Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 26 (2023), No. 6, pp. 1683–1689
DOI : 10.47974/JDMSC-1614

Image steganography using Fresnelet transformations, stated coefficients and a pre-processed message

Munthir Bahir Tuieb *
Hind Jumaa Serteep †
Doaa Muhsin Abed Ali §
Department of Computer Science
College of Education
Mustansiriyah University
Baghdad
Iraq

Abstract

The method of concealing confidential information inside an image is known as image steganography. In this work, the image steganography technique is developed. The framework is made up of three components: preprocessing of secret messages, selecting coefficients for the hiding process, and the hiring process. The secret message is organized as a two dimentional array, then processed via mathematical equations, which provide more security because the result is an encrypted message. The paper suggests a set of steps to hide the message efficiently. The experimental results show that the suggested method provides a high steganographic quality of the cover image and a high capacity for embedding information, which are two characteristics of a successful steganography technique.

Subject Classification: *Primary 93A30, Secondary 49K15.*

Keywords: *Fresnelet transform, Scrambling mechanism, Pre-processed message, Steganography.*

1. Introduction

Owing to the increase in communication mediums, such as the internet, and improvements in the area of digital communications, the security of data transferred over these mediums has become a very crucial

* *E-mail:* munthir_b_t87@uomustansiriyah.edu.iq (Corresponding Author)
† *E-mail:* hind_2018@uomustansiriyah.edu.iq
§ *E-mail:* doaa_muhsin@uomustansiriyah.edu.iq

factor. Cryptography and steganography are important tools for protecting data. Cryptography uses encryption (to make messages confidential) by converting readable words into unreadable ones [1]. Steganography, comparatively, refers to the study of concealing communication for avoiding unintended outsiders from learning that a message has been sent [2]. Least Significant Bit (LSB) is a spatial domain steganography method commonly utilized because of its easiness. It has a lower possibility of degrading the actual image [3]. It replaces the LSB of image pixels with data bits [4]. Transform domain technique conceals secret data bits within the altered image's coefficients. It is more reliable and difficult than spatial domains like LSB procedures [5].

The Fresnelet transform was first introduced in the context of Fresnelet diffraction. This transform was utilized to recover an image from an FT hologram considering varying factors such as wavelength (L), object-to-image-plane distance (di), and image resolution. The fundamental functionalities of FT are level-by-level reduction shifting variants. When implemented to a wavelet base, FT provides multi-resolution features. Unitary, duality, translation, and dilation are only a few of the features of the Fresnelet transform. The unitary feature allows for precise image recovery. The inverse Fresnelet transform is computed using the duality condition.

S. Uma Maheswari et. al. the Fresnelet transform (FT) is used to conceal the message of QR coded the sub-bands at high frequency and LSB are utilized [6]. Shabieh Farwa et. al. present diffraction of Fresnelet in the wave-propagation field with the scrambling mechanism of image utilizing elliptic curve [7]. Nazeer Muhammad et. al. present Fresnelet transform and varying key settings. The wavelets are used to hide the obtained coded layout into certain sub-bands of the carrier [8].

2. The Method

The suggested scheme's framework is depicted in Figure 1. The pre-coded confidential message is embedded into an original image (which is pre-processed) during the embedding step.

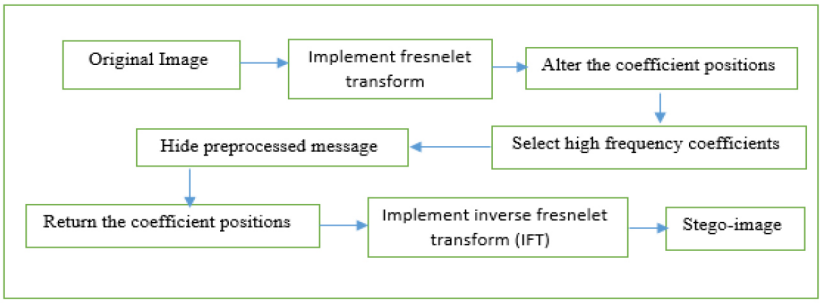

Figure 1

Framework of the scheme

The secret message is preprocessed based on the following steps:

Step 1: Arrange the message (M) as two dimensions array, with padding the remaining empty cells by zeros values (zv).

Step 2: Compute z (i, j) = M(x, k(r, c)), where k(r, c) is computed as in the following equations:

$$k(r,c)=\begin{cases} q(r/2,c) & \text{where } r \text{ is even and } q(r/2,c)<c/2 \\ 4r-4q(r/2,c)-1 & \text{where } r \text{ is even and } q(r/2,c)\geq c/2 \\ q((4r-1 \bmod r)/2,c) & \text{where } r \text{ is odd and } (4r-1 \bmod r)/2<c/2 \\ 4r-4q((4r-1 \bmod r)/2,c)-1 & \text{where } r \text{ is odd and } (4r-1 \bmod r)/2>=c/2 \end{cases}$$

Where Rand = random number, a = (Rand * r) c + 1 mod r and b = (Rand * c) r + 1 mod c, and q(r, c) = q (a, b).

Step 3: Memorize the locations of (zv) and Rand values to adjust the recovery process for hiding messages, they are acting as a key.

The scrambling mechanism is used to improve the algorithm's security. The scrambling approach is employed in this study as follows:

Im (x, y) = I (x + Rand, y + (Rand * x)) mod A, where the image of size A*A, I (x, y) is an original image, Im (x, y) is a scrambled image.

The coefficients are selected in 8 * 8 block of them, F is the total number of all blocks. Then 64F possible position for hiding follows the following steps for the hiding process:

Step 1: Set TS is a threshold value, where (1 <= TS <= 4), to minimize the distortion after the hiding process and enhance perceptibility which leads to minimizing color variation that can be noticed by an investigator.

Step 2: For selected coefficient SCk and El = z (i, j) element of message, perform subtraction process as follows: HB = SCk – El, where HB <= TS.

Step 3: If HB = TS

Then perform one-bit shifting operation to the right.

Else don't change HB value.

Step 4: Perform SCn = SCk + HB as hiding process, and collect all SCn to rebuild the original image.

3. Experimental Results and Discussions

The PSNR (Peak signal-to-noise ratio) as a performance criteria is utilized in this work to assess the stego image's quality. It is the signal's maximum strength (cover) to the strength of degrading noise (stego image) ratio, which influences the representation accuracy. The MSE (mean square error) is used for calculating the PSNR. The MSE is the sum of the squared errors of the degrading noise and the signal's maximum strength. The stego image quality is better if value of PSNR is larger. MATLAB is utilized to execute a project.

$$MSE = \frac{1}{i * j} \sum_{m=1}^{i} \sum_{n=1}^{j} [im(m,n) - St\_im(m,n)]^2 \quad (1)$$

$$PSNR = 10 \frac{255^2}{MSE} \quad (2)$$

Where $im(m,n)$ is the cover image, $St\_im(m,n)$ is the stego image. Figure 2 shows the tested cover images in gray-level.

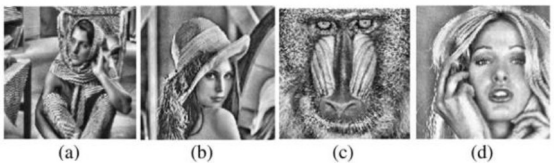

Figure 2

Cover (original) images (a) Babara (b) Lena (c) Baboon (d) Tiffany

The PSNR value (dB) and no. of bits to be hidden which is called an (embedding capacity) of tested images for d1 = 0.03 m, d2 = 3000 m with wave-length (L = 654.6 nm).

Table 1

Value of PSNR (dB) and embedding capacity for tested images

Image	d1 = 0.03		d2 = 3000	
	PSNR	embedding capacity	PSNR	embedding capacity
Babara	43.26	433.322	47.13	433.322
Lena	43.20	433.322	47.11	433.322
Baboon	43.22	433.322	47.13	433.322
Tiffany	43.27	433.322	47.15	433.322

Table 1 shows that the PSNR values are high for d2= 3000 m, which indicates that when the space (an outcome changes depending on the space) between the image plane and the objects grows, so does the value of PSNR. For both distances, the capacitance for hiding information is similar. High PSNR indicates decreasing noise in the stego image, although embedding hidden message. The suggested scheme achieved a PSNR value of 47.15. Similarly, the embedding capacity is 433.322 bits, indicating that a significant amount of data may be stored in the original image. Figures 3 and 4 display the stego images using d1= 0.03 m as well as d2= 3000 m respectively.

Figure 3

Stego image with d1= 0.03 m

Figure 4

Stego image with d1= 3000 m

4. Conclusion

Fresnelet transform is presented in this work, which leads to fast restoration of Fresnel holograms and achieves better resolution. The security is enhanced by changing the coefficient's position and avoiding straight embedding. It preserves the quality after the embedding process, where PSNR is 47.15 dB for the Stego image and high bits are embedded (433.322 bits). Thus, two factors are fulfilled: high Stego image quality and high embedding capacity.

References

[1] Wassim Alexan, Mazen El Beheiry and Omar Gamal–Eldin, A Comparative Study Among Different Mathematical Sequences in 3D Image Steganography, *International Journal of Computing and Digital Systems* (2020).

[2] G. Mostafa and W. Alexan, "A high capacity double–layer gray code based security scheme for secure data embedding," in 2019 International Symposium on Networks, Computers and Communications (ISNCC), Turkey, Jun. (2019).

[3] A. Baby and H. Krishnan, "Combined Strength of Steganography and Cryptography- A Literature Survey," *Int. J. Adv. Res. Comput. Sci.*, Vol. 8, No. 3, pp. 1007–1010 (2017).

[4] Dr. H. B. Kekre, Ms. Archana Athawale, "Information Hiding using LSB Technique with Increased Capacity" *International Journal of Cryptography and Security*, Vol 1, No. 2 (Oct-2008).

[5] Saurabh V. Joshi, Ajinkya A. Bokil, Nikhil A. Jain and Deepali Koshti Image Steganography Combination of Spatial and Frequency Domain *International Journal of Computer Applications* (0975 – 8887) Volume 53– No. 5, (2012).

[6] S. Uma Maheswari, D. Jude Hemanth, "Frequency domain QR code based image steganography using Fresnelet transform". *AEÜ - International Journal of Electronics and Communications* (2015).

[7] Shabieh Farwa, Nargis Bibi and Nazeer Muhammad, "An efficient image encryption scheme using Fresnelet transform and elliptic curve based scrambling", *Multimedia Tools and Applications* (2020).

[8] Nazeer Muhammad1, Nargis Bibi, Zahid Mahmood and Dai-Gyoung Kim , "Blind data hiding technique using the Fresnelet transform", SpringerPlus (2015).

[9] Shubham Sharma & Ahmed J. Obaid, Mathematical modeling, analysis and design of fuzzy logic controller for the control of ventilation systems using MATLAB fuzzy logic toolbox, *Journal of Interdisciplinary Mathematics*, 23:4, 843-849 (2020), DOI: 10.1080/09720502.2020.1727611.

[10] B. Lakshmi Sirisha, Image steganography based on SVD and DWT techniques, *Journal of Discrete Mathematical Sciences and Cryptography*, 23:3, 779-786 (2020), DOI: 10.1080/09720529.2019.1698801.

Received February, 2022

Revised April, 2022