# Secure Data Hiding Technique using Secret Image Scrambling

Vijay kumar sharma
Computer and Communication Engineering Department
Manipal University Jaipur
Jaipur, INDIA
Vijaymayankmudgal2008@gmail.com

Jaya Krishna R
Computer Science and Engineering Department
Manipal University Jaipur
Jaipur, INDIA
Jaya.krishna@jaipur.manipal.edu

Arjun Singh
Computer and Communication Engineering Department
Manipal University Jaipur, Jaipur, INDIA
vitarjun@gmail.com

Vikram Singh Rathore
Assistant Professor, Computer Science Department, CEG,
Department of Technical Education, Govt. of Rajasthan,
Jaipur
rathorevsmail@gmail.com

*Abstract*— Today secure data hiding is remaining as the demanding topic because of its advantages. Most of the things are delivering electronically during these days, so steganography fulfills this requirement by providing safe data hiding. In this paper, wavelet based secure data hiding is proposed. Initially, the secrete image is encrypted by using pixel scrambling operation with circular shift and swapping operation then the resultant image is added to the cover image. Scrambling process is applied up to N round. The resultant image picture quality has been improved by applying pixel-based correlation operation. The results show the strength of proposed technique. The proposed technique is more robust because the secret image is initially scrambled before embedding.

*Keywords*— *Wavelet; image scramble; data hiding; image; steganography, watermarking, cryptography*

## I    INTRODUCTION

Today, secure data transfer plays a vital role in data integrity. It is the demanding field because of dominant attackers, who can identify even the data transferred in the hidden form [1] [2]. If data is being transferred in its original form without hidden form, then there is a high chance for an attacker to steal data. So, it is the reason which motivate to develop a secure data hiding technique.

There are so many techniques for data protection like cryptography, steganography, and watermarking [2-4]. They differ according to their application areas.

The steganography plays big role in data hiding as data is transferred in hidden form, so there is less chance that, data is attacked by an attacker. It is very hard and practically not possible to identify, something is hidden inside the media file by human eyes.

In this paper a secret image is scrambled before embedding into the cover image that makes the technique more robust. Even if an attacker identify that the image is stego image, finding the secret image is not possible as extraction final image is a scrambled image. So proposed technique is more robust as compared to without scrambled technique. Scrambling is one of the best security features that makes the technique better than existing approaches. this is the main motivation behind using it in proposed steganography technique.

## II  LITERATURE REVIEW

Steganography have been used science the ancient time. In digital era the modern steganography is known as digital steganography [4]. In [5] author proposed a secure fingerprint hiding inside the person's face image for authentication of smartcard. Least significant bit-based steganography have been explained in [6]. In this author explained LSB technique steganography for RGB image.

Visual cryptography is an important role in communication. Data can be sent through steganography technique which is encrypted by Visual cryptography. The visual cryptography-based encryption techniques were explained in [7]. Image fusion based methods are explained in [8-9] in which can two images are joined with the help of fusion-based operations.

In [10] scrambling technique based on Arnold transformation and EX-OR operation had been proposed. Initially the image is scrambled using Arnold transformation which change the pixel position using some iterative loop then bitwise EX-OR operation is applied on the pixels. This increased the robustness and confidentiality of secret image. A detailed review of current image steganography and the latest contributions in each group in multiple modalities is discussed

in [11]. This paper also delivers a complete summary of image steganography with broad operation, desires, diverse aspects, different types and their performance valuations.

In [12] authors discussed the main features of coverless image steganography research, the vital frameworks, pre-processing, generation of hash sequence and feature extraction.

## III    PROPOSED TECHNQUE

Initially the secret image is encrypted using pixel-based swapping operation like swapping and circular shifting operation, then after performing the wavelet-based embedding to hide the scrambled secret image inside the cover image. The proposed technique flow is shown in figure-1.

The algorithmic steps of proposed technique are as follow:

1.  Input secret image
2.  Input cover image
3.  Perform circular sift and column swapping operation on secret image and get the scrambled image
4.  Perform wavelet based embedding process to hide scrambled image inside cover image
5.  Perform the pixel-based correlation on two nearest pixel by performing random flipping operation to improve stego image picture quality.
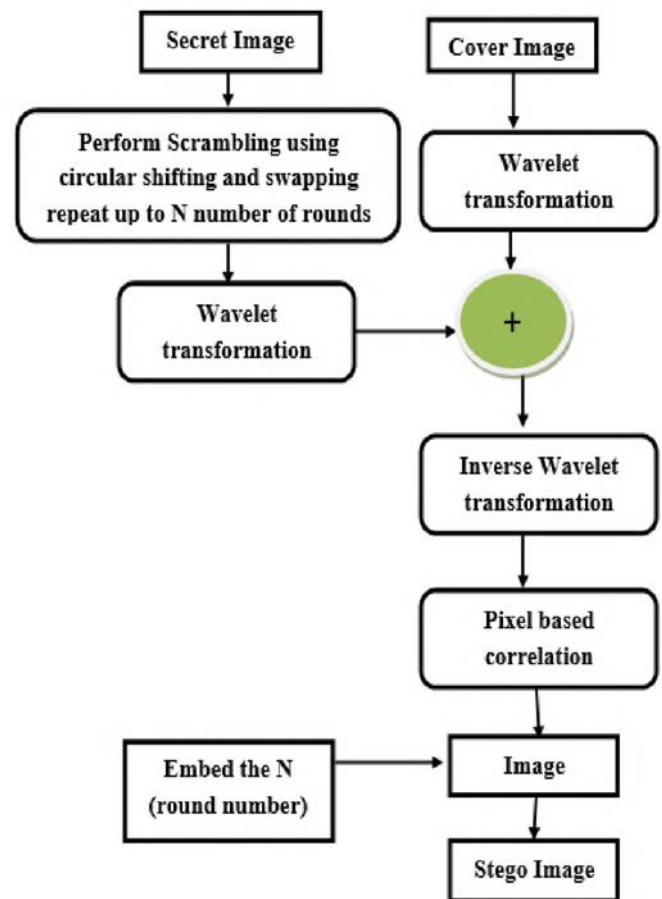6.  Hide round number inside the stego image



Figure 1. Embedding process

The extraction process of the proposed scheme is shown in the figure 2. The algorithmic steps are as follow:

1. Take cover image

2. Take stego image

3. Extract round number, which is hidden inside stego image

4. Perform wavelet based decoding process to get scramble secret image.

5. Descrambled the scramble image obtained from step 4 (using reverse step of Step3 in embedding process) and generate the secret image.
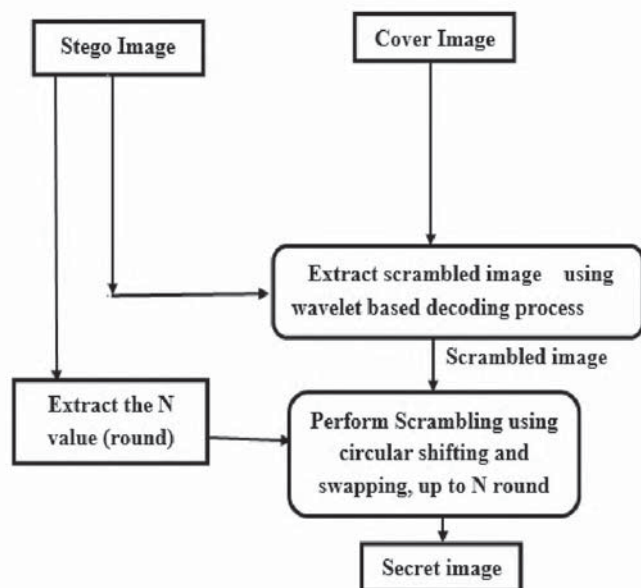
Figure 2: Extraction process

The figure 2 shows the complete extraction process of secret image from the stego image. The picture quality of all the images are shown in the results section. From the results, it is evident that strength of proposed technique is better than other approaches.
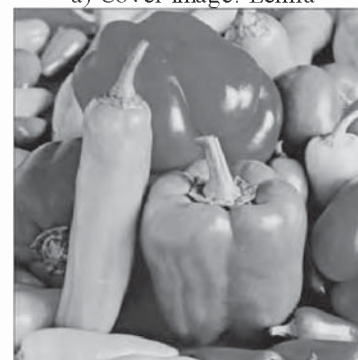
## IV    RESULTS

This section depicts the results obtained after processing the technique, for that MATLAB R 2019 version is used. All the results are derived for image size 256 X 256 images.
The figure 3-5shows the results obtained by the proposed technique on the different cover and secret image.

The results show the good quality of scrambled image and stego image can be generated after performing the proposed technique. There is no difference between the cove image and stego image. From the results it is said that the technique provides good results for both the scrambled secret image and the stego image.

In figure 3 cover image Lenna and secret image pepper are taken to derive the results
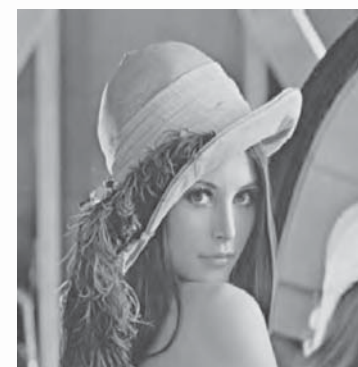


a) Cover image: Lenna



b) Secret image: Pepper



c) Scrambled image



d) Stego image
Figure3: Obtained results for cover image lenna and secret image peppers.
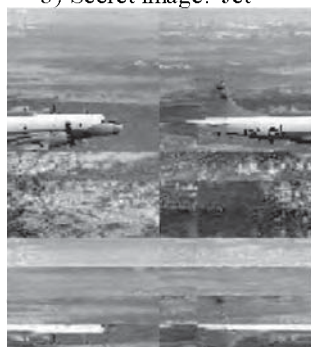
In next Figure 4 shows the results related to cover image Homi J. Bhabha and secret image Jet.

a) Cover image: Homi J. Bhabha
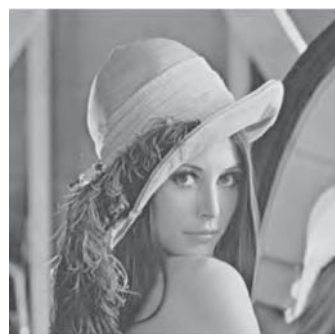


b) Secret image: Jet



c) Scrambled secret image



d) Stego image

Figure 4. Obtained results for cover image Homi J. Bhabha and secret image jet

In figure 5 cover image Lenna and secret image goldhill are taken.



a) Cover image: Lenna



b) Secret image: Goldhill



c) Scrambled image



d) Stego image

Figure 5. Obtained results for cover image Lenna and secret Goldhill

The numeric results of the proposed technique have been tested on the different image quality measurements. The parameters for image quality measurements are: peak signal to

noise ratio (PSNR), mean square error (MSE) [13], normalize crose correlation (NCC) [14], Average difference (AD) and structural contents (SC) [15], these are represented as:

Table 1. results related to PSNR and MSE

| Cover image | Secret image | PSNR (db) | MSE |
|---|---|---|---|
| Lenna | Peppers | 47.0654 | 7.4193e+04 |
| Homi J. Bhabha | Jet | 45.8443 | 9.8281e+04 |
| Lenna | Goldhill | 47.7825 | 6.2900e+04 |

From above table 1 it can be said that the achieved range of

PSNR is near around 45 to 47 Db.

Table 2. Results related to NCC and AD

| Cover image | Secret image | NCC | AD |
|---|---|---|---|
| Lenna | Peppers | 0.9933 | -0.9675 |
| Homi J. Bhabha | Jet | 0.9923 | -1.1220 |
| Lenna | Goldhill | 0.9938 | -0.8976 |

From above table, it can be said that the achieved range of NCC is near around 0.99 that is nearest to highest range 1.

Table 3. Results related to SC

| Cover image | Secret image | SC |
|---|---|---|
| Lenna | Peppers | 0.9867 |
| Homi J. Bhabha | Jet | 0.9847 |
| Lenna | Goldhill | 0.9877 |

Figure 6, figure 7 and figure 8 shows the obtained comparative results of image quality parameters in terms of PSNR, NCC, AD and SC for different cover image and secret image as shows in table 1 to table 3.
From the tables 1-3 it is observed that the NCC and SC values are near about to .99, which denotes excellent quality of stego image.
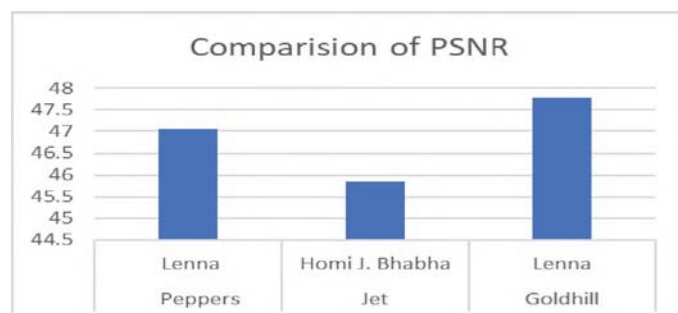


Figure 6. Comparison of PSNR

From the figure 6, it is observed that for cover image Lanna and secret image Goldhill with better PSNR can be obtained then the other cover images and secret images.
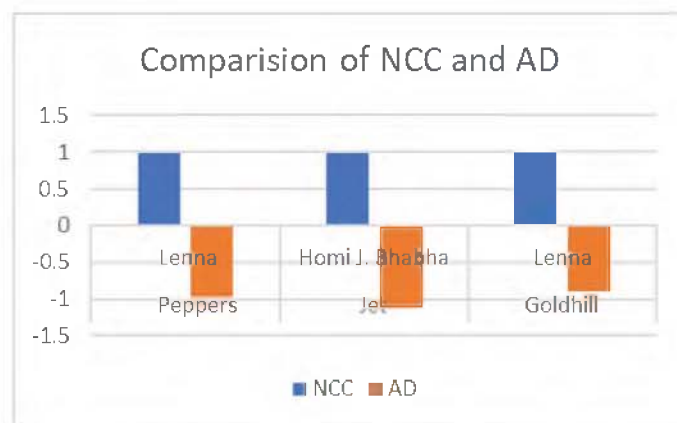


Figure 7. Comparison of NCC and AD

From the figure 7, it can observe that for cover image observe range of NCC is near about to 100% and AD is also very less. Which means excellent quality of stego image can be obtained.
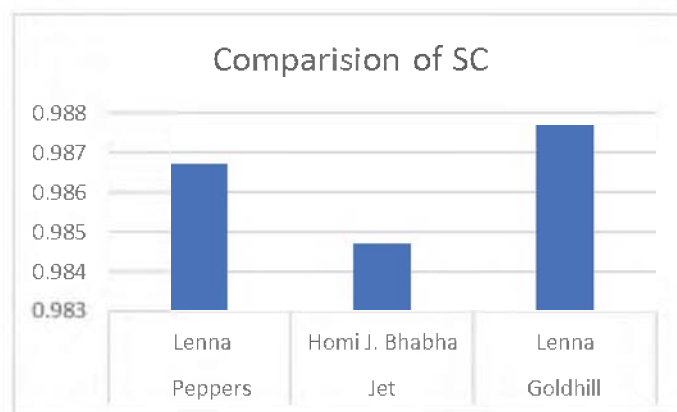


Figure 8. Comparison of SC

The observed range of SC is .98, which means the 98% similarity can obtained in between cover and stego image.

## IV    CONCLUSION

The proposed technique provides good results related on different parameters of image quality. From the results section the proposed technique provides good results In-terms of PSNR, NCC and Sc parameters and technique also give good results for AD. The technique gave good results for cover image Lenna and secret image Goldhill. And it also gave good results for cover image Lenna and secret image peppers.

### References:

[1]. Shrestha, A., Timalsina, A.: Color image steganography technique using Daubechies discrete wavelet transform. In: 9th International Conference on Software, Knowledge, Information Management and Applications (SKIMA), pp. 9–15 (2015)

[2]. Savita Goel, Shilpi Gupta and Nisha Kaushik, "Image Steganography –
Least Significant Bit with Multiple Progressions", Proc. of the 3rd Int. Conf.
on Front. of Intell. Comput. (FICTA) 2014, pp. 105-115.

[3]. J. Fridrich, M. Goljan & R. Du. Reliable Detection of LSB Steganography
in Grayscale and Color Images. Proc. ACM, Special Session on Multimedia
Security and Watermarking, Ottawa, Canada, 2001, 27–30.

[4]. Onkar Dabeer, Kenneth Sullivan and Upamanyu Madhow, "Detection of
Hiding in the Least Significant Bit", IEEE TRANSACTIONS ON SIGNAL
PROCESSING, VOL. 52, NO. 10, OCTOBER 2004 pp. 30

[5]. S Brindha, I Vennila, "Hiding Fingerprint in Face using Scattered LSB
Embedding Steganographic Technique for Smart card based Authentication
system", International Journal of Computer Applications 26 (10), 51-55, 2011.

[6]. A. Singh and H. Singh, "An improved LSB based image steganography
technique for RGB images," 2015 IEEE International Conference on
Electrical, Computer and Communication Technologies (ICECCT),
Coimbatore, 2015, pp. 1-4,

[7]. Ashish Sharma, Devesh Kumar Srivastava, "A Comprehensive View on
Encryption Techniques of Visual Cryptography", International Journal of
Recent Research and Review, Vol. 5, Issue 2, 87-94, June 2014.

[8]. J.B.Sharma, K.K.Sharma, and Vineet Sahula, "Hybrid image fusion
scheme using self-fractional Fourier functions and multivariate empirical
mode decomposition", Signal Processing, Volume 100, July 2014, Pages 146-
159.

[9]. Sharma, K.K., Sharma, M. Image fusion based on image decomposition
using self-fractional Fourier functions. SIViP 8, 1335–1344 (2014).

[10]. H. Ye, S. Huang and W. Liu, "Research on Image Scrambling Method
Based on Combination of Arnold Transform and Exclusive-or Operation,"
2020 IEEE 4th Information Technology, Networking, Electronic and
Automation Control Conference (ITNEC), Chongqing, China, 2020, pp. 151-
154.

[11] Inas Jawad Kadhim, Prashan Premaratne, Peter James Vial, Brendan
Halloran, Comprehensive survey of image steganography: Techniques,
Evaluations, and trends in future research, Neurocomputing, Volume 335,
2019, Pages 299-326.

[12] J. Qin, Y. Luo, X. Xiang, Y. Tan and H. Huang, "Coverless Image
Steganography: A Survey," in IEEE Access, vol. 7, pp. 171372-171394, 2019,
doi: 10.1109/ACCESS.2019.2955452.
[13]. Pradhan, A., Sahu, A.K., Swain, G., et al.: 'Performance evaluation
parameters of image steganography techniques'. Int. Conf. Research
Advances in Integrated Navigation Systems., 2016, pp. 1–8
[14]. Khalili, M., Asatryan, D.: 'Colour spaces effects on improved discrete
wavelet transform-based digital image watermarking using Arnold transform
map', IET Signal Process., 2013, 7, pp. 177–187
[15]. Prabakaran, G., Bhavani, R.: 'A modified secure digital image
steganography based on discrete wavelet transform'. Int. Conf. Computing,
Electronics and Electrical Technologies, March 2012, pp. 1096–1100