International Journal on Emerging Technologies 10(1): 64-67(2019)

ISSN No. (Print) : 0975-8364
ISSN No. (Online) : 2249-3255

# An Approach with Steganography and Scrambling Mechanism for Hiding Image over Images

**G. Manikandan[1], R. Bala Krishnan[2], E. Preethivi[1], K.R. Sekar[1], R. Manikandan[1] and J. Prassanna[3]**
[1]School of Computing, SASTRA Deemed University, (Tamil Nadu), INDIA
[2]Department of Computer Science, SASTRA Deemed university, Kumbakonam, (Tamil Nadu), INDIA
[3]VIT University, Chennai Campus, (Tamil Nadu), INDIA

(Corresponding author: G. Manikandan)
(Received 22 February 2019, Revised 20 April 2019 Accepted 02 May 2019)
(Published by Research Trend, Website: www.researchtrend.net)

**ABSTRACT: The projected scheme creates non imbrications image blocks from the confidential cover image. The blocks are then subjected to the projected Synthetic Ciphering scheme, which would generate the cipher image. The cipher image would then be subjected to LSB Substitution practice over another cover image. The outcome of the LSB substitution offers an Stego image, which would be channelized over the network path. The receiver needs to apply the LSB extraction to generate the cipher image and then Inverse Synthetic Ciphering needs to be applied to obtain the original image. The major benefit of such a proposed scheme is its lossless decomposition, efficiency and portability. Both experiments and analysis show the proposed scheme produces an adept cipher image, which flout the typical cipher assails. The potency of the projected scheme proves that it is suitable for image applications.**

**Keywords:** Enciphering, Cipher Image, Scrambling, Image Encryption, Steganography.

## I. INTRODUCTION

In modern era of network communication systems, the need for information security and transmission of confidential digital data such as images over the network medium is increasing in tremendous entailment. The basic individuality of the image in digitized form comprises a huge amount of data and proficient interrelations over the image pixels. Conventional crypto mechanisms like DES (Data Encryption Standard), IDEA (International data encryption algorithm) and AES (Advanced Encryption Standard) under the symmetric and Asymmetric key strategies aren't appropriate for image based ciphering systems, predominantly for real-time high end systems. To make improvements the overload concern of the traditional crypto mechanisms, Fridrich *et. al.,* suggested an picture enciphering architecture using baker maps with 2D discrete chaotic process, which is accumulated with critical mix-up and dissemination conventions [1]. With the attributes of uncertainty, nonperiodicity, nonconvergent and sensibility to starting constraints and attributes [2], the execution principles like pels reordering by following the locations have been extensively used to accomplish tenable lossless compression mode and are precise as the optimistic enciphering tradeoff model. At present, copious image encryption techniques have been recommended [3-4] and are clustered into unlike classes such as blocks transmutation and pels values replacement [5-6].

In this proposed research work, an image encryption model for digital binary images is presented, which is based on the proposed Synthetic ciphering pattern, which classes the image into blocks and on each blocks the pattern for pixel swapping is applied and it results a scrambled image, which is then subjected to LSB substitution over the digital color image otherwise called Cover image. The outcome of the enciphering and the hiding process generates a stego image, which would then be subjected for the transmission over the channel. The residual unit of the anticipated research exertion is structured as follows. The section II renders the concerned survey of digital image encryption. Anticipated scheme is affirmed in Section III and the experimental annotations are depicted in Section IV, Implication of the Proposed Approach in V. At last, the conclusion of the proposed practice with its qualities is stated in section VI.

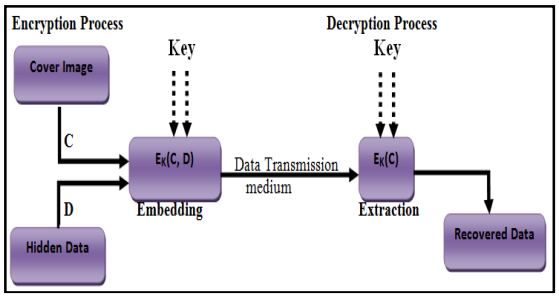


**Fig. 1.** Procedure for Content embedding and extraction.

## II. RELATED WORKS

In recent years, there are many covered writing techniques used to hide content for the attainment of secured data transmission. Due to the simple data structure of bitmap (BMP) format most of the researchers perform the embedding operations in the bitmap image format and the procedure is stated in Fig.1.

The equations for the embedding and extraction procedure is stated as follows

Embedding:

$$C \oplus K \oplus D \rightarrow C' \quad ...(1)$$

Extraction:

$$Ex\,(Em(c,k,d)) \approx d, \forall c \in C, k \in K, d \in D \quad ...(2)$$

*A. Least significant bit Substitution*

A novel information hiding method based on Multi-Pixel Differencing (MPD) is proposed by K.H. Jung *et al.,*.

The difference between 4 x 4 sub-blocks is calculated. The calculated differences are added to embed the cryptic content.
If the result is high on the edged block MPD method hides data in this region else the secret data is concealed in smooth region [7].
A novel scheme for least significant bit substitution (LSB) mechanism was offered by the authors Y. K. Jain et al. This spatial domain embedding scheme [8] divides the secret image pels ranges from zero to 255 and gives a stego-key. It also regulates the modification of cryptic content in the processed image (stego), which results in an eminent concealed capacity.
An adaptive substitution schema using LSB technique has been proposed. This approach exploits the edges, brightness and grain of the steg image to compute the number of S-bit LSB for information hiding [9]. To balance the visual tone of the image, the evaluated value of 'S' is rich at unrestricted area of the image. Similarly the calculated value of 'S' is considerably poor over tender area of the image. The LSB's (k) for embedding is calculated by the high-order bits of the image.
To attain new adaptive LSB steganographic scheme, C.-H. Yang et al., proposed adaptive data hiding scheme in the edge regions with direct manipulation of pixels [10]. The identified difference between the neighboring pels helps us to embed the cryptic content. The range of difference value is categorized into low level, middle level and high level.

## III. PROPOSED METHODOLOGY

For the input binary image I(m, n) of size 'm' x 'n' to be encrypted, the process of the proposed Synthetic Ciphering based image encryption is composed of two phases, block partitioning and pixel transformation. The detailed execution methodology is stated in Figure 2. The input images are partitioned in to blocks of size 'm' x 'n' and the blocks are then partitioned into blocks of size 'm1' x 'n1'. The input secret image has been classes into same size blocks and is then subjected to the proposed Synthetic Transformation process and the outcomes of the transformation process are combined to obtain the cipher image [11]
The cipher image is subjected to LSB Substitution over a Cover Image of Size 'M'x 'N' where M > m and N > n. The Substitution process generates the stego image, which is going to be transmitted over the network channel and at the receiver end the inverse of the LSB Substitution and Synthetic Transformation pattern is followed to obtain the original secret image (binary image). The execution methodology of the proposed scheme is stated in the Figure 2.
The complete sketch of the proposed image hiding procedure is presented as follows:
*Step_1:* The Input Binary image 'Img' is partitioned in to sub-blocks (S1, S2,…..Sn) of size m x n and then to m1 x n1.
*Step_2:* Determine the mid-location from each of the image blocks and consider the point as origin for pixel value transformations.
*Step_3:* After the swapping pattern on the block:
Swap the pixel (positive (x), 0) with (0, position(y)) and Swap the pixel (negative (x), 0) to (0, negative(y))
*Step_4:* Apply the Steps 3 on the all the image blocks created in Step_1.
*Step_5:* Obtain the final Cipher image CI.
The Cipher image CI is subjected to LSB Substitution process over the color image and the procedure is presented as follows:
*Step_1:* The Cipher image CI is subjected to binary stream conversion.

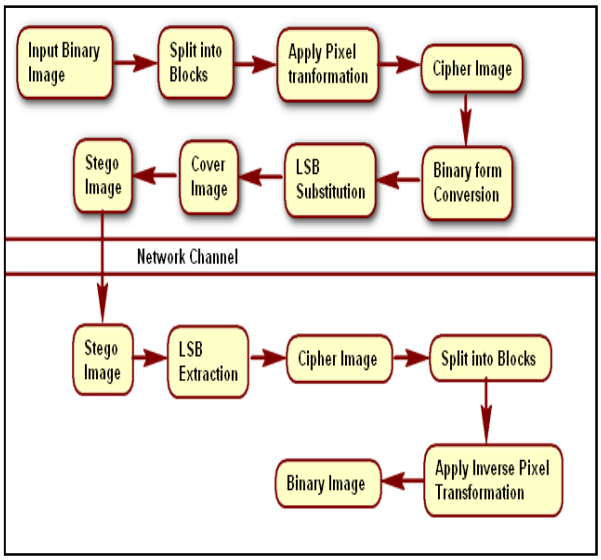


**Fig. 2.** Execution pattern of the anticipated embodiment.

*Step_2:* Apply the Step_1 for all the blocks and then apply LSB substitution over the color image which is of size 'M' x 'N' where M>m and N>n.
*Step_3:* The outcome of Step_2 is the image embedded Stego Image.

## IV. EXPERIMENTAL RESULTS

The anticipated IPC based Digital Image enciphering model has been implemented using C# DOTNET. The execution arrangement is evaluated on a system with the processor Pentium Core 2 Duo of 2.6 GHz with 4 GB RAM Capacity and the model has been executed on Windows 8 operating system. The experimentations are deported by reckoning the typical color cover images with resolution 1200 x 1200 and binary form input secret images with resolution 100 x 100.
The images which are taken as input for the experimentations are stated in the Figure 3 and Figure 4. The observed stego image with the secret content is posited in the Figure 5. From the observations, it is to be recognized that there are no visual diversity between the Cover and the Stego image. From the substantiation of the scrutiny, it is consummate that the anticipated method for digital image encryption grants a proficient information hiding practice for image based software applications. The final lossless extracted binary image at the receiver end is depicted in Figure 6, which is similar to the binary secret image [12]

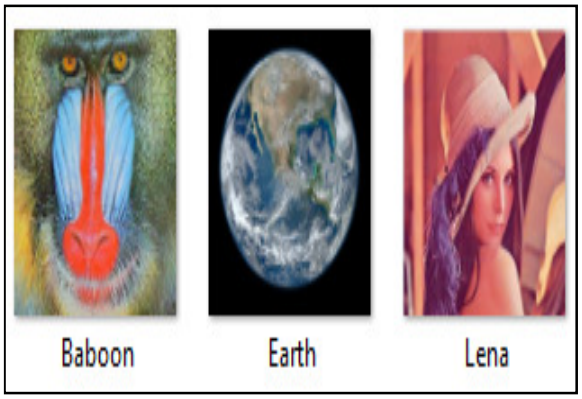


**Fig. 3.** Cover images.

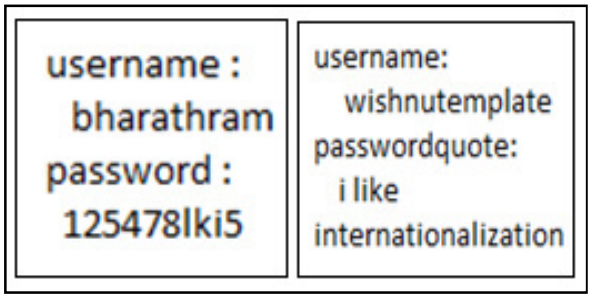


**Fig. 4.** Binary images hold the secret data.

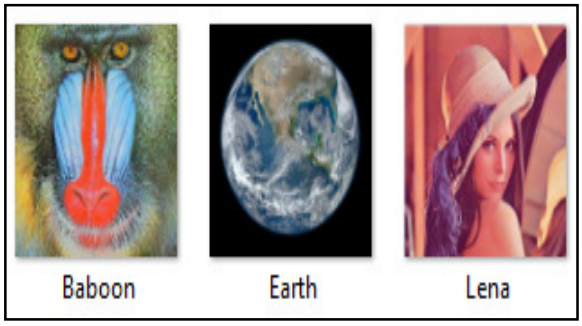


**Fig. 5.** Stego images.

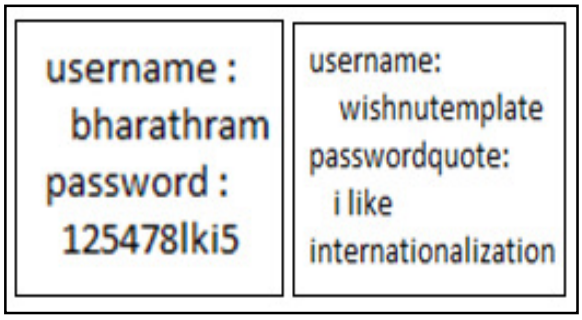


**Fig. 6.** Extracted Binary images at receiver end.

**Table 1: MSE comparison of Cover Image and Data Embedded image.**

| Cover Image | Quality Metrics | | |
|---|---|---|---|
| | MSE | | |
| | Red | Green | Blue |
| Baboon | 2443.15 | 2707.441 | 2440.42 |
| Earth | 10802.9 | 9795.237 | 8052.36 |
| Lena | 4210.54 | 3970.06 | 3745.05 |

**Table 2: PSNR comparison of Cover Image and Data Embedded image.**

| Cover Image | Quality Metrics | | |
|---|---|---|---|
| | PSNR | | |
| | Red | Green | Blue |
| Baboon | 14.251 | 13.805 | 14.256 |
| Earth | 7.795 | 8.221 | 9.072 |
| Lena | 11.887 | 12.142 | 12.396 |

.

## V. IMPLICATION OF THE PROPOSED APPROACH

In the normal steganographic approaches, the pixels accessing order needs to be known to extract the content but the proposed approach hold the first lock at image reconstruction at the receiver end; the second lock at the image scrambling process and then final complicated lock on the pels accessing order.

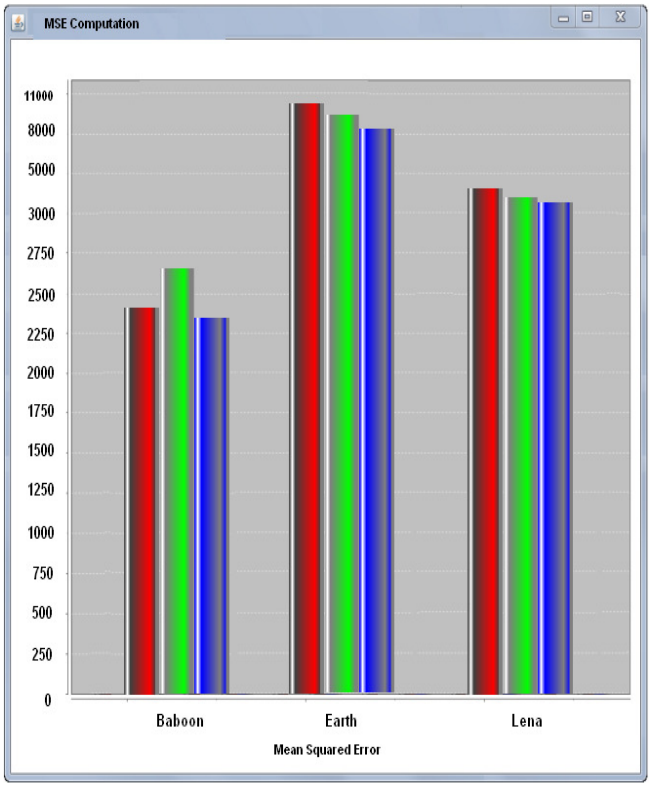


**Fig. 7.** MSE values for cover and stego images.

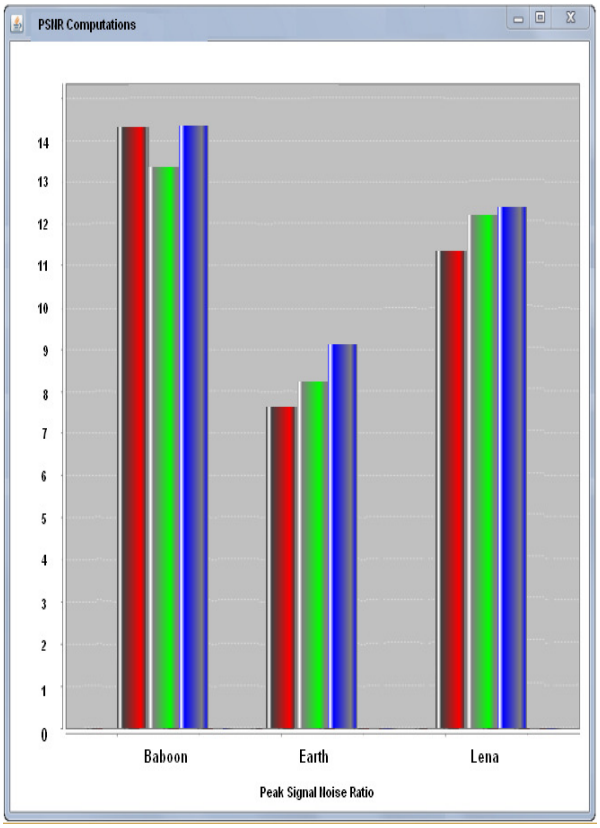


**Fig. 8.** PSNR values for cover and stego images.

## VI. CONCLUSION

The projected approach offers an efficient scheme for hiding an image over another image using LSB substitution scheme The image scrambling holds the lock on the image which needs to open to extract the content from the image. The significant feature of the proposed approach is that the image scrambling order, which holds the secrecy of the model and the scrambled image gets embedded over another image, which forms an additional lock on the secret content and it helps the network channel with fewer payloads as compared with the original image. At the receiver end the image can be perfectly reconstructed and the secret content gets extracted without any loss. From the experimental observations it is apparent that the proposed scheme offers a proficient methodology for information concealment over images. From the Table 1 and Table2, it is evident that the input cover image is having no significant difference with the stego image after the content embodiment which is represented graphically in Figure 7 and Figure 8.Focus on video data could be the future direction of this research work.

**Conflict of interest**: No

## REFERENCES


[1]. Fridrich, J. (1998). Symmetric ciphers based on two-dimensional chaotic maps. *International Journal of Bifurcation and chaos*, **8**(06): 1259-1284.

[2]. Zhang, G., & Liu, Q. (2011). A novel image encryption method based on total shuffling scheme. *Optics Communications*, **284**(12): 2775-2780.

[3]. Parah, S.A., Sheikh, J.A., Hafiz, A.M., & Bhat, G.M. (2014). Data hiding in scrambled images: A new double layer security data hiding technique. *Computers & Electrical Engineering*, **40**(1): 70-82.

[4]. Raghupathy, B.K., Kumar, N.R., & Raajan, N.R. (2014). An Enhanced Bishop Tour Scheme for Information Hiding. *International Journal of Applied Engineering Research*, **9**(1): 145-151.

[5]. Gu, G., & Ling, J. (2014). A fast image encryption method by using chaotic 3D cat maps. *Optik*, **125**(17): 4700-4705.

[6]. Manikandan, G., Kamarasan, M., & Sairam, N. (2013). A New Approach for Secure Data Transfer based on Wavelet Transform. *IJ Network Security*, **15**(2): 106-112.

[7]. Huang, X. (2012). Image encryption algorithm using chaotic Chebyshev generator. *Nonlinear Dynamics*, **67**(4): 2411-2417.

[8]. Jain, Y.K., & Ahirwal, R.R. (2010). A novel image steganography method with adaptive number of least significant bits modification based on private stego-keys. *International Journal of Computer Science and Security*, **4**(1): 40-49.

[9]. Yang, C. H., Weng, C. Y., Wang, S. J., & Sun, H. M. (2008). Adaptive data hiding in edge areas of images with spatial LSB domain systems. *IEEE Transactions on Information Forensics and Security*, **3**(3): 488-497.

[10]. Yang, H., Sun, X., & Sun, G. (2009). A high-capacity image data hiding scheme using adaptive LSB substitution. *Radio engineering*, **18**(4): 509-516.

[11]. Muhammad K., Sajjad M., Mehmood I., Rho S., Baik S.W. (2018). Image steganography using uncorrelated color space and its application for security of visual contents in online social networks. *Future Generation Computer Systems*. **86**: 951-60.

[12]. Mukherjee S, Roy S, Sanyal G. (2018). Image Steganography Using Mid Position Value Technique. *Procedia computer science,* **132**: 461-8.



**How to cite this article:** Manikandan, G., Bala Krishnan, R., Preethivi, E., Sekar, K.R., Manikandan, R. and Prassanna, J.(2019). An Approach with Steganography and Scrambling Mechanism for Hiding Image over Images. *International Journal on Emerging Technologies,* **10**(1): 64-67.