IJICIS, Vol.21, No.1, 95-103
DOI: 10.21608/ijicis.2021.66476.1069

International Journal of Intelligent Computing and Information Sciences

https://ijicis.journals.ekb.eg/

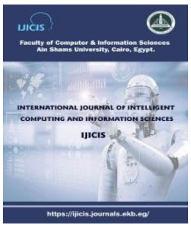

IJICIS
Faculty of Computer & Information Sciences Ain Shams University, Cairo, Egypt.
INTERNATIONAL JOURNAL OF INTELLIGENT COMPUTING AND INFORMATION SCIENCES
IJICIS
https://ijicis.journals.ekb.eg/

IMAGE HIDING USING LOWER-UPPER DECOMPOSITION TECHNIQUE

Reham A. El-Shahed *

Department of Scientific Systems,
Computer and Information Science,
Ain Shams University,
Cairo, Egypt
rehamahmed@cis.asu.edu.eg

M. N. Al-Berry

Department of Scientific Systems,
Computer and Information Science,
Ain Shams University,
Cairo, Egypt
Maryam_nabil@cis.asu.edu.eg

Hala M. Ebeid

Department of Scientific Systems,
Computer and Information Science,
Ain Shams University,
Cairo, 11566, Egypt
halam@cis.asu.edu.eg

Howida A. Shedeed

Department of Scientific Computing,
Computer and Information Science,
Ain Shams University,
Cairo, 11566, Egypt
dr_howida@cis.asu.edu.eg

Received 2021- 03-9; Revised 2021-4-21; Accepted 2021-4-30

Abstract. *Data security is one of the most important sciences nowadays. There is a huge amount of data transferred over the internet each moment and this data should be secured. Steganography is a type data security techniques that is used to hide the secret message into a cover object. Image steganography is the technique that hides an image in another image. This paper proposed a technique that depends on Lower-Upper (LU) decomposition. In the proposed technique LU decomposition is applied for both cover and secret images. The proposed method was tested using some gray and color images. The proposed technique achieved high results with reference to Peak Signal to Noise Ratio (PSNR), Structural Similarity Index Measure (SSIM), and Normalized Cross-Correlation (NCC). The PSNR for the cover image is ranging from 36 to 44 dB. The similarity between the secret image and the extracted image is 100% and the NCC is 1.*

Keywords: *Image Hiding, Steganography, LU factorization*

1. Introduction

* Corresponding author: Reham A. El-Shahed
Department of Scientific Systems, Computer and Information Science, Ain Shams University, Cairo, Egypt
E-mail address: rehamahmed@cis.asu.edu.eg

Information security is an important science nowadays. There are multiple techniques to keep data and information secure over the internet such as cryptography, steganography, and watermarking. Steganography is the art of hiding messages in which the messages are hidden behind a cover file. The cover file may be audio, image or video. The objective of steganography is to hide the secret message in the cover file in such a way that no other one can notice the existence of the hidden secret message. Thus the main components of any steganography algorithm are the cover object and the secret object which are combined to produce the stego-object.

Both steganography and watermarking are using the same algorithms to hide objects, the difference between steganography and watermarking is the purpose of hiding. Watermarking uses hiding techniques to keep the copyright or ownership rights of digital content secured. Steganography keeps the secret data secured for different purposes.

Images are one of the most used objects in social media applications, such as Facebook, Instagram, Pinterest, …etc. So images can be used as cover objects to conceal secret data. Digital images consist of pixels. The value of the pixel represents the intensity or gray-value of the image element at that location.

There are four important properties for any steganography technique, which are imperceptibility, hiding capacity, robustness, and security. First, the imperceptibility is the probability for the Human Visual System (HVS) to detect that there is something invisible in the cover object. The second one is ‘Hiding capacity’, i. e., how much data could be embedded in the cover object. ‘Robustness’ is the third property or concern. This is about the robustness of the steganography technique against problems or distortions that occurs during transmission or compression. The last one is ‘Security’. This means that the algorithm and the key used in hiding should be kept secret [1].

Steganography algorithms process the image on its spatial-domain or in frequency-domain. In the spatial domain, the algorithm inserts the secret message in the pixels directly. The least Significant Bit (LSB) techniques are the most widely used in the spatial-domain techniques. LSB techniques insert the binary message in the least significant bits of the image pixels. This is a simple technique but the imperceptibility is low, so some techniques combine the LSB algorithm with other algorithms to enhance the imperceptibility of the steganography technique.

Transform domain-techniques deals with the cover image after being transformed to another domain.

Discrete Wavelet Transform (DWT) [2], Discrete Fourier Transform (DFT)[3], Discrete Cosine Transform (DCT) [4], Integer Wavelet Transform (IWT)[5], Discrete Curvelet Transform (DCVT) [6], and Stationary Wavelet Transform (SWT) [7] are all types of transforms that can be used in transform-domain techniques. DCT, DWT, and SWT are the most widely used for steganography. DCT provides greater security but the data embedding capacity is less than spatial domain techniques. DWT techniques provide better performance in terms of embedding capacity and robustness [8].

Recent steganography algorithms also used different types of matrix decomposition to enhance the robustness of the steganography algorithms. There are different types of matrix decomposition techniques, such as Singular Value Decomposition (SVD), QR factorization, Lower-Upper (LU) factorization, and Schur decomposition. These techniques are used along with transform-domain techniques to enhance the algorithm.

In this paper, a new image steganography algorithm is suggested. The algorithm depends on LU factorization to hide a grayscale image in a color image.

The rest of the paper is organized as follows; section 2 is a review of some image steganography techniques. Section 3- presents the proposed method and algorithms in detail. Section 4, contains the performance criteria and results. Section 5- concludes the paper.

2. Related work

This is a review section for some image hiding algorithms. Most of the recent algorithms combine transform-domain techniques with matrix decomposition techniques to provide more hiding capacity, robustness, and security.

Vinayagam et al. [9] proposed a watermarking algorithm that hides a watermark image in a host image. The algorithm combined QR decomposition and the LSB technique. The cover image was decomposed into blocks and QR decomposition was applied. The QR matrices were then embedded in the LSB of image pixels. The proposed algorithm greatly improved both tamper localization accuracy and the PSNR of the self-recovered images.

Rawat and Bhandari [10] proposed another algorithm for hiding an image in another image using the enhanced LSB technique. The enhanced technique depended on hiding in the 24-bit color image instead of the ordinary LSB technique that used an 8-bit color image. The Most Significant Bits (MSB) of the secret image was embedded in the LSB of the cover image. Experimental results were measured using PSNR and Mean Squared Error (MSE) and showed that the stego-image is visually indistinguishable from the original cover image in the case of 24 bits.

In [11], Kamaldeep et al. proposed a method of image hiding, which hid the information in a selected pixel and on the next value of the selected pixel. A mathematical function was applied on the 7th bit of the pixels, that generated a temporary variable (pixel $+ 1$). The 7th bit of the selected pixel and the 7th bit of pixel $+ 1$ were used for hiding and extracting information. The performance of the method was checked using PSNR and MSE and then compared to other proposed techniques. This proposed image steganography showed interesting, promising results when compared to other existing techniques.

Combining spatial and frequency domains Gulve and Joshi [12] proposed to use the spatial-domain based techniques to embed the secret message in the frequency-domain. The cover image is transformed to the wavelet domain using IWT. Then the secret information was embedded in the wavelet coefficients using Pixel Value Differencing (PVD) approach. The PSNR values of the algorithm were near to 39.5 which are good and above the threshold of 36 dB after using the full hiding capacity of the cover image. This proved that the stego-images were of good visual quality. Results also showed that the human visual system (HVS) cannot distinguish between the cover image and stego-image.

Using another frequency domain Bhattacharjee and Bandyopadhyay [13] proposed a new image steganography algorithm. First, a pre-processing was applied to the secret image using XOR and shifting operation. Then, a DCT was applied to get the frequency-domain components. At last, the data was embedded within the DCT matrix. This algorithm showed very good results in visual analysis and numerical analysis also i.e. calculation of PSNR and Structural SIMilarity (SSIM).

Kadhim et al. [14] proposed another image steganography algorithm, which used canny edge detection and divided the cover image into blocks. The Dual-Tree Complex Wavelet Transform (DT-CWT) was then applied. The secret image/message was converted to binary and embedded in wavelet coefficients. Experimental results showed that the stego-image achieved good PSNR.

Most of the previously discussed methods achieved good performance in terms of PSNR. But the steganography is still an important open issue; there is a need for more enhancements in the imperceptibility, robustness, and security of the steganography algorithms. This proposed method aims at providing a steganography algorithm with high imperceptibility in terms of PSNR, SSIM, and NCC.

3. Proposed method

The proposed method depends on matrix factorization techniques to hide an image within another image. The cover image is decomposed using LU decomposition. The same matrix decomposition is applied to the secret image and both matrices are embedded using a scaling factor. Inverse multiplication is applied to produce a stego-image. This is shown in Figure 1.

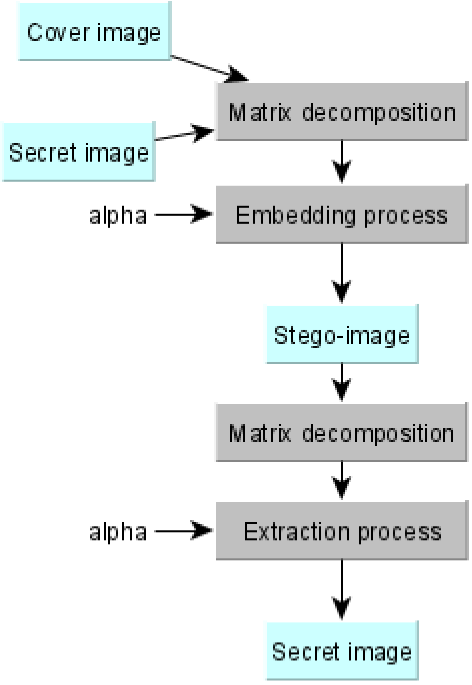


Figure. 1: Block diagram for the proposed algorithm.

3.1. LU factorization

LU factorization is a matrix factorization technique which calculates a matrix as the product of two matrices. The first one is a lower triangular matrix with ones on the main diagonal and the second matrix is an upper triangular matrix. LU decomposes an $n \times n$ non-singular square matrix Ainto a product of matrices L, U as [15]:

$$A = L \times U \tag{2}$$

3.2. Embedding process

Algorithm 1 shows the embedding process steps.

Algorithm 1: Embedding process:

1- Read the cover image A_c

2- Apply matrix decomposition

$$[L_c\,, U_c] = lu\,(A_c) \tag{3}$$

3- Read the secret image A_s

4- Apply same matrix decomposition

$$[L_s\,, U_s] = lu\,(A_s) \tag{4}$$

5- Embed both matrices

$$U_n = U_c + (alpha \times U_s) \tag{5}$$

6- Produce the stego-image

$$si = L_c \times U_n \tag{6}$$

3.3. Extraction process

Algorithm 2 shows the extraction process steps.

Algorithm 2: Extraction process

1- Read the stego-image si

2- Apply matrix decomposition

$$[L_{si}\,, U_{si}] = lu\,(si) \tag{7}$$

3- Extract the embedded matrix

$$U_{new} = \frac{(U_{si} - U_c)}{alpha} \tag{8}$$

4- Output the secret image

$$secim = L_s \times U_{new} \tag{9}$$

4. Results and discussion

4.1. Performance criteria

1- Peak Signal to Noise Ratio

The visual performance of the stego-video and the secret image is measured using PSNR [16]. Structural Similarity Index Measure (SSIM) [16] and Normalized Cross-Correlation [17]. PSNR calculates the ratio between two images. It depends on the Mean Square Error (MSE) in calculations. The MSE is computed as:

$$\text{MSE}=\frac{1}{\text{xy}}\sum_{\text{i=0}}^{\text{x-1}}\sum_{\text{j=0}}^{\text{y-1}}\left[\text{M(i.j)-N(i,j)}\right]^2 . \tag{10}$$

The PSNR is computed as:

$$\text{PSNR} = 10.\log_{10}\left(\frac{\text{MAX}_\text{M}^2}{\text{MSE}}\right) . \tag{11}$$

where MAX is the maximum possible pixel value of the image, image M is x × y matrix and N is its noisy approximation.

2- Structural Similarity Index

The SSIM measures the similarity between two images. It is calculated as:

$$\text{SSIM(x,y)}= \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} . \tag{12}$$

where x and y are two windows of common size,μ_x is the average of x, μ_y is the average of y, σ_x^2 is the variance of x, σ_y^2 is the variance of y and σ_{xy} is the covariance of x and y.

3- Normalized Cross-Correlation

The NCC calculates the cross-correlation based on the size of the images [18]. Then, it calculates the local sums by pre-computing running sums. It uses local sums to normalize the cross-correlation to produce correlation coefficients. The output matrix is holding the correlation coefficients, which can range between −1.0 and 1.0. NCC is defined as [17]:

$$\mathrm{NCC} = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n}(P[i,j] \times S[i,j])}{\sum_{i=1}^{m}\sum_{j=1}^{n}(P[i,j])^2} \qquad (13)$$

The NCC is more robust under uniform illumination changes. The value of NCC close to 1.0 represents the perfect visual quality of the stego-image.

4.2. Qualitative results

The proposed algorithm is tested using different color and grayscale images. The size of the cover and secret images are the same. Figure 2 shows the result of hiding image using LU factorization. The size of the images is 256×256 and the value of $alpha$ is 0.01.

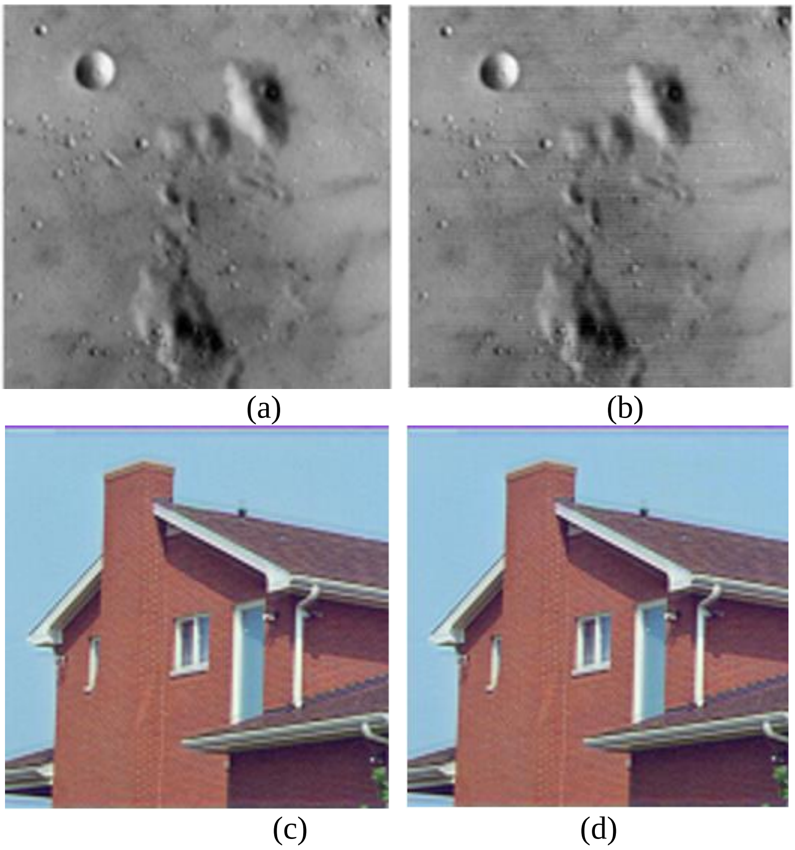
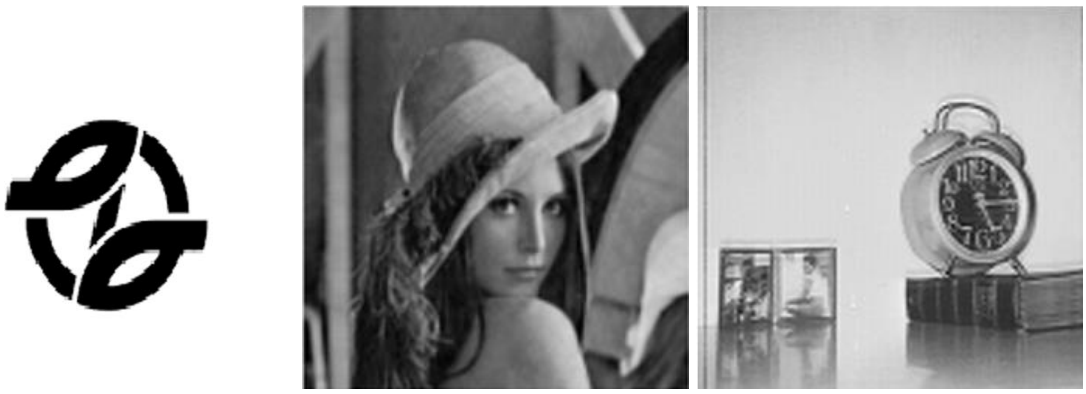


Figure. 2: Comparison between the original cover image and stego-image using LU factorization (a) and (c) the original cover images, (b) and (d) the stego-images.

As shown in Figures 2 and 3, the human visual system cannot distinguish between the original cover images and the stego-images using the LU decomposition technique. Figures 3- display the extracted secret images using LU decomposition.



(a) (b) (c)

Figure. 3: The extracted secret images using LU factorization
(a) Logo (b) Lena (c) Clock images.

4.3. Quantitative results

Table 1 shows the performance of the proposed algorithm using LU factorization for different cover and secret images. The performance is measured using PSNR for the cover image and SSIM and NCC for the secret image.

Table. 1: Performance of the algorithm using LU factorization

Cover image+ Secret image	Cover PSNR	Secret image SSIM	Secret image NCC
Moon + logo	36.8	1	1
Moon + lena	40.3	1	1
Moon + clock	37.5	1	1
House + logo	42.5	1	1
House + lena	42.88	1	1
House + clock	44.09	1	1

As shown in Table 1 the imperceptibility of the algorithm is very high as the cover PSNR is ranging from 36 to 44 dB. The secret image similarity and NCC is 1 which means that the secret image extracted without any distortion.

4- Conclusion

With rapid growth for multimedia over the internet, computer networks are subjected to different types of attacks. Data should be hidden to keep it secure. Steganography is the art of hiding data. In steganography, the data is hidden in a cover object. The proposed technique is an image steganography technique, which hides an image in another image. The technique depends on matrix decomposition techniques to hides the secret image. Two types of matrix decomposition are used and compared QR decomposition and LU decomposition. The performance of the algorithm is measured using PSNR, SSIM and NCC. The PSNR of the cover image is ranging from 36 to 44 dB. The similarity between secret and extracted image is 100% and the NCC is 1.

References

1. P. Joseph and S. Vishnukumar. A study on steganographic techniques. Global Conference on Communication Technologies (GCCT), Thuckalay, 2015, pp. 206-210
2. G., Amara. An Introduction to Wavelets. IEEE computational sciences and engineering, vol. 2, 1995, pp. 50-61.
3. S. W. Smith . The scientist and engineer's guide to digital signal processing. 2nded, Publisher: California Technical Publishing, USA, Chapter 8, 1999, pp. 141-167.
4. N. Ahmed, T. Natarajan and K. R. Rao, Discrete Cosine Transform. in *IEEE Transactions on Computers*, vol. C-23, no. 1, Jan. 1974, pp. 90-93.
5. A.R. Calderbank, Ingrid Daubechies, Wim Sweldens, Boon-Lock Yeo, Wavelet Transforms That Map Integers to Integers, Applied and Computational Harmonic Analysis, 5 (3),1998, pp. 332-369.
6. Emmanuel Candès, Laurent Demanet, David Donoho, and Lexing Ying .Fast Discrete Curvelet Transforms. SIAM Journal Multiscale Model. Simul, vol. 5, 2006, pp. 861–899.
7. O. g. Sundararajan. The Discrete Stationary Wavelet Transform. In Discrete wavelet Transform: A Signal Processing Approach, chapter 13, 2015, pp. 234-246
8. Mary Shanthi RaniMary Shanthi Rani S. Lakshmanan S. LakshmananP Saranya. A Study on Video Steganography using Transform Domain Techniques. Conference: 5th National conference on Computational Methods, Communication Techniques and Informatics At: Gandhigram Rural Institute - Deemed University, Gandhigram, Dindigul vol. 1, 2017.
9. Vinayagam.P, Rajesh Kumar.G, Mohan raj .G, Sethumathavan.V. QR decomposition based secure watermarking images. International Journal of Applied Engineering Research ISSN 0973-4562 Volume 14, Number 6, 2019.
10. Deepesh Rawat and Vijaya Bhandari. A Steganography Technique for Hiding Image in an Image using LSB Method for 24 Bit Color Image. International Journal of Computer Applications (0975 – 8887) Volume 64– No.20, 2013
11. amaldeep Joshi, Swati Gill, Rajkumar Yadav. A New Method of Image Steganography Using 7th Bit of a Pixel as Indicator by Introducing the Successive Temporary Pixel in the Gray Scale Image, Journal of Computer Networks and Communications, vol. 2018, 2018.
12. Avinash K. Gulve, Madhuri S. Joshi, An Image Steganography Method Hiding Secret Data into Coefficients of Integer Wavelet Transform Using Pixel Value Differencing Approach, Mathematical Problems in Engineering, vol.11, 2015
13. Himadri Bhattacharjee and Samir Kumar Bandyopadhyay. Frequency Domain Approach of Image Steganography. International Journal of Innovative Research in Information Security (IJIRIS) Issue 02, Volume 3 , 2016
14. Kadhim I.J., Premaratne P., Vial P.J. Adaptive Image Steganography Based on Edge Detection Over Dual-Tree Complex Wavelet Transform. In: Huang DS., Gromiha M., Han K., Hussain A.

(eds) Intelligent Computing Methodologies. ICIC 2018. Lecture Notes in Computer Science, vol 10956.

15. Subhedar, M.S. Cover selection technique for secure transform domain image steganography. Iran J Comput Sci, 2021.
16. A. G. George, A. K. Prabavathy : A survey on different approaches used in image quality Assessment international journal of emerging technology and advanced engineering. 3(2), 2013 197-203
17. Wang, Z.; Bovik, A.C.; Sheikh, H.R.; Simoncelli, E.P. Image Quality Assessment: From Error Visibility to Structural Similarity. IEEE Trans. Image Process, 13, 2004, 600–612