Konyar M. Z. (2023), Image Data Hiding with Local Binary Pattern of Neighbor Pixels. 5th International Congress on Engineering Sciences and Multidisciplinary Approaches, pp 69-74.

# IMAGE DATA HIDING WITH LOCAL BINARY PATTERN OF NEIGHBOR PIXELS

***Mehmet Zeki KONYAR***

***Kocaeli University, Engineering Faculty, Software Engineering Dept., Kocaeli / Türkiye***

**Abstract:** In recent years, the huge increase in digital images made data hiding more popular. Many new methods have been proposed to send hidden text inside ordinary images for information security. These methods aim to embed more secret bits in the cover image and keep the visual quality as possible as high. Image feature extraction-based data-hiding methods have a big importance for embedding procedures. Local binary pattern (LBP) is one of the important texture feature extractors. In this study, we proposed to use a modified LBP-based data hiding method for images with distance-based local neighbors. The proposed method keeps the visual quality while embedding a high number of secret bits with security. In the proposed method, the cover image divides into 3x3 non-overlapping blocks. The center of the blocks defines the center pixel, and the other eight pixels are defined as neighbors. Each block contains five secret bits. So, the LBP code is constructed by binary comparison of the first five pixels with their next neighbors. The secret message bits are ciphered with the obtained LBP codes by logical ex-or operation. The three bits of ciphered secret message embed into the three least significant bits of the center pixel, the remaining bits are embedded into the least significant bits of the last two neighbor pixels. The secret message embeds into all blocks and the stego image sends to the receiver. The receiver extracts the secret message as similar as embedding. Firstly, the LBP codes obtained from stego blocks. Then, related bits of the center pixel and neighbor pixels are extracted and logical ex-or operated with LBP codes. The experimental results show the proposed method achieves a high visual quality with 47 dB PSNR and 0.989 SSIM for 144501 secret bits capacity for test images. The proposed method has comparable results with the literature in terms of quality, security, and capacity.

***Keyword:*** Data Hiding, Local Binary Pattern, Texture Features, Information Security

## INTRODUCTION

The development of the internet and communication technologies makes media files very popular. Every day billions of multimedia objects are shared between internet users. Data hiding is the art of secret communication with these classical cover media. The secret message is embedded into cover files as image, video and audio with an data hiding algorithm (Konyar et al 2020, Kaçar et. al. 2022, Altınbaş et al. 2021). The stego file contains secret message and shared with the receiver via communication channel. The receiver extracts secret message with a known extracting algorithm. The most important advantage of the data hiding is the invisiblity of the message with a naked eye.

Images are the most popular carrier cover files for data hiding. The image-based data hiding can be classified into two types according to the secret message embedding, spatial domain, and transform domain. In the spatial domain application bit wise embedding methods as the least significant bit substitution (LSB), and pixel-wise embedding methods as pixel value differencing are widely used (Mandal et al 2022, Rahman et al 2022, Konyar 2022). In the transform domain application, the cover image is transformed with popular image transform methods (Zhang 2022, Alotaibi 2019). Secret message bits are embedded into the transform coefficients of the images.

Many data hiding methods have been presented in the literature in terms of different algorithms for images. These algorithms aim to achieve better capacity, visual quality, or security. In the last decade, local binary pattern (LBP) based algorithm based method was introduced (Wenyin 2011, Chang 2013, Singhal 2016,). LBP is one of the important texture feature extractors and used for statistical definiti-

on of the images. In accordance with the LBP logic, most of the data hiding algorithms in the current studies divide the image into blocks. Each existing study combines spatial domain or transform domain approaches with LBP. In the (Chang 2013), it is proposed to detect the tamper and secret watermark recovery. They used LBP to generate the authentication information for data embedding. In the (Zhang et al 2017), the LBP is used for blind tamper detection. The LSB of the cover image are substituted by the encrypted watermark. The encryption of the secret data is done with Arnold transform and logistic map chaotic encryption methods. In the methods of the (Ali et al. 2018), it was proposed a zero watermarking method and determines the characteristics of audio samples with the One-Dimensional LBP operator. In the (Rahman 2018) LBP is used to generate a binary matrix from the low frequency component of the integer wavelet transform of the image to embed secret message. In the method of (Tuncer 2018) center symmetric LBP based data hiding method is proposed. The LBP bits are generated from 4 × 4 non-overlapping blocks of high frequency component of the integer wavelet transform of the cover image. In the (Pal et al. 2019) LBP-based dual image-based method is proposed. The cover image is divided into 3 × 3 non-overlapping blocks. Then the LBP code generated from the blocks and perform ex-or with secret bits. Two bits verification code is generated from the LBP code vector and embedded into the dual image.

In the (Chakraborty 2018) 8 secret bits embedded in the local neighborhood of the cover image. Their method calculates the LBP code and encrypted the secret message bits with the LBP code. The encrypted and shuffled bits embed to the LSB of each neighbor pixel. The methods claim to develop a blind method. However, in their method, the LBP code of the data extraction side can be suffered from the data embedding process. Because secret message bits are obtained from LBP code and LSB values of the 3x3 blocks. But, during the message embedding, it is possible to change the LSB of each pixel of the block. When the pixels changed, it is possible to change LBP code. Then, the receiver may not extract the true bits.

In the proposed method of this study, a distance-based LBP code generation method is used. Also, secret bits embed into unused pixel of the sub-blocks. This method provides high capacity and keep the LBP code during the secret data embedding and extracting process.

**MATERIAL and METHODS**

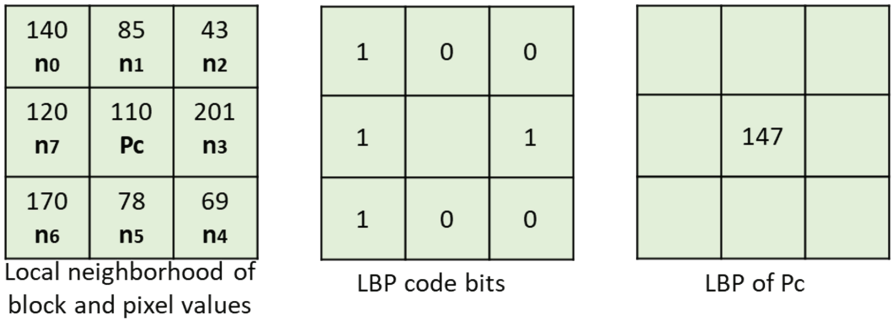
The LBP is one of the important texture feature extractors and was proposed by (Ojala et al. 1996). The LBP has been widely used for many texture-based applications. With this approach, the spatial relationship between the neighbor pixel and the center pixel is compared. The LBP of a block calculates the pixel values of block center Pc and its neighbors $n_t$. As defined in Equation 1, if any pixel value is larger than the center pixel value or equal than the corresponding code bit is assigned as 1, otherwise the bit is assigned as 0. Each bit for all pixels is calculated and from a pre-defined position of the block LBP code is generated. For a block with radius R and with T pixels against center pixel around Pc the LBP is calculated as follows:

$$LBP_{T,R}(c) = \sum_{t=0}^{T-1} sign(n_t - Pc) \times 2^t \qquad (1)$$

$$sign(x) = \begin{cases} 1 & x \geq 0 \\ 0 & x < 0 \end{cases}$$

where n denotes neighbors of the center pixel. The R value is 1 and T value is equal to 8 bits for a 3x3 block. If the block size increases T and R values increases accordingly. An example of the classical LBP code generation is given in Figure 1.

**Figure 1. Code generation example for classical LBP**




In this paper instead of the classical LBP, it is proposed to use a version of distance based LBP of neighbor pixel (Kaya 2015). In this method, LBP code is generated depends on the relationship of neighbor pixels with each other. Assume we have a 3x3 block, then the neighbor pixel array is n={n0, n1, n2, n3,n4, n5, n6, n7}. The LBP code for distance d=1 is obtanied with comparison of each pixel with its next neighbor pixel as follows:

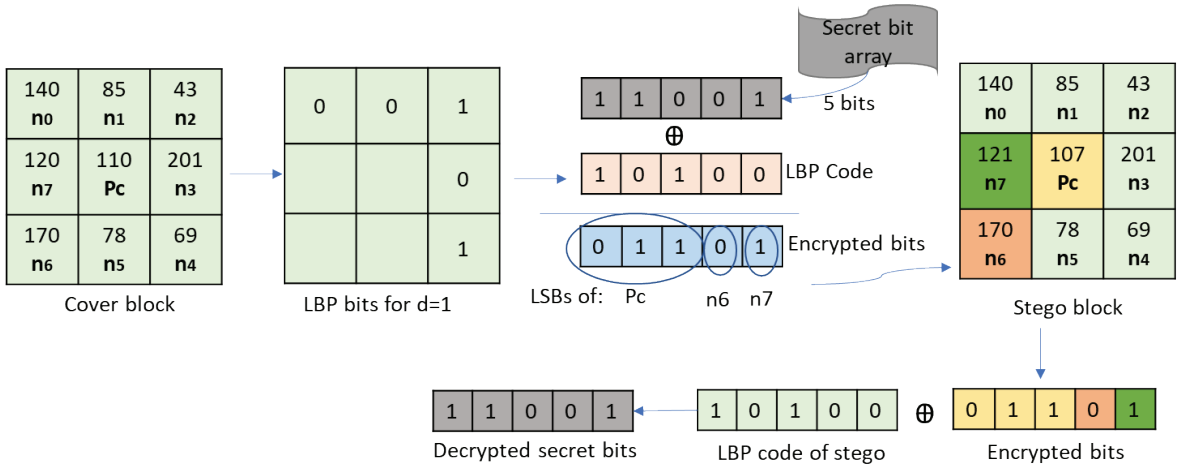
$$LBP_{d=1}(c) = \sum_{t=0}^{T-1} f(n_{t+1} - n_t) \times 2^t$$

$$f(x) = \begin{cases} 1 & x > 0 \\ 0 & otherwise \end{cases} \quad (2)$$

Proposed study aims to keep the visual quality of stego image while the secret bit capacity increases. So, a new embedding strategy is developed for this method. Instead of 8 bits LBP, for each non-overlap 3x3 cover block it is calculated a 5 bits LBP code for d=1. The secret message with 5 bits length and the LBP code is encrypted with logical ex-or operation (⊕). The output of ex-or operation is embedded into unused pixels of the block namely Pc, n6, n7. The 5 bit array is embedded to 3 LSBs of center pixel, 1 LSB of n6 and 1 LSB of n7 respectively. All non-overlapped 3x3 blocks operated with secret message array and the stego image is obtained. The stego image sends to the receiver via communication channel.

The data extraction strategy of the proposed method is similar with embedding. On the receiver side, for each non-overlapped 3x3 blocks the 5 bits encrypted secret messages extracted from 3 LSBs of center pixel, 1 LSB of n6 and 1 LSB of n7 respectively and combined. The LBP code for 5 bits length is calculated with Equation 2. The encrypted secret message and LBP codes decrypted with logical ex-or operation and secret message is obtained.

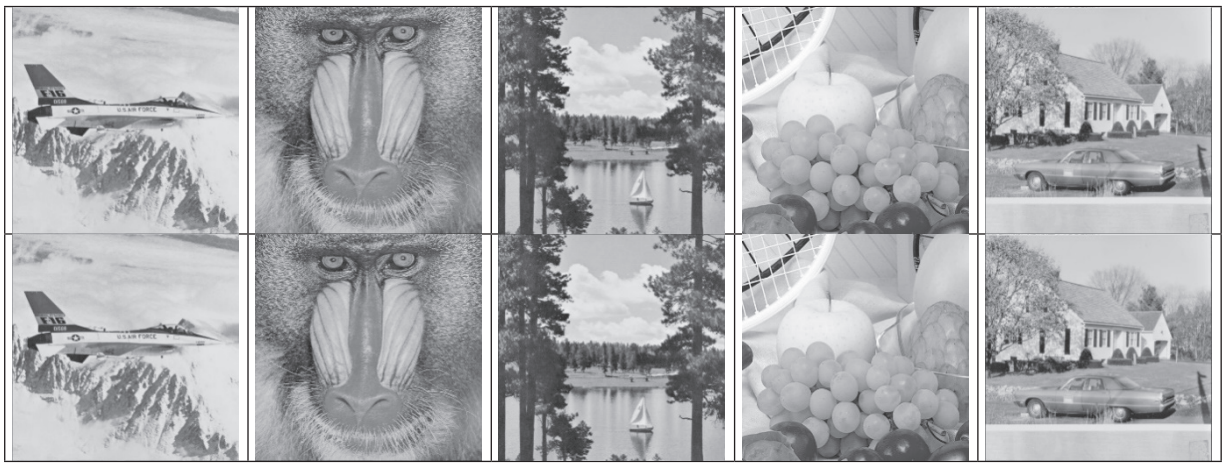
**Figure 2. Secret message embedding and extraction of proposed method**




## EXPERIMENTAL RESULTS

The proposed method evaluated with 6 common 512x512 grayscale test images, Airplane, Baboon, Boat, Fruits, and House. A binary bit stream was used as secret message. The performance of the proposed method is evaluated with qualitative and quantitative methods. The first evaluation of the proposed method is based on qualitative methods. In this method the visual quality of the cover image and stego images compared. The cover and stego images are given in the Figure 3. It is clearly seen from Figure 3, there is not any important distortion of the stego images.

**Figure 3. Original cover images (above) and the stego images (below).**



The second evaluation of the proposed method is a quantitative method with Peak Signal-Noise Ratio (PSNR), and secret message embedding capacity. The goal of the data hiding is sending the stego image to the receiver with higher secret bits. However, the visual quality of the stego image must not decrease. The PSNR, one of the most known visual quality metric is used for quantitative evaluation of secret message carrier image namely stego. The PSNR results obtained for different embedding levels. The higher value is also the higher embedding capacity of the proposed method. The results were also checked according to half and quarter capacity. The PSNR results of the proposed method are given in Table 1 according to the embedding capacity. PSNR value achieves 47 dB for higher capacity 144501 bits. When the embedding capacity is reduced, the mean PSNR value increases and achieves 50dB for 72250 bits, and 53dB for 36125 bits.

**Table 1. Objective evaluation results of the proposed method for test images.**

| Test Images | PSNR (dB) | Capacity (bits) | PSNR (dB) | Capacity (bits) | PSNR (dB) | Capacity (bits) |
|---|---|---|---|---|---|---|
| Airplane | 47.15 | 144501 | 50.13 | 72250 | 53.19 | 36125 |
| Baboon | 47.09 | 144501 | 50.14 | 72250 | 53.13 | 36125 |
| Fruits | 47.18 | 144501 | 50.23 | 72250 | 53.28 | 36125 |
| Lena | 47.13 | 144501 | 50.11 | 72250 | 53.09 | 36125 |
| Boat | 47.06 | 144501 | 50.10 | 72250 | 53.14 | 36125 |
| House | 47.06 | 144501 | 50.00 | 72250 | 53.05 | 36125 |

## CONCLUSION

This paper proposed to use a modified LBP-based data hiding for images. In the proposed method secret message bits are encrypted with distance-based LBP codes and embed in the 3x3 non-overlapped blocks. Each block contains five secret bits, where three of them embeds in the three LSBs of the center pixel of the block, and the remaining two bits are embedded in one LSBs of two neighbor pixels. The proposed method, tested with common test images in terms of subjective and objective metrics. The obtained results are remarkable and have a potential for improvement in future works.

## ACKNOWLEDGEMENTS

The author would like to acknowledge the support of Kocaeli University Software Technologies Research (STAR) Laboratory for this study.

## REFERENCES

Kaçar, S., Konyar, M. Z., & Çavuşoğlu, Ü. (2022). 4D chaotic system-based secure data hiding method to improve robustness and embedding capacity of videos. *Journal of Information Security and Applications*, 71, 103369.

Konyar, M. Z., & Öztürk, S. (2020). Reed Solomon coding-based medical image data hiding method against salt and pepper noise. *Symmetry*, 12(6), 899.

Altinbaş, A. E., & Yalman, Y. (2021, September). Bit Reduction Based Audio Steganography Algorithm. *In 2021 6th International Conference on Computer Science and Engineering (UBMK)*, pp. 703-706, IEEE.

Mandal, P. C., & Mukherjee, I. (2022). High-capacity data hiding based on multi-directional pixel value differencing and decreased difference expansion. *Multimedia Tools and Applications*, 81(4), 5325-5347.

Rahman, S., Uddin, J., Khan, H. U., Hussain, H., Khan, A. A., & Zakarya, M. (2022). A novel steganography technique for digital images using the least significant bit substitution method. *IEEE Access*, 10, 124053-124075.

Konyar, M. Z., (2022, December). Reversible Data Hiding Method Based on Double-Side Histogram Shifting of Image Sub-Blocks. *In 2022 9th International Marmara Sciences Congress (Imascon 2022 Autumn)*, pp. 1-5, Kocaeli, Türkiye.

Zhang, H., Sun, S., Hu, L., & Meng, F. (2022). A novel data hiding scheme based on improved diamond encoding in IWT domain. *Multimedia Tools and Applications*, 1-19.

Alotaibi, R. A., & Elrefaei, L. A. (2019). Text-image watermarking based on integer wavelet transform (IWT) and discrete cosine transform (DCT). *Applied Computing and Informatics*, 15(2), 191-202.

Singhal A, and Bedi P (2016) Local binary pattern operator-based steganography in wavelet domain. 2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI).

Wenyin, Z., & Shih, F. Y. (2011). Semi-fragile spatial watermarking based on local binary pattern operators. *Optics Communications*, 284(16-17), 3904-3912.

Chang, J. D., Chen, B. H., & Tsai, C. S. (2013, February). LBP-based fragile watermarking scheme for image tamper detection and recovery. *In 2013 international symposium on next-generation electronics* (pp. 173-176). IEEE.

Zhang, H., Wang, C., & Zhou, X. (2017). Fragile watermarking based on LBP for blind tamper detection in images. *Journal of Information Processing Systems*, 13(2), 385-399.

Ali, Z., Imran, M., Alsulaiman, M., Zia, T., & Shoaib, M. (2018). A zero-watermarking algorithm for privacy protection in biomedical signals. Future Generation Computer Systems, 82, 290-303.

Rahman, S., Saha, C., & Tamal, T. A. (2018). Integer wavelet transform based dual watermarking technique using tent map and local binary pattern. *Global Journals of Research in Engineering*, 18(F3), 33-41.

Tuncer, T., & Kaya, M. (2019). A novel image watermarking method based on center symmetric local binary pattern with minimum distortion. *Optik*, 185, 972-984.

Pal, P., Jana, B., & Bhaumik, J. (2019). Watermarking scheme using local binary pattern for image authentication and tamper detection through dual image. *Security and Privacy*, 2(2), e59.

Chakraborty, S., & Jalal, A. S. (2020). A novel local binary pattern based blind feature image steganography. *Multimedia Tools and Applications*, 79, 19561-19574.

Ojala, T., Pietikäinen, M., & Harwood, D. (1996). A comparative study of texture measures with classification based on featured distributions. *Pattern recognition*, 29(1), 51-59.

Kaya, Y., Ertuğrul, Ö. F., & Tekin, R. (2015). Two novel local binary pattern descriptors for texture analysis. *Applied Soft Computing*, 34, 728-735.