# Postprint: A Lossless Information Hiding Algorithm Based on Difference Histogram Shifting of LBP Face Texture Features

**Authors:** Zhang Tao, Liu Yunong, Ren Shuai, He Yuan, Xu Zhenchao, Wang Zhen, Mu Dejun

**Date:** 2019-05-10T00:00:00+00:00

## Abstract

To address the inherent contradiction between increasing embedding capacity and enhancing robustness in information hiding algorithms, a multi-carrier information hiding algorithm is proposed. This approach employs multiple facial expression images as carriers, utilizing Local Binary Pattern (LBP) texture features to identify facial expression regions for embedding encrypted information. The adjacent pixel difference matrix of the carrier region is computed, and embedding space is constructed by shifting the histogram of corresponding elements in the difference matrix, thereby achieving reversible hiding of encrypted information and lossless recovery of the carrier image. Algorithmic analysis demonstrates that the proposed method offers superior embedding capacity compared to existing algorithms while maintaining high robustness, achieving a maximum embedding capacity of 0.561 with a Peak Signal-to-Noise Ratio (PSNR) of 38.421 dB, with the PSNR value in the identified embedding region reaching 46.286. Robustness experiments reveal that under filtering attacks, the algorithm maintains a similarity greater than 99% with the original information image; when subjected to cropping and translation attacks, the Normalized Correlation (NC) coefficient of the secret image reaches minimum values of 0.743 and 0.728, respectively, which substantially exceeds that of other algorithms. Comparative experimental results with alternative methods validate the effectiveness of the proposed algorithm.

## Full Text

## Preamble

**Differential Histogram Shift Lossless Information Hiding Algorithm Based on LBP Facial Texture Features**

Zhang Tao[1] , Liu Yunong[1] †, Ren Shuai[1] , Zhang Degang[2]
(1. a. School of Electronic & Control Engineering; b. School of Information Engineering, Chang' an University, Xi' an 710068, China; 2. Education Training Evaluation Center, Yunnan Power Grid Co., Ltd., Kunming 650033, China)

**Abstract:** To address the trade-off between embedding capacity and robustness in information hiding algorithms, this paper proposes a multi-carrier information hiding algorithm. Multiple facial expression images are used as carriers, with Local Binary Pattern (LBP) texture features employed to identify facial expression regions for embedding encrypted information. The algorithm calculates the adjacent pixel difference matrix of the carrier region and constructs embedding space by shifting the histogram of corresponding elements in the difference matrix, thereby achieving reversible concealment of encrypted information and lossless recovery of carrier images. Algorithm analysis demonstrates superior performance over existing methods, with a maximum embedding capacity of 0.561 while maintaining a Peak Signal-to-Noise Ratio (PSNR) of 38.421 dB, and the PSNR in identified embedding regions reaches 46.286. Robustness experiments show that under filtering attacks, the similarity to the original information image exceeds 99%; when facing cropping and translation attacks, the Normalized Coefficient (NC) of the secret image reaches minimum values of 0.743 and 0.728 respectively, significantly outperforming other algorithms. Comparative experimental results validate the effectiveness of the proposed algorithm.

**Keywords:** lossless information hiding; multi-carrier; local binary pattern; difference matrix; histogram shift

## 0 Introduction

With the development of IoT, big data, social networks, and virtual reality technologies, techniques for transmitting confidential information using human behavior and objective 事物描述信息 as carriers have grown rapidly. Resolving the contradiction between large-capacity secret information and embedding algorithm robustness has become a mainstream research direction. The inevitable problem of using multiple carriers for information hiding is categorized as multi-carrier information hiding and joint analysis. Ker investigated three strategies: carrier counting analysis, average joint analysis, and generalized likelihood ratio testing [1], studied game equilibrium regarding threshold selection in carrier counting analysis [2], proved that multi-carrier secure embedding capacity is proportional to the square root of carrier quantity rather than carrier quantity itself [3], and that single-carrier secure embedding capacity is proportional to the square root of carrier size [4], subsequently proposing multi-carrier hiding strategies that minimize KL divergence [5].

Addressing the problems of small hiding capacity and low security in single-carrier information hiding algorithms, recent multi-carrier based schemes in-

clude: 文献 [6] proposed a multi-carrier sharing steganography algorithm based on Bernstein polynomials, providing larger embedding space for secret information, but the shared carrier images exhibited strong correlations, resulting in robustness only against specific attacks; 文献 [7,8] proposed a multi-image hiding scheme based on error diffusion, using uncorrelated images as carriers and dispersing quantization errors to neighboring pixels, achieving good visual effects, but the extracted information differed from the original image, and loss of any shared image prevented secret information extraction; 文献 [9] proposed a fixed blocking based multi-carrier dispersed information hiding algorithm.

While mainstream embedding algorithms still employ single-carrier hiding methods, multi-carrier information hiding effectively resolves the contradiction between carrier embedding capacity and algorithm robustness. This paper proposes a novel multi-carrier information hiding algorithm based on Local Binary Pattern (LBP) facial expression recognition [10] regions. In multiple facial expression images, block matching determines the motion vectors of facial expression features, and Principal Component Analysis (PCA) generates a low-dimensional subspace from these vectors, termed the feature motion space [11]. Using automatically recognized expression motion feature spaces, differential histogram shifting adjusts pixel values in the feature space to embed preprocessed encrypted information [12]. Experiments demonstrate that after embedding encrypted information, the stego expression images maintain original facial expressions due to large embedding space, and exhibit good robustness against cropping, Gaussian noise, and rotation attacks. Using inverse differential histogram shifting to extract encrypted information yields expression images and information images identical to the original carriers, thereby achieving lossless information hiding with large embedding capacity across multiple carriers.

## 1 Facial Expression Feature Region Recognition

Multi-carrier information hiding technology has increased computational complexity compared to single-carrier algorithms but effectively solves the difficulty of improving embedding capacity [13]. This paper selects four different expression images from the JAFFE (Japanese Female Facial Expression) database. The expression feature region extraction steps are:

(a) Valley-peak image (b) General feature block (c) Main feature block (d) Information embedding region

[Figure 3: see original paper] Encrypted information embedding area selection

e) Repeat steps a)~d) to extract encrypted information embedding regions for the other three facial expression images.

## 2 Secret Information Preprocessing

In this algorithm, a 128×128 binary fingerprint image S is selected as secret information and segmented into four sub-images S1, S2, S3, and S4 of equal

size.

[Figure 4: see original paper] Original secret image and segmented sub-image

a) Adjust the facial region in the original expression images to 512×512 size, with four expression carriers represented as C1, C2, C3, C4.

[Figure 1: see original paper] Image of the emoticon after resizing

b) Extract expression texture features through LBP. Select a 3×3 matrix, and according to the LBP transformation formula (1), traverse the entire image using the center pixel value as threshold to perform matrix transformation as shown in [Figure 2: see original paper], obtaining LBP feature textures that clearly reflect local expression details.

Scrambling encryption disrupts image pixel order, effectively removing pixel correlations to enhance secret information security during transmission. The segmented secret information sub-images undergo Logistic map chaotic scrambling. While one-dimensional Logistic map and super Logistic map exist, a quantum Logistic map has been proposed [14] with complex nonlinear dynamics characteristics. To simplify computational complexity, in the one-dimensional Logistic map iteration formula (3), setting parameters =3.99 and initial value x =0.5 yields a non-periodic, non-convergent chaotic sequence after n iterations, with larger n values producing higher scrambling effectiveness.

where: [0,4], x (0,1). [Figure 5: see original paper] shows the secret information sub-images S1l, S2l, S3l, S4l after Logistic map scrambling, demonstrating that the secret information has lost its original texture features.

where: (x_c, y_c) is the center pixel of the 3×3 matrix, i_p, i_c are neighborhood pixels, s(x) is the sign function defined as:

[Figure 5: see original paper] Secret information Logistic map scrambling

## 3 Embedding Algorithm

(a) Local region (b) Region pixel matrix (c) LBP transformation matrix (d) Facial texture features

[Figure 2: see original paper] LBP facial expression texture feature extraction

c) Based on the feature texture images from step b), perform binarization to obtain valley-peak images (Figure 3: see original paper). Use block matching to determine motion vectors of the expression face, and apply Principal Component Analysis (PCA) to generate low-dimensional subspaces from these vectors, obtaining general feature regions R1, R2, R3, R4.

d) Select important feature regions from R1, R2, R3, R4 as embedding space for encrypted information, choosing the largest region R4 as the embedding area.

This paper adopts a multi-carrier approach. Kittawi et al. [15] proposed constructing redundant space using histogram shifting of carrier images to embed hidden information, but direct histogram shifting creates limited redundant space, preventing higher information embedding capacity. 文献 [16,17] proposed reversible data hiding using median difference histograms, achieving blind extraction of hidden information by modifying two selected regions and preserving histogram midpoints, with good visual results. Based on the algorithm in [16], this paper proposes an information embedding algorithm using differential histogram shifting, which constructs redundant space using the histogram of adjacent pixel differences, increasing embedding space and enabling lossless extraction of both carrier images and secret information.

### 3.1 Calculating Adjacent Pixel Differences

Define carrier image C{C1, C2, C3, C4} as an M×N 8-bit grayscale image, with C(i,j) representing the pixel value at position (i,j). Calculate adjacent pixel differences in the column direction row by row, expressed as:

where: 1 i M, 1 j N-1. Row-direction adjacent pixel differences are:

where: 1 i M-1, 1 j N. [Figure 6: see original paper] shows grayscale histograms and pixel difference histograms for carrier images C1 and C3:

C1 grayscale histogram C1 adjacent pixel difference histogram C3 grayscale histogram C3 adjacent pixel difference histogram

[Figure 6: see original paper] C1, C3 gray histogram and pixel difference histogram

In [Figure 6: see original paper], the adjacent pixel difference histograms of carrier images C1 and C3 exhibit Laplacian distribution. C1' s grayscale histogram peak is 9762, while the adjacent pixel difference value at "0" is 42592; C3' s histogram peak is 12063, with the pixel difference at "0" being 55776. The adjacent pixel difference peaks are significantly larger than grayscale histogram peaks, indicating that larger redundant space for information embedding can only be constructed between adjacent pixels with identical values.

### 3.2 Secret Information Embedding

Either column-direction pixel differences can be calculated row by row or row-direction differences column by column. To simplify algorithm complexity, column-direction pixel differences are selected to construct redundant space, denoted as D=Dl being the difference matrix. Perform row adjustment on difference matrix D as shown in [Figure 7: see original paper] to construct redundant space, where is the absolute pixel difference value.

a) When =0, information is embedded between adjacent pixels with identical values. Scan the difference matrix D in raster order, applying transformation (6) to each element, which eliminates elements with value 1 from the

difference matrix.

b) When >0, information is embedded in pixels with adjacent differences of ± . Scan difference matrix D in raster order, keeping elements outside [- , ] unchanged while modifying only elements within [- , ] according to the following rules. During this histogram shifting process, the histogram of pixel difference values greater than shifts right (or left) by 1 position, resulting in no elements with value ±1 in matrix D .

Based on the above steps, obtain the adjusted adjacent pixel difference matrix D and embed encrypted information b. Scan D in raster order, embedding b in all elements with values - -1 and +1. The pixel difference matrix after information embedding is D , with embedding rules as follows:

The stego image after embedding encrypted information is:

where: 1 i M, 1 j N-1. Since the difference matrix size is M×(N-1) while the carrier image size is M×N, the extra last column serves as reference pixels for secret information extraction and remains unchanged before and after embedding. The secret information embedding program implementation flow is shown in [Figure 8: see original paper].

(a) =0 (b) >0

[Figure 7: see original paper] Pixel difference histogram adjustment

[Figure 8: see original paper] Data embedding program flow chart

### 3.3 Secret Information Extraction

Data extraction and image recovery are inverse processes of data embedding. First, calculate the column-direction adjacent pixel difference matrix from the stego carrier image from right to left. Since the last column elements remain unchanged before and after extraction, C(i,N)=CS(i,N) for i [1,M], calculate the adjacent pixel difference matrix based on C(i,N). As the encrypted information to be embedded is a binary bitstream, denote the embedded information bit value as b. Scan matrix D in raster order, using 0 elements in the matrix according to formula (7).

where: 1 i M, 1 j N-1. Recover the carrier image difference matrix D based on the absolute value of adjacent pixel differences, divided into two cases: =0 and >0.

a) When =0, for information embedded where adjacent pixel differences are 0. Scan D in raster order: if the scanned element value is 0, extract hidden information value "0" ; when the scanned element is 1, extract hidden information value "1" and set the element value to 0; when the scanned element is greater than 1, decrease the element value by 1. The carrier image pixel difference matrix is recovered as follows:

b) When >0, extract information embedded using pixels with difference values - and . Scan D : if matrix elements have values - or , extract embedded information "0" ; if matrix elements have values - -1 or +1, extract embedded information "1" and adjust corresponding element values by adding 1 or subtracting 1; if element values are greater than +1 or less than - -1, adjust corresponding element values by subtracting 1 or adding 1. The extraction rules are as follows:

Recover the carrier image C based on the obtained adjacent pixel difference matrix:

where: 1 i M, 1 j N-1.

The secret information embedding process performs C(i,j)+1 or C(i,j)-1 operations on partial pixel values, inevitably causing underflow (C(i,j)<0) or overflow (C(i,j)>255). Therefore, pixels with C(i,j)<0 are set to 0, and pixels with C(i,j)>255 are set to 255 to resolve overflow/underflow issues. The secret information extraction program implementation flow is shown in [Figure 9: see original paper].

[Figure 9: see original paper] Data extraction program flow chart

### 3.4 Embedding Algorithm Experiments

For facial expression carrier images C{C1, C2, C3, C4}, the mouth region of 225×144 size extracted through LBP texture features is used to embed Logistic map scrambled encrypted information Sl{S1l, S2l, S3l, S4l}, obtaining stego carriers CS{CS1, CS2, CS3, CS4}. Apply the recovery procedure from Section 3.3 to extract secret information S {S1 , S2 , S3 , S4 } and recover carrier images C {C1 , C2 , C3 , C4 }. Comparison shows that the differential histogram shifting embedding algorithm does not alter carrier image texture features after information embedding, and since the embedding region is where expression feature motion energy is high, facial expressions remain unchanged. Using inverse differential histogram shifting to extract encrypted information yields lossless carrier expression images, and inverse scrambling recovers recognizable secret information.

Peak Signal-to-Noise Ratio (PSNR) is a quantitative metric measuring distortion between original and stego images. PSNR values reflect secret image embedding quality. [Figure 11: see original paper] examines the relationship between embedding capacity and PSNR for carrier images C1, C2, C3, C4.

[Figure 10: see original paper] Secret information embedding and recovery

**Table 1** Carrier image distortion detection

| Max capacity (dpp) | Min capacity (dpp) | PSNR(max)/dB | PSNR(min)/dB |
|---|---|---|---|

The differential histogram shifting embedding algorithm constructs large embedding space. In the designated expression region, when carrier C3 reaches maximum embedding capacity of 0.563, PSNR(C3)max=46.286, demonstrating excellent embedding performance and imperceptibility. However, maximum embedding capacity inevitably reduces robustness. In [Figure 11: see original paper], as effective embedding capacity increases, PSNR decreases, with PSNR(C1)min=36.485. **Table 1** data shows average maximum embedding capacity and corresponding PSNR values of 0.557/37.403, and average minimum embedding capacity and corresponding PSNR values of 0.122/45.823. Data analysis reveals that when embedding capacity reaches 0.55, peak signal-to-noise ratio still achieves 37, indicating high similarity between stego carrier images and original expression images.

Comparing algorithm performance with reference algorithms using 512×512 carrier images, Yang et al.'s algorithm employs median difference histogram shifting to construct high embedding space, with maximum embedding capacity of 0.214 and PSNRmax=49.532. The proposed algorithm also uses differential histogram shifting for secret information embedding, achieving higher PSNR values than other algorithms when embedding capacity exceeds 0.318, with slower distortion variation as embedding capacity increases, demonstrating superior robustness. Wu et al.'s image sharing algorithm suffers from large correlation between carrier images, causing significant distortion after embedding with PSNRmax=24.719.

**Table 2** Algorithm performance comparison

| Algorithm | PSNR/dB | Embedding capacity |
|---|---|---|
| Cheng et al. | | |
| Wu et al. | | |
| Kittawi algorithm | | |
| Yang et al. | | |

## 4 Robustness Experiments

Robustness is primarily evaluated through unauthorized embedding attacks such as spatial filtering, lossy compression, and geometric deformation [18], examining the recovery degree of extracted secret information. The normalized correlation coefficient between extracted and original secret information serves as the robustness evaluation standard:

where w_i and ŵ_i are pixel points of original and extracted secret information, T is a predetermined threshold. Experiments show that when T=0.6, the extracted secret information···

### 4.1 Spatial Filtering Robustness Experiments

Perform mean filtering, Gaussian filtering, Laplacian filtering, Gaussian-Laplacian filtering, median filtering, and Gaussian noise attacks on stego

carrier images CS{CS1, CS2, CS3, CS4}, extracting and recovering encrypted information. NC values for carrier CS1 under filtering attacks are shown in **Table 3**.

**Table 3** The NC value of carrier CS1 under spatial filtering attack

| Attack type | Encrypted info S1 | Encrypted info S2 | Encrypted info S3 | Encrypted info S4 | Average NC |
|---|---|---|---|---|---|
| Mean filter | 0.9987 | 0.9985 | 0.9986 | 0.9987 | 0.9986 |
| Gaussian filter | 0.9988 | 0.9989 | 0.9993 | 0.9987 | 0.9989 |
| Laplace filter | 0.9992 | - | - | - | - |
| Gaussian-Laplace filter | 0.9993 | - | - | - | - |
| Median filter | 0.9986 | - | - | - | - |
| Add Gaussian noise | 0.9985 | - | - | - | - |

[Figure 12: see original paper] CS1 Spatial filtering attack

**Table 3** data shows that after preprocessing secret information, NC values remain above 0.99 under spatial filtering attacks, far exceeding the NC threshold of 0.6. Maximum NC values of 0.9990 are achieved under Laplacian filtering and Gaussian noise attacks, demonstrating 99% similarity between recovered encrypted information and original information after spatial filtering attacks, thus exhibiting excellent resistance to spatial filtering attacks.

### 4.2 Geometric Attack Robustness Experiments

Perform translation, cropping, and scaling attacks on stego carrier images CS, extract encrypted information to calculate NC values, and compute the average NCS value:

**Table 4** NC mean of translational attack

| NC value | Translation amount | NC value | Translation amount |
|---|---|---|---|

**Table 5** NC mean of shear attack

| Cropping % | NC value | Cropping % | NC value | Cropping % | NC value |
|---|---|---|---|---|---|

**Table 6** NC Mean of Scaling Attacks

| NC value | Scaling ratio |
|---|---|

[Figure 13: see original paper] Translational attack algorithm performance experiment

[Figure 14: see original paper] Shear attack algorithm performance experiment

[Figure 15: see original paper] Scaling attack algorithm performance experiment

Robustness experiments against geometric deformation attacks show: in **Table 4**, when translation amount=500, the extracted secret information NC value is 0.698; in **Table 5**, when cropping degree=50%, extracted secret information NC=0.728; in **Table 6**, when carrier image scaling ratio is 0.2, NCmin=0.691, with NCmin>0.6, thus extracted secret information maintains high recognizability with minimal geometric attack damage. Algorithm performance comparison shows: in [Figure 13: see original paper], Kittawi et al.' s algorithm demonstrates high robustness against translation attacks, but the proposed algorithm surpasses Kittawi' s algorithm when translation amount>405; in [Figure 14: see original paper] cropping attack comparison, the proposed algorithm outperforms Kittawi' s algorithm when cropping degree<28.5%, though it is weaker than Cheng et al.' s algorithm, but superior to other algorithms when cropping degree>40%. Data analysis confirms that the proposed algorithm exhibits advantageous robustness against geometric attacks, maintaining high recognizability of extracted information.

## 5 Conclusion

This paper proposes a multi-carrier lossless information hiding algorithm based on differential histogram shifting in the LBP facial texture feature domain. LBP texture features extract and identify mouth expression regions of the face. Secret information consists of a original secret image segmented into four equally-sized sub-images, encrypted through Logistic map chaotic scrambling. In fixed-size expression regions, adjacent pixel differences of carrier images are calculated to obtain difference matrices, and matrix histograms are adjusted according to algorithm rules to construct embedding space for binary encrypted information, with secret information losslessly extracted and carrier images recovered through the inverse process. Experiments demonstrate that the multi-carrier embedding algorithm achieves embedding capacity of 0.561 while maintaining PSNR of 38.421, addressing the limited embedding capacity of single images.

Robustness experiments show that the differential histogram shifting embedding algorithm effectively resists spatial filtering and geometric deformation attacks, with performance comparisons revealing significant advantages in attack resistance and robustness over other algorithms.

## References

[1] Ker A D. Batch steganography and pooled steganalysis [C]//Proc of the 8th Information Hiding Workshop. 2006: 265-281.

[2] Ker A D. Batch steganography and the threshold game [C]//Proc of SPIE: Security, Steganography, and Watermarking of Multimedia Contents. 2007: 401-413.

[3] Ker A D. A capacity result for batch steganography [J]. IEEE Signal Processing Letters, 2007, 14(8): 525-528.

[4] Filler T, Ker A D, Friderich J. The square root law of steganographic capacity for markov covers [C]//Proc of SPIE: Security, Steganography, and Watermarking of Multimedia Contents. 2009: 18-22.

[5] Ker A D. Steganographic strategies for a square distortion function [C]//Proc of SPIE: Security, Steganography, and Watermarking of Multimedia Contents. 2008: 681904. 1-13.

[6] Chen Gouxi, Shen Honglei, Wu Yuliang, et al. Research on multi-carrier image separation and steganography algorithm [J]. Computer Engineering, 2012, 38(4): 116-118.

[7] Wu Xiaotian, Sun Wei. Image sharing scheme based on error diffusion [J]. Journal of Computer Applications, 2011, 31(1): 74-77+81.

[8] Ou Zhengying, Wu Xiaotian, Cheng Binyi, et al. (2,n) XOR image separation scheme based on flip operation [J]. Journal of Graphics, 2015, 36(1): 56-61.

[9] Liang Wei, Jiang Yan, Peng Li, et al. A fixed blocking based dispersed information hiding algorithm for multiple carriers [J]. Journal of Computational & Theoretical Nanoscience, 2015, 12(10): 3722-3726.

[10] Guo Hefei, Liu Jianfeng, Dong Zhongwen. Face recognition method based on improved LBP algorithm [J]. Modern Electronics Technique.

[11] Peng Sijiang, Dai Houping, Zhou Chengfu, et al. An inter-age face recognition algorithm based on HOG/PCA/SVM [J]. Journal of Jishou University & Natural Science Edition, 2018, 39(5): 24-28.

[12] Zheng Shuli, Xing Huifen, Wang Meiling, et al. Reversible watermarking based on histogram translation and differential histogram [J]. Journal of System Simulation, 2013, 25(11): 2717-2722.

[13] Elshoura S M, Megherbi D B. A secure high capacity full-gray-scale-level multi-image information hiding and secret image authentication scheme via

Tchebichef moments [M]. Elsevier Science Inc., 2013: 531–552.

[14] Luo Yuling, Du Minghui. Image encryption algorithm based on quantum Logistic map in wavelet domain [J]. Journal of South China University of Technology & Natural Science Edition, 2013, 41(6): 53-62.

[15] Kittawi I N, Al-Haj A. Reversible data hiding in encrypted images [C]//Proc of International Conference on Information Technology. Piscataway, NJ: IEEE Press, 2017: 808-813.

[16] Yang H W, Liao I, Chen C C. Reversible data hiding based on median difference histogram [J]. Journal of Information Science & Engineering, 2011, 27(2): 577-593.

[17] Liu, Li, Chang, Chinchen, Wang Anhong. Reversible data hiding scheme based on histogram shifting of n-bit planes [J]. Multimedia Tools and Applications, 2016, 75(18): 11311-11326.

[18] Maloo S, Laskshmi N, Pareek N K. Study of digital watermarking techniques for against security attacks [M]//Information and Communication Technology for Intelligent Systems. 2018: 509-515.

*Note: Figure translations are in progress. See original paper for figures.*