Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
DOI : 10.47974/JIOS-2054

Covert communication using reversible and lossless image steganography with high embedding capacity

B. Lakshmi Sirisha *
Department of Electronics and Communication Engineering
Siddhartha Academy of Higher Education (Deemed to be University)
Vijayawada 520007
Andhra Pradesh
India

G. Sridevi †
Department Electronics and Communication Engineering
Aditya University
Surampalem
Kakinada 533437
Andhra Pradesh
India

K. V. S. L. Harika §
Department of Computer Science and Engineering
Gokaraju Rangaraju Institute of Engineering and Technology
Hyderabad 500090
Telangana
India

Shahnazuddin ‡
Department of English
Siddhartha Academy of Higher Education (Deemed to be University)
Vijayawada 520007
Andhra Pradesh
India

* *ORCID-ID:* **0000-0002-1225-9760**
† *ORCID-ID:* **0000-0002-7884-3409**
§ *ORCID-ID:* **0000-0004-7220-1693**
‡ *ORCID-ID:* **0009-0007-5101-2780**

* *E-mail:* **suravarapuls@yahoo.co.in (Corresponding Author)**
† *E-mail:* **sridevi_gamini@yahoo.com**
§ *E-mail:* **haarika.karibandi@gmail.com**
‡ *E-mail:* **shanaz.uddin3@gmail.com**

Abstract

In digital world, security is one of the important challenging issues. Data hiding is one of the ways out. Covert communication is possible with data hiding. Steganography technique is one of the useful data hiding method, the secret is hided with the help of cover so that the third party cannot identify. Data may be in the form of text, image, audio/video. In this paper, a novel image steganography algorithm based on modulus and polynomial theory is proposed for data hiding. In proposed method image is taken as data, both secret and cover images are reconstructed at the receiver side by the authorized person without any damage hence this method satisfies the reversibility property. Proposed method gives high embedding capacity, good quality with a PSNR of 64.45dB compared with existing techniques.

Subject Classification: *94A60, 11T71, 11C08.*

Keywords: *Covert communication, Data hiding, Image metrics, Image steganography, Modulus, Polynomial theory.*

1. Introduction

Secret communication [1] is necessary in many fields like banking sector, military, forensic labs and intelligence bureau etc. This can achieve with the help of hiding techniques. Cryptography, Watermarking and Steganography are data hiding techniques. Cryptography [2] is suited for text data hiding. Watermarking [3] is suited for image hiding however, if the image is flipped or rotated this technique is failed. Steganography [4] is one of the powerful techniques to embed the secret data in to cover data. It is suited for any type of data such as text, image, audio and video. Steganography system is designed with the secret and cover data. The secret is embedded into cover (carrier) via password to get stego data. The stego data looks like cover data so that unauthorized person cannot access the secret. In any case the secret data is damaged, rotated, flipped or stolen by unauthorized persons it is recovered by stego images and secret key, it is not possible with cryptography and water marking techniques.

The rest of the paper is organized as. Literature survey is presented in section 2. The proposed work is introduced in 3. Experimental results and discussions are analysed in section 4. Concluding remarks and future scope are concluded in 5.

2. Literature survey

High embedding capacity is possible with the polynomial based steganography only. Shamir [5] introduces polynomial theory in steganography for high embedding capacity. In this work, secret data is distributed to n number of participants. t Participants out of n are needed to reveal the secret data, less than t cannot gain information. Lin and Tsai [6] proposed a method using lossy polynomial, however this method was failed to recover the secret data. Wu, Thien, and Lin [7] proposed a method using modulus operation however, this

method also failed to recover the secret due to truncated pixels. Chang, Hsieh, and Lin [8], Zhao et al.,[9] and Lin, Lee, and Chang [10] solve the problem of truncated pixels [11] which are greater than 250. However, these methods attract the attackers due to random nature of stego images. Moreover, these methods do not reconstruct the secret data perfectly. Lin and Chan [12] proposed a new polynomial function to overcome these problems, but in this method Lagrange interpolation [13] is used to reconstruct the secret and cover data so that the computational cost is very high. Moreover, this method works based on prime number, which leads it not so flexible. Mohsin et al., [14] proposed a method related to COVID-19 data security. This work is based on the block chain technology along with hash function. In this method, patient's data is hiding in hospital digital records. Their result shows, good stego quality and embedding capacity. However, their work is study work not implemented on real patient's reports because of lockdown situation.

Inspired by the practical requirement [15], a novel image steganography method is proposed. This is a lossless polynomial technique hence it recovers the secret and cover data, no problem with truncated pixels. This method requires less number of computations compared with existing methods hence computational cost is low and speed is high. It is flexible as there is no use of any primary numbers for this proposed work.

3. Proposed method

In proposed work, high embedding capacity with good quality and security is the prime parameter. To achieve this, polynomial theory and modulus operation are used for covert communication. The cover image's size must match or exceed the secret images in order for the secret image to be perfectly embedded into the cover image. For this work, secret and cover images that have the same size M x N are selected. This work is appropriate for both colour and gray scale images.

In this work, modulus operation is performed on secret image and quotients were used to generate polynomial equations, which will enhance security. Example of modulus operation is shown in Figure 1. 17 mod 5 = 2, this means divide 17 by 5, we get 3 is represented as quotient with a remainder 2. Actually, modulus is another name for remainder after performing division.

In proposed embedding algorithm, modulus by 5 is used to achieve good results. When considering low modulus values, the computational cost is high because it requires more calculations. The stego image quality will decrease when considering a high modulus value. The Proposed embedding algorithm presented in 3.1

3.1 *Embedding algorithm*

Step 1: Choose a secret image with size of M X N and divide into sub images of size m x n. where M > m, N > n. Cover image size also same as secret image.

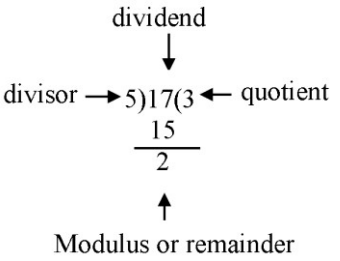

Figure 1
Example for Modulus operation

Step 2: Apply Modulus operation by T on each pixel of sub image to form a quotient 1 and remainder1 matrixes

Step 3: Apply Modulus operation with T on quotient 1 matrix again get quotient 2 and remainder 2 matrixes.

Step 4: This process will continue until the quotient matrix values are less than T.

Step 5: Polynomial equation is formed with the final quotient matrix and all remainder matrixes along with cover pixel as

$$p(x) = (a_1x^1 + a_2x^2 + a_3x^3 + a_4x^4 + c) \quad (1)$$

where, c is the cover pixel, a_1 is final quotient matrix value and $a_2$is the final remainder matrix value, a_3 and a_4 are remainder 2 and remainder 1 matrix values respectively.

Step 6: Generate n stego images by feeding the password (secret key) in to equation (1) to get $y_1 = p(1), y_2 = p(2), \ldots y_n = p(n)$.

Embedding algorithm is implemented on secret and cover images of size 2 X 2. Modulus value T is chosen as 5. Example of embedding algorithm is presented in 3.1.1.

3.1.1 Example of embedding algorithm

Step 1: Choose the secret (s) and cover (c) images of size 2 X 2

$$s = \begin{pmatrix} 253 & 201 \\ 255 & 198 \end{pmatrix}$$

$$c = \begin{pmatrix} 169 & 123 \\ 201 & 255 \end{pmatrix}$$

Step 2: Apply modulus operation with 5 on secret image (s), we get quotient matrix 1= $\begin{pmatrix} 50 & 40 \\ 51 & 39 \end{pmatrix}$ and remainder matrix 1 = $\begin{pmatrix} 3 & 1 \\ 0 & 3 \end{pmatrix}$.

Step 3: Apply modulus operation with 5 on quotient matrix 1= $\begin{pmatrix}50 & 40\\51 & 39\end{pmatrix}$get quotient matrix 2= $\begin{pmatrix}10 & 8\\10 & 7\end{pmatrix}$ and remainder matrix 2= $\begin{pmatrix}0 & 0\\1 & 4\end{pmatrix}$.

Step 4: apply modulus operation with 5 on quotient matrix 2 = $\begin{pmatrix}10 & 8\\10 & 7\end{pmatrix}$ get quotient matrix 3 = $\begin{pmatrix}2 & 1\\2 & 1\end{pmatrix}$ and remainder matrix 3 = $\begin{pmatrix}0 & 3\\0 & 2\end{pmatrix}$.

Step 5: These matrixes are final because the quotient matrix 3 values are less than 5.

Step 6: final quotient = $\begin{pmatrix}2 & 1\\2 & 1\end{pmatrix}$, final remainder = $\begin{pmatrix}0 & 3\\0 & 2\end{pmatrix}$.

remainder 2 = $\begin{pmatrix}0 & 0\\1 & 4\end{pmatrix}$, remainder 1 = $\begin{pmatrix}3 & 1\\0 & 3\end{pmatrix}$.

The polynomial equation is formed with these matrixes along with cover (c) as shown in equation (2)

$$p(x) = \begin{bmatrix}(2x^1 + 0x^2 + 0x^3 + 3x^4 + 169) & (1x^1 + 3x^2 + 0x^3 + 1x^4 + 123)\\(2x^1 + 0x^2 + 1x^3 + 0x^4 + 201) & (1x^1 + 2x^2 + 4x^3 + 3x^4 + 255)\end{bmatrix} \quad (2)$$

Generate stego images as

$$y_1 = p(1), y_2 = p(2), \dots y_n = p(n). \quad (3)$$

Stego image and secret keys are provided for the authorized participants for extraction. In equation (3), 1,2,… n are the secret keys. As less as x value in equation (2), we get good quality of stego. In extraction algorithm cramer's rule is used. This algorithm recovers the secret and cover images without any loss. The extraction algorithm is presented in 3.2.

3.2 *Extraction algorithm*

Step 1: Compute the polynomial coefficients of function $p(x)$ using cramer's rule,

$$a_n * x = y_n \quad (4)$$

where y_n is stego image, x is secret key, a_n is the coefficient of polynomial. Using equation (4), $a_n$coefficients are calculated.

Step 2: The coefficients a_1 , a_2, a_3, a_4 are considered as values of final quotient matrix, final remainder matrix, remainder 2 matrix, remainder 1 matrix respectively. Constant value is considered as cover pixel value.

Step 3: Reconstruct the secret blocks of size m x n, then merge all the sub images to get secret image of size M X N. Cover image also recovered with constant values which derived at step 2.

3.2.1 Example of extraction procedure

Calculate the coefficients of polynomial function $p(x)$ using cramer's rule for example

Step 1: Consider the stego pixels and secret key for reconstruction.

$$p(x) = (2x^1 + 0x^2 + 0x^3 + 3x^4 + 169)$$

a_1 a_2 a_3 a_4 cover pixel

Step 2: Coefficients a_1, a_2, a_3, a_4 are values of final quotient matrix, final remainder matrix, remainder 2 matrix, remainder 1 matrix respectively. Constant value is considered as cover pixel value.

Step 3: Similarly sovle all the equations and generate $final\ quotient = \begin{pmatrix} 2 & 1 \\ 2 & 1 \end{pmatrix}$, $final\ remainder = \begin{pmatrix} 0 & 3 \\ 0 & 2 \end{pmatrix}$, $remainder\ 2 = \begin{pmatrix} 0 & 0 \\ 1 & 4 \end{pmatrix}$, $remainder\ 1 = \begin{pmatrix} 3 & 1 \\ 0 & 3 \end{pmatrix}$.

Step 4: Multiply final quotient with 5 and add to the final remainder matrix to get quotient matrix 2 $\begin{pmatrix} 10 & 8 \\ 10 & 7 \end{pmatrix}$, again multiply with 5 and add to remainder matrix 2 to get $\begin{pmatrix} 50 & 40 \\ 51 & 39 \end{pmatrix}$again multiply with 5 and add to remainder matrix 1 to get $\begin{pmatrix} 253 & 201 \\ 255 & 198 \end{pmatrix}$. Consider this is secret block because there is no another remainder matrixes.

Step 5: Finally, merge all the secret blocks get reconstructed secret image. All the constant values derived from the equations are forming a proper order to get reconstructed cover image as $\begin{pmatrix} 169 & 123 \\ 201 & 255 \end{pmatrix}$.

4. Result analysis and discussions

The main focus of the proposed method is to generate high quality stego image with good embedding capacity. Various bench mark images are used for this work as shown in Figure 2. Most of the existing algorithms embed the text data into cover image, some algorithms embed small size secret image than cover image. In proposed method the sizes of secret and cover images are same, so that the embedding capacity will increase. This proposed work is best suited for embedding 2 secret images into a cover image with polynomial theory. However, if try to embed more images in single cover means quality of stego is decreases as shown in Figure 3. The quality of stego image more than 30 dB is acceptable. If less, the secret data is out from the cover data so there is no use of data hiding. In proposed work, cover and stego images are looks like same is

shown in Figure 2 that means the stego quality is good, it cannot reveal the secret data.

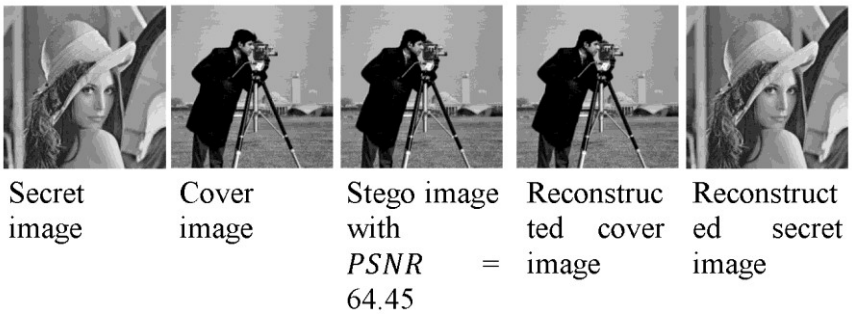

Figure 2
Embedding and reconstructed images

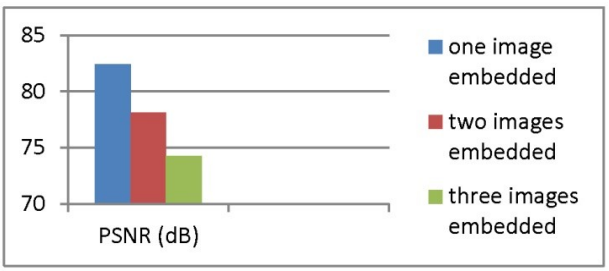

Figure 3
Results of stego quality Vs embedding capacity

4.1 *Quality of images*

In image steganography quality of the resultant images are very important. The quality parameters [21-24] of stego image with different cover images are presented in Table 1. Comparisons of proposed method with existing methods are presented in Table 2. *PSNR* (Peak Signal Noise Ratio) is one of the important image metric to measure the quality of stego [25-26] it is represented as

Table 1
Quality assessment of stego image

Stego image	PSNR	SSIM
Camera Man	64.45	0.9992
Barb	64.45	0.9992
Boat	63.48	0.9981
Girl	64.48	0.9991
House	63.46	0.9982

$$PSNR = 10\ log_{10}\left(\frac{255^2}{MSE}\right)\ dB \tag{5}$$

where MSE (Mean Square Error) between cover and stego image is calculated by

$$MSE = 1/(M\ X\ N)\sum(Cover\ pixel - stego\ pixel)^2 \tag{6}$$

$M\ X\ N$ is the size of the image.

Table 2

Comparison of proposed method with existing methods

Method	PSNR (dB)	Reconstruct the secret image without loss	Reconstruct the cover image without loss	Embedding capacity (bpp)
Lin, Lee, and Chang [10]	32	Yes	No	-
Wu, Thien, and Lin [7]	34	No	No	-
Yang et al., [11]	40	Yes	No	2
Zhao et al., [9]	39	Yes	No	2
Lin and Chan [12]	42	Yes	Yes	4
Lee and Lee [19]	44	Yes	Yes	4
Wei and Wen [25]	46.03	Yes	No	8
Duan et al. [20]	40	Yes	Yes	8
Xinliang et al., [18]	40.66	Yes	No	8
Rustad et al. [17]	40.28	Yes	Yes	2
Kosuru el al. [16]	36.76	Yes	Yes	8
Wang et al. [1]	41.21	Yes	Yes	8
Proposed method	64.45	Yes	Yes	8

Structural SIMilarity (SSIM) [27] is one of the powerful image metric to measure the similarity between cover and stego images is given by

$$SSIM(x,y) = \frac{(2\mu_x\mu_y+C_1)(2\sigma_{XY}+C_2)}{(\mu^2{}_X+\mu^2{}_Y+C_1)(\sigma^2{}_X+\sigma^2{}_Y+C_2} \tag{7}$$

where μ_x and μ_y are mean, $\sigma^2{}_X$ and $\sigma^2{}_Y$ are variance, σ_{XY} is the covariance of x, y. $C_1 = (k_1L)^2$, $C_2 = (k_2L)^2$, L is dynamic range of the pixel values, predefined values k_1=0.01, k_2=0.03. Because the SSIM value is so close to unity shown in Table 1, the stego image and the cover image appear to be identical, preventing unauthorized individuals from thinking about the secret data [28] that is now there. That enhances the security level.

5. Conclusions

An efficient image hiding method is proposed to embed secret image into cover image of same size $M\ X\ N$. This method reconstructs the images at

receiver without any damage. Histograms of cover and stego image are same so that unauthorized user can not access the secret data. In the sense of quality, proposed method yields 64.45dB, this is an excellent approach compared to existing steganography methods. In proposed work, secret image of size 512 x 512 is embedded into cover image of size 512 x 512. In most of existing methods, embedded secret is less size than the cover. That shows, proposed work efficiency. This work is also analysed by embedding 3, 4 and 5 secrets into single cover image. However, the secret will be out in case of 4 images are embedded. Further improvement focused on color image steganography. In color image processing RGB channels are there so that more data can be embedded.

References

[1] T. Wang, H. Cheng, X. Liu, Y. Xu, F. Chen, M. Wang, and J. Chen, "Lossless image steganography: Regard steganography as super-resolution," *Information Processing & Management,* vol. 61, no. 4 (Jul. 2024).

[2] S. S. Midha and B. Ramola, "Cryptography in network security," in 2022 International Conference on Cyber Resilience (ICCR), Dubai, UAE, pp. 1–5 (2022).

[3] M. A. Tahiri, H. Karmouni, M. Sayyouri, H. Qjidaa, M. Ahmad, M. Hammad, P. Pławiak, O. Alfarraj, and A. A. Abd El-Latif, "An improved reversible watermarking scheme using embedding optimization and quaternion moments," *Scientific Reports*, vol. 14, art. no. 18485 (2024), doi: 10.1038/s41598-024--69511-3".

[4] B. L. Sirisha, S. F. Ahamed, and V. B. K. L. Aruna, "Patient data hiding and transmitting during COVID-19 for telemedicine application using image steganography," *Current Medical Imaging,* vol. 20, pp. 1–8 (2024).

[5] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613 (1997).

[6] W. H. Tsai and C. C. Lin, "Secret image sharing with steganography and authentication," *Journal of Systems and Software*, vol. 73, no. 3, pp. 405–414 (2004).

[7] Y. S. Wu, C. C. Thien, and J. C. Lin, "Sharing and hiding secret images with size constraint," *Pattern Recognition*, vol. 37, no. 7, pp. 1377–1385 (2004).

[8] C. C. Chang, Y. P. Hsieh, and C. H. Lin, "Sharing secret in stego images with authentication," *Pattern Recognition*, vol. 41, no. 10, pp. 3130–3137 (2008).

[9] R. Zhao, J. J. Zhao, F. Dai, and F. Q. Zhao, "A new image secret sharing scheme to identify cheaters," *Computer Standards & Interfaces,* vol. 31, no. 1, pp. 252–257 (2009).

[10] P. Y. Lin, J. S. Lee, and C. C. Chang, "Distortion-free secret image sharing mechanism using modulus operator," *Pattern Recognition,* vol. 42, no. 5, pp. 886–895 (2009).

[11] C. N. Yang, T. S. Chen, K. H. Yu, and C. C. Wang, "Improvements of image sharing with steganography and authentication," *Journal of Systems and Software*, vol. 80, no. 7, pp. 1070–1076 (2007).

[12] P. Y. Pei and C. S. Chan, "Invertible secret image sharing with steganography," *Pattern Recognition Letters*, vol. 31, pp. 1887–1893 (2010).

[13] B. Lakshmi Sirisha and B. Chandra Mohan, "Review on spatial domain image steganography techniques," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 24, no. 6, pp. 1873–1883 (2021).

[14] H. Mohsin, A. A. Zaidan, B. B. Zaidan, K. I. Mohammed, O. S. Albahri, A. S. Albahri, and M. A. Alsalem, "PSO–Blockchain-based image steganography: towards a new method to secure updating and sharing COVID-19 data in decentralized hospitals intelligence architecture," Springer, pp. 14137–14161 (Dec. 2020).

[15] Y. Ren, J. Qin, X. Xiang, and Y. Tan, "Reversible data hiding in encrypted images based on secret sharing and hierarchical embedding," *Computers and Electrical Engineering*, vol. 119, Part B (2024).

[16] S. N. V. J. Devi Kosuru, A. Pradhan, K. Abdul Basith, R. Sonar, and G. Swain, "Digital image steganography with error correction on extracted data," *IEEE Access,* vol. 11 (2023).

[17] S. Rustad, D. R. I. M. Setiadi, P. N. Andono, A. Syukur, and Purwanto, "Optimization of cross diagonal pixel value differencing and modulus function steganography using edge area block patterns," *Cybernetics and Information Technologies*, vol. 22, no. 2 (2022).

[18] X. Bi, X. Yang, C. Wang, and J. Liu, "High capacity image steganography algorithm based on image style transfer," *Security and Communication Networks,* vol. 1, pp. 1–14 (2021).

[19] Y. P. Lee and J. C. Lee, "High-payload image hiding with quality recovery using tri-way pixel value differencing," *Information Sciences,* pp. 214–225 (2012).

[20] X. Duan, D. Guo, N. Liu, and B. Li, "A new high capacity image steganography method combined with image elliptic curve cryptography and deep neural network," *IEEE Access,* vol. 8 (Feb. 2020).

[21] B. L. Sirisha, "Image steganography based on SVD and DWT techniques," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 23, no. 3, pp. 779–786 (Feb. 2020).

[22] A. K. Sahu and M. Sahu, "Digital image steganography and steganalysis: A journey of the past three decades," *Open Computer Science,* vol. 10, pp. 296–342 (2020).

[23] B. L. Sirisha, S. Srinivas Kumar, and B. Chandra Mohan, "Steganography based image sharing with reversibility," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 19, no. 1, pp. 67–80 (2016).

[24] B. L. Sirisha, S. Srinivas Kumar, and B. Chandra Mohan, "Identification of cheaters in elections using steganography," *Journal of Information and Optimization Sciences*, vol. 37, no. 2, pp. 271–278 (2016).

[25] W. Wei and Y. Wen, "A novel image steganography using wavelet contrast and modulus operation," *Lecture Notes in Computer Science*, pp. 418–425 (2016).

[26] B. L. Sirisha, S. Srinivas Kumar, and B. Chandra Mohan, "Steganography based information security with high embedding capacity," in National Conference on Recent Advances in Electronics & Computer Engineering (RAECE), IIT Roorkee (2015).

[27] N. Ayub and A. Selwal, "An improved image steganography technique using edge based data hiding in DCT domain," *Journal of Interdisciplinary Mathematics,* vol. 23, no. 2, pp. 357–366 (2020).

[28] V. K. Sharma, B. P. Soni, N. Janu, S. Aziz, and D. Shekhawat, "Review on image steganography using different LSB methods," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 27, no. 4, pp. 1319–1329 (2024).

Received February, 2025