N image is computed using

$$EC_{PNBE} = \frac{M * N * N_U}{8}, \tag{1}$$

where M and N are the width and height of the cover image, N_U is the number of unused bits. N_U will take the value 16, by using 8 bits from group G5 according to Fig. 2, which have the embedding code and the remaining 8 bits from the eight groups G1 to G9 one bit from each group except G5.

Peak-Signal-to-Noise-Ratio (PSNR) is used as a quality measure for obtaining the quality of the given input image and obtained stego image. The quality of the image is high when the PSNR value is high. The two steps involved in calculating PSNR values are described as follows, 1 and 2.

1. Calculating the Mean Square Error as given in (2).

$$MSE_{Image} = (double(A) - double(B))^2, \tag{2}$$

   where A and B in (2) are the original carrier image and the stego image, respectively.

2. Computing the PSNR value using the MSE_{Image} in terms of

$$PSNR_{Value} = 10 * log_{10} \frac{255^2}{MSE_{Image}}. \tag{3}$$

The proposed PNBE scheme is applied on Dog, House, Moon and Taj Mahal of 332 x 300, 256 x 256, 256 x 256 and 225 x 225 sized images. Figs. 3a and 3b show the the carrier image before and after the encoding. The data hiding capacity achieved by the PNBE on Dog image is 12,448 bits. The LBP [4] technique on the same image has achieved capacity of about 7,820 bits of data, which is approximately 4Kb less than the PNBE scheme. PNBE on the House image

(a) Original image. (b) Stego image - capacity of 12,448 bits.

Fig. 3. Experimental results for Dog image of size 332*300

(a) Original image of size 256 *256 (b) Stego image - capacity of 65,520 bits.

Fig. 4. Experimental results for House image

Table 1. Capacity and quality evaluation for the proposed PNBE method

S. No.	Image	Image size	Capacity (Bits)	Quality (dB)
1	House	256 * 256	8190	49.94
2	Moon	256 * 256	8190	51.36
3	Dog	332 * 300	12448	61.78
4	Taj Mahal	225 * 225	6327	77.88

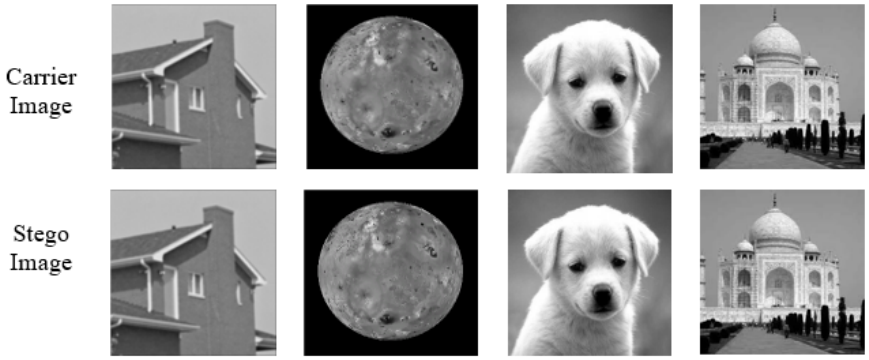

Fig. 5. Experimental results of the test images obtained before and after message encoding.

as shown in Fig. 4a offers the data capacity of about 65520 bits. Fig. 4b illustrates the result obtained after the PNBE encoding.

Fig. 5 shows the carrier image and the stego images before and after encoding the hidden message using the PNBE scheme proposed in this paper. Table 1 shows the varying capacity in bits and quality in dB for the images which are listed in Fig. 5.

From the results obtained, it can be observed that the quality of the stego image generated by our proposed PNBE technique is within 50 dB and 80 dB, where the average quality is found to be 63.75 dB. With respect to the quantity of data, the PNBE scheme proposed in this paper has the ability to encode an average of 10914 bytes in the carrier image.

The proposed PNBE scheme was next compared with the scehmes reported in [12] and [4] on different carrier images as listed in Table 2. The comparison is based on both data hiding capacity in bits per pixel and the PSNR in dB. The images are all of same size as 512 x 512. The proposed scheme has the ability of encoding a maximum of 262128 bits per pixel of fixed capacity, whereas the other two scehemes in Table 2 have not shown similar and lesser performance.

The difference in capacity between the proposed PNBE and [12] is in the range of 222053 bits to a maximum of 247968 bits, whereas the difference between the proposed PNBE and [4] is about 76736 bits to a maximum of 247927 bits. This clearly shows the data hiding efficiency of the PNBE scheme is better than the two other existing schemes compared here.

The maximum PSNR is obtained for the Bridge image with 51.24 dB which has been greater than the other two schemes significantly. The average PSNR of the proposed sceheme is greater than 50% than the average PSNR of 40.38% obtained by [12] and 38.22% by [4]. The proposed PNBE scheme has performed better than the competing schemes with respect to capacity, without compromising the quality of the stego image.

Table 2. Comparison of the results of Mali et al.'s approach [12], Varsaki et al.'s approach [4] and the approach proposed in this paper.

	Proposed		Mali et al.'s [12]		Varsaki et al.'s [4]	
Carrier	Capacity	PSNR	Capacity	PSNR	Capacity	PSNR
Pepper	262128	50.01	14160	41.77	185392	36.93
Baboon	262128	51.06	40075	39.67	56528	39.06
Bridge	262128	51.24	35868	40.98	113880	38.02
Boat	262128	51.02	21063	41.08	168536	40.04
Couple	262128	51.06	23700	38.40	14201	37.06

5. Conclusions

A novel steganography approach expresed as a scheme has been proposed to secure the data during transmission focusing on the Prime Number Based Embedding (PNBE) technique to hide and retrieve the secret data. The proposed scheme based on PNBE has a maximum capacity of about 2,62,128 bits of data hidden in the image sized 512 * 512. The proposed scheme is able to embed large amount of data without any distortion in the image, whose quality in PSNR is maintained above 50 dB. The applications of the approach suggested in htis paper include image authentication, tamper proofing, and secret communications. Overall, it is hoped that the

development of the approach will lead to the improvement of both capacity and quality of the images. Future work shall be extended by making the proposed PNBE approach to work for color images.

References

[1] M. U. CELIK, G. SHARMA, E. SABER and A. M. TEKALP, *Hierarchical watermarking for secure image authentication with localization*, IEEE Transactions on Image Processing **11**(6), 2022, pp. 585–595.

[2] C. C. LIN, W. L. TAI and C. C. CHANG, *Multilevel reversible data hiding based on histogram modification of difference images*, Pattern Recognition **41**(12), 2008, pp. 3582–3591.

[3] C. C. LIN and N. L. HSUEH, *A lossless data hiding scheme based on three-pixel block differences*, Pattern Recognition **41**(4), 2008, pp. 1415–1425.

[4] E. E. VARSAKI, V. FOTOPOULOS and A. N. SKODRAS, *Data hiding based on image texture classification*, Signal, Image and Video Processing **7**(2), 2013, pp. 247–253.

[5] J. FRIDRICH, M. GOLJAN and R. DU, *Lossless data embedding—new paradigm in digital watermarking*, EURASIP Journal on Advances in Signal Processing **2002**(2), 2002, paper 986842.

[6] G. FENG and L. FAN, *Reversible data hiding of high payload using local edge sensing prediction*, Journal of Systems and Software **85**(2), 2012, pp. 392–399.

[7] H. C. WU, C. C. LEE, C. S. TSAI, Y. P. CHU and H. R. CHEN, *A high capacity reversible data hiding scheme with edge prediction and difference expansion*, Journal of Systems and Software **82**(12), 2009, pp. 1966 –1973.

[8] M. GOLJAN and R. DU, *Reliable detection of LSB steganography in grayscale and color images*, Proceedings of the 2001 ACM Workshop on Multimedia and Security, Ottawa, ON, Canada, 2001, pp. 27–30.

[9] J. X. WANG and Z. M. LU, *A path optional lossless data hiding scheme based on VQ joint neighboring coding*, Information Sciences **179**(19), 2009, pp. 3332–3348.

[10] S. DUMITRESCU, X. WU and Z. WANG, *Detection of LSB steganography via sample pair analysis*, in F. A. P. Petitcolas (Ed.), IH 2022: Information Hiding, Springer, Berlin, Heidelberg, Lecture Notes in Computer Science, vol. 2578, 2003, pp. 355–372.

[11] S. LIAO, W. FAN, A. C. CHUNG and D. Y. YEUNG, *Facial expression recognition using advanced local binary patterns, tsallis entropies and global appearance features*, Proceedings of 2006 International Conference on Image Processing, Atlanta, GA, USA, 2006, pp. 665–668.

[12] S. N. MALI, P. M. PATIL, and R. M. JALNEKAR, *Robust and secured image-adaptive data hiding*, Digital Signal Processing **22**(2), 2012, pp. 314–323.

[13] M. D. SWANSON, M. KOBAYASHI and A. H. TEWFIK, *Multimedia data-embedding and watermarking technologies*, Proceedings of the IEEE **86**(6), 1998, pp. 1064–1087.

[14] A. WESTFELD, *F5 - a steganographic algorithm*, in I.S. Moskowitz (Ed.), IH 2001: Information Hiding, Springer, Berlin, Heidelberg, Lecture Notes in Computer Science, vol. 2137, 2001, pp. 289–302.

[15] N. I. WU and M. S. HWANG, *Data hiding: current status and key issues*, IJ Network Security, **4**(1), 2007, pp. 1–9.

[16] X. T. ZENG, L. D. PING and X. Z. PAN, *A lossless robust data hiding scheme*, Pattern Recognition **43**(4), 2010, pp. 1656–1667.

[17] Y. A. HO, Y. K. CHAN, H. C. WU and Y. P. CHU, *High-capacity reversible data hiding in binary images using pattern substitution*, Computer Standards & Interfaces **31**(4), 2009, pp. 787–794.

[18] Y. C. LI, C. M. YEH and C. C. CHANG, *Data hiding based on the similarity between neighboring pixels with reversibility*, Digital Signal Processing **20**(4), 2010, pp. 1116–1128.

[19] L. YU, Y. ZHAO, R. NI and T. LI, *Improved adaptive LSB steganography based on chaos and genetic algorithm*, EURASIP Journal on Advances in Signal Processing **2010**(1), 2010, pp. 876–946.

[20] Z. H. WANG, C. C. CHANG, K. N. CHEN and M. C. LI, *An encoding method for both image compression and data lossless information hiding*, Journal of Systems and Software **83**(11), 2010, pp. 2073–2082.

[21] R.-E. PRECUP, C.-A. BOJAN-DRAGOS, E.-L. HEDREA, R.-C. ROMAN and E. M. PETRIU, *Evolving fuzzy models of shape memory alloy wire actuators*, Romanian Journal of Information Science and Technology **24**(4), 2021, pp. 353—365.

[22] I. D. BORLEA, R. E. PRECUP and A. B. BORLEA, *Improvement of k-means cluster quality by post processing resulted clusters*, Procedia Computer Science **199**, 2022, pp. 63—70.

[23] C. POZNA and R. E. PRECUP, *Aspects concerning the observation process modelling in the framework of cognition processes*, Acta Polytechnica Hungarica **9**(1), 2012, pp. 203—223.