# An Efficient Image Steganography using Hybrid GA-PSO

Saurabh Paliwal
Department of Computer Science & Engineering
T.I.T.S
Bhopal, India
saurabh.paliwal34@gmail.com

Prof. Rajesh Kumar Nigam
Department of Computer Science & Engineering
T.I.T.S
Bhopal, India
Rajeshrewa37@gmail.com

**Abstract—**Image Steganography is a technique of encrypting the images so that the hidden information can be made secure from unauthorized users. The Existing Genetic Algorithm based Image Steganography provides Zero Mean Square Error for Decrypting the Images, but degrade the Peak Signal to Noise ratio as well Perceptual Quality Measure of image. Hence a new and efficient technique is implemented here for the Optimization of Genetic Algorithm (GA) using Particle Swarm Optimization (PSO). The Proposed methodology improves the encryption ratio as well as also provides less Mean Square Error for Encryption and decryption and high Peak Signal to Noise Ratio.

**Index Terms—**Visual Cryptography, Image Steganography, Information Hiding, LSB, Genetic Algorithm, Particle Swarm Optimization.



## I. Introduction

With the increasing form of digital visual media, the growing require for objective quality assessment that correlates well with subjectively distinguished quality has been recognised as an influential device for system design and optimisation. Especially in recent years, the efforts in visual quality assessment have increased considerably, leading to a number of quality metrics that have been proposed. More and more things are increasingly digital, such as photos, videos, music, documents, personal information, and so on. Therefore, how to protect digital information is a hot issue. Cryptography and steganography are two popular technologies used to protect digital products. Basic steganography diagram is shown in figure1. In the basic steganographic process, the secret message is hidden into a cover object. The cover object can be any of text, image, audio, video etc [1]. After the embedding process, the stego image should look matching to the cover image and be challenging to normal analysis in order to avoid raising suspicion. A stego key is typically utilized in the embedding process to improve security since only the person who knows it will be able to extract the secret message. The expression payload is utilized to explain the size of the secret message that can be embedded in a particular image. A secret key is also used and the secret message is embedded into the cover object using the secret key. This novel message acquired is called stego message. The stego message is transmitted over the public channel. The receiver gets the message and retrieves the message using the stego key which is same as used by the sender. In this technique security is accomplished by hiding the continuation of the message.

Image steganography is a development that hides the message into cover-image and produces a stego-image. That stego-image then sent to the receiver without anyone else identifying that it contain the hidden message. The receiver can remove the message with or without stego-key that depends on the hidden method [2].

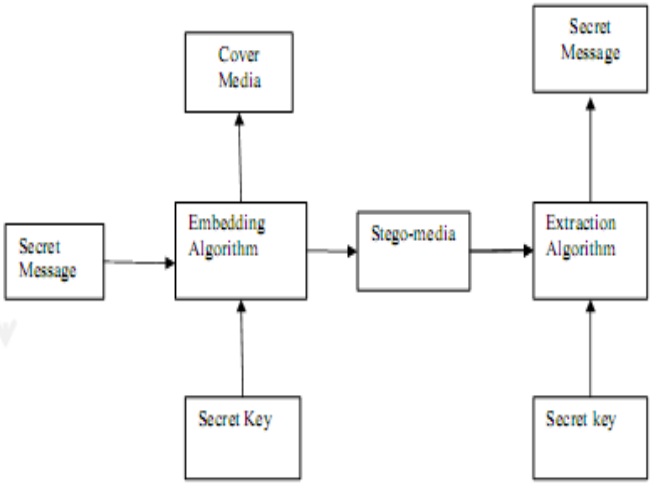

Figure-1: Basic Steganographic process.

Utilizing digital signal processing and digital imaging technologies to conceal secret data without reducing the quality of the cover image is called data hiding. This technique is not enthusiastically perceptible and hides information in any form (text, images, and video). The present research in the area of information hiding can be usually classifed in three sub fields; Spatial domain, Frequency Domain and Adaptive domain methods. In the Spatial domain [3], the way of hiding data is the direct manipulation of the pixel values of a cover medium. In the Frequency Domain techniques, such as DCT (Discrete Cosine Transform) and DWT (Discrete Wavelet Transform), the information is embedded in the transform coefficients of the cover medium. In the Adaptive domain, the model human visual systems are used and exploits assured image characteristics like luminance, corners, edges to embed information in cover medium [4–6]. Least Signifcant Bit (LSB) substitution [7], [8] is most commonly used method that substitutes the pixels in the cover image with secret data bits to get stego-image. Here the data to be protected is embedded in the least signifcant bits of the cover image. Te LSB substitution method is straightforward to put into practice as embedding and removing procedures do not need difficult calculations. In [9], a steganography technique based on GA is accessible which is protected against RS attacks. This technique in first step embeds secret bits into host image just like uncomplicated LSB and in second step modifies pixel values to make stego image RS factors be seated in protected area.

## II. Literature Survey

In this paper [10], here author has try to find best position for embedding modified secret data in host image to realize high level of protection. The process of embedding is completed in two major steps: Initially it was to modify secret bits and another one is to embed it into host image. Different places in host image described by arrange of scanning host pixels and initial point of scanning and best LSBs of each pixel. Additional choices of host bits are characterized too. Here they propose a tunable visual image quality and data lossless method in spatial domain based on a genetic algorithm (GA). The most important design of the recommended method is modeling the steganography difficulty as an exploration and optimization difficulty. It developed to discover the most excellent initial point, scanning categorize and extra preferences such that the PSNR of the stego-image maximized. An achievability and use examination for the proposed method is performed using some standard images. The scheme [10] presentation is evaluated with the presentations of some earlier well-liked subsisting methods. Experimental results shown that currently popular steganography of proposed algorithm is better and consistent not only accomplishes high embedding competence but also improves the PSNR of the stego image.

In this paper [11], a steganography and authentication based secret image sharing method is proposed. In this scheme, the authentication is put into practiced by the idea of CRT was suggest an enhanced method to develop authentication capability and cannot only recover the value of the stego images. As extreme as the quality of the stego images is anxieties, it depends on the number of the hidden shared pixels. The smaller amount shared pixels are concealed, the better visual quality of the stego images can be guaranteed. To the extent that the authentication capability is feared, the use of CRT creates the collaboration applicants be capable to confirm truthful ones simply. Accordingly, the proposed method can accomplish high authentication capability at specifically all applicants can authenticate each other disquieting the authority of the stego images before modernizing the secret image. The experimental results also demonstrate that the proposed method can accomplish both the high PSNRs of the stego images and the enhanced authentication among the contrasted techniques.

In this paper [12], author proposes a novel reversible steganographic method based on the SMVQ concept for vector quantization (VQ) compressed images. Both input and output of our embedding technique are justifiable VQ compressed codes. In that technique, a hit pattern is utilized to contract with inconsistency cases. The novel technique utilizes the hit pattern to accomplish reversibility and the hit pattern approach effectively decreases the transparency. The codebook is partitioned by the expansion technique which creates the stego-image have good visual characteristics. Also, here they use a look-up table to speed up the partitioning process. As their technique not only reduces the overhead of the hit pattern, but also enhances the embedding capacity. The experimental results demonstrate that the proposed technique has superior capacity, improved visual quality, and lower operation time.

In this paper [13], here they suggest a new secret image sharing method by concerning optimal pixel adjustment procedure to improve the image quality under unusual payload capability and a variety of authentication bits conditions are block-wise and considered in the spatial domain. For this explanation, gray scale or gray level images are extensively utilized for hiding data. Generally, these

methods separate cover images into non-overlapping 2 × 2 blocks and in a straight line put back the least significant bits of pixels in each bock with the secret share and authentication code. The reinstating procedure may initiate some alteration or manufactured articles in the stego-image. Here author [13] has initiated one of the enhanced techniques called the optimal LSBs method in this script. The technique can significantly develop the image quality by concerning an optimal pixel adjustment procedure to the stego-image. Here they also make available numerous experiments to exhibit the effectiveness of authentication competence of the proposed method.

Here author present a strong steganographic method recognized in entire its steps in the wavelet domain using the benefits of wavelet decomposition accessible based on color local complexity estimation based steganographic (CLCES) technique [14] that is proficient of both preventing visual degradation and on condition that the high image quality methods with a reasonable embedding capacity. The embedding capacity for each pixel is established by the local complexity of the cover image, permitting good visual quality in addition to embedding a huge amount of secret messages. Three different descriptions of the proposed technique are accessible using different criteria to hide data to make available cooperation between embedding capacity and image visual quality. A preprocessing phase is functional in the proposed method to get better the steganography security and they categorize the pixels using a threshold based on the standard deviation of the local complexity in the cover image to make available cooperation between the embedding capacity and the image visual quality. The experimental results exhibited that the steganographic algorithm CLCES suggested [14] creates insignificant visual distortion due to the hidden message. It makes available a high embedding capacity that is better-quality high opinion to the presented by the presented methods. The suggested technique is a protected steganographic algorithm; it can refuse to go along with the image quality determines (IQM) steganalysis attack. The RGB, YCbCr, and HSV color spaces are integrated in the proposed method to make sure that the difference between the cover image and the stego-image which is impossible to differentiate by the human visual system (HVS). Finally, the proposed method is straightforward, well-organized, and reasonable for the adaptive steganographic functions.

In this paper [15], author has propose a new steganography method that uses contourlet transform for hiding secret data in image. In this method, they first apply contourlet transform on image and then hide secret data in proper contourlet coefficients. The human visual system has been tuned so as to capture the essential information of a natural scence using a least number of visual active cells. So, an efficient image representation should be based on a local, directional and multiresolution expansion. In this method we embed data in non-smooth region of carrier image. So, the visual degradation is minimal. Here they examine their algorithm by a well-known steganalysis method and they found that it couldn't discriminate between cover and stego images with rate better than random guess.

## III. Proposed Methodology

The Proposed methodology implemented here for the Visual Cryptography of Image Steganography consists of following steps:

1. Take an input Image.
2. Apply Genetic Algorithm for providing the Cryptography to the secrete image.
3. Optimization of genetic Algorithm using Particle Swarm Optimization.

**Particle Swarm Optimization**

| Parameter | Summary |
|---|---|
| I | Particle Index |
| K | Discrete time index |
| V | Velocity of the ith particle |
| X | Position of ith particle |
| P | Best position found by ith particle |
| G | Best position found by swarm |
| $\gamma_{1,2}$ | Random numbers on the interval [0,1] applied to ith particle. |

Table 1. Basic Notations used in PSO

1. For each particle initialize particle
2. Repeat for each particle
   a). Calculate fitness value
   b). If the fitness value is better than best fitness value (Pbest) in history, set current value as the new Pbest.
3. Choose the particle with the best fitness value of all the particles as the Gbest.
4. For each particle
   a).Update particle velocity
   b).Update particle position.
5. until stopping criteria.

**Algorithm for PSO**

Start with the Initialization of Population

While! ( Ngen || Sc)

For p=1 :Np

If fitness Xp> fitness pbestp

Update pbestp = Xp

For

If fitness Xk>gbest

Update gbest = Xk

Next K

For each dimension d

$$v_{pd}^{new} = w * v_{pd}^{old} + c_1 * rand_1 * (pbest_{pd} - x_{pd}^{old}) + c_2 * rand_2 * (gbest_d - x_{pd}^{old})$$

(3)

$$v_{pd} = \max(\min(V_{max}, v_{pd}$$

Next d

Next p

Next generation till stop

**BASIC STEPS OF GA**

1. Start
2. T1=0 (here T1 is the initialization time to start)
3. Initialize the population of genetic p1(T1) ( initialize a usually random population of individuals)
4. Now Compute and calculate the fitness value p1(T1)
5. T1=T1+1
6. Check if the termination criterion satisfies
7. If yes then move and achieved go to step 10
8. Now select p1(T1) from p1(T1-1)
9. crossover both the populations p(T1)
10. and Mutate these populations p(T1)
11. Now go to step 3
12. output the best population and stop
13. End

## IV. Result Analysis

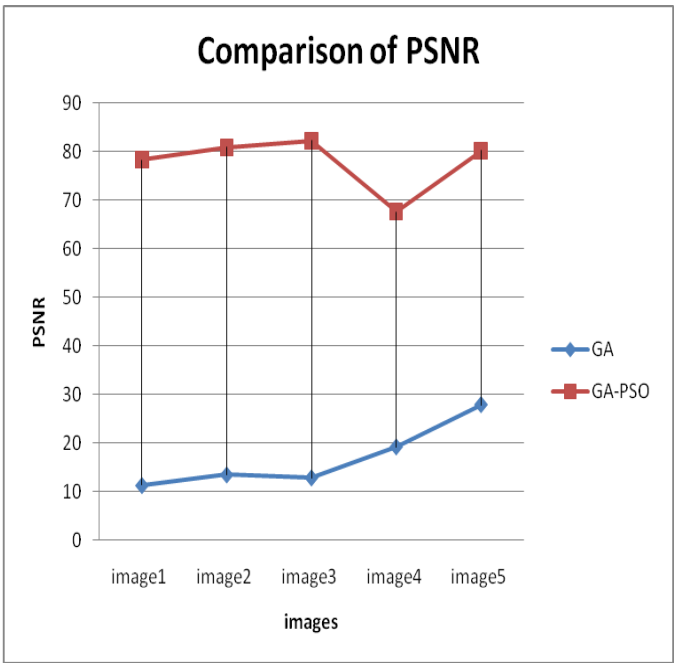


Figure 2. Compaison of PSNR

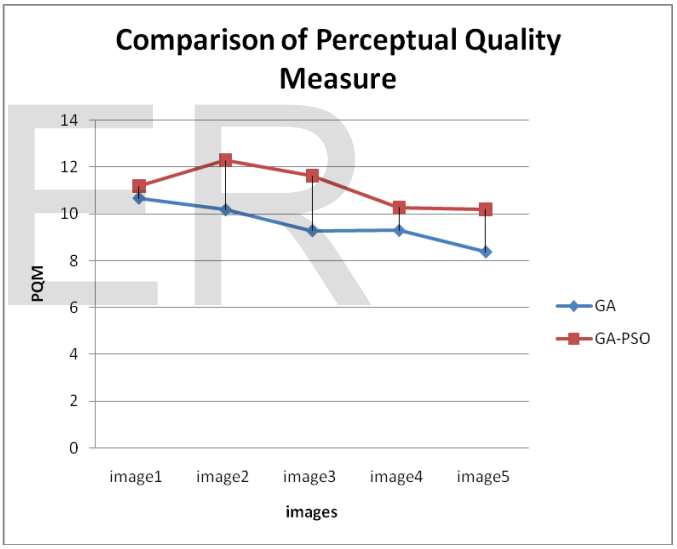


Figure 3. Comparison of PQM

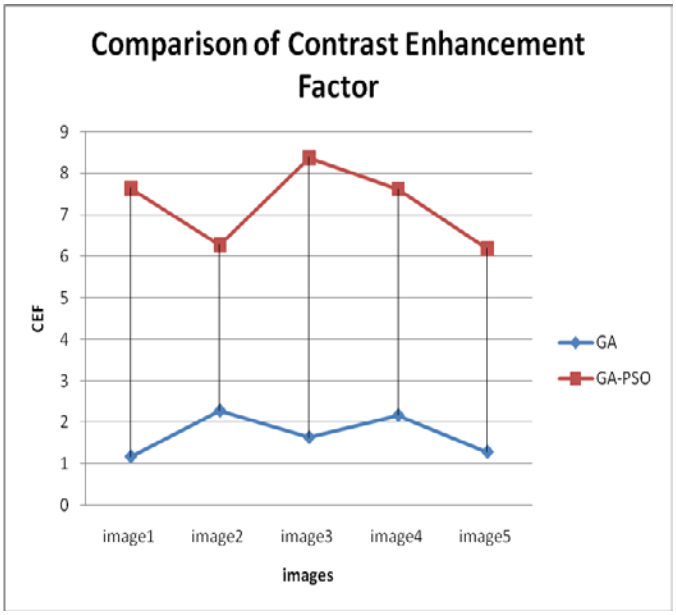


Figure 4. Comparison of CEF

| | PSNR | |
|---|---|---|
| **Images** | **GA** | **GA-PSO** |
| image1 | 11.28 | 78.29 |
| image2 | 13.46 | 80.84 |
| image3 | 12.85 | 82.26 |
| image4 | 19.2 | 67.65 |
| image5 | 27.86 | 80.16 |

Table 1. Analysis of PSNR

| | MSE | |
|---|---|---|
| **Images** | **GA** | **GA-PSO** |
| image1 | 1.54E+03 | 0.3 |
| image2 | 1.39E+03 | 0.4 |
| image3 | 2.58E+03 | 0.9 |
| image4 | 3.48E+03 | 0.3 |
| image5 | 2.39E+03 | 0.2 |

Table 2. Analysis of MSE

| | PQM | |
|---|---|---|
| **Images** | **GA** | **GA-PSO** |
| image1 | 10.659 | 11.175 |
| image2 | 10.165 | 12.284 |
| image3 | 9.275 | 11.619 |
| image4 | 9.285 | 10.264 |
| image5 | 8.3765 | 10.193 |

Table 3. Analysis of PQM

| | CEF | |
|---|---|---|
| **Images** | **GA** | **GA-PSO** |
| image1 | 1.175 | 7.642 |
| image2 | 2.285 | 6.284 |
| image3 | 1.64 | 8.372 |
| image4 | 2.175 | 7.629 |
| image5 | 1.287 | 6.185 |

Table 4. Analysis of CEF

.

## V. Conclusion

The Methodology adopted here for the Optimization of Genetic Algorithm using Particle Swarm Optimization for Image Steganography provides secure and efficient Encryption of Images. Here Experimental results are performed on various images and comparison is done between Genetic Algorithm and GA-Particle Swarm optimization, where Propose methodology provides high PSNR and MSE.

## References

[1] Cheddad, A. et al. Digital image steganography: Survey and analysis of current methods. Signal Processing, 90(3), 727–752. 2010.

[2] Johnson, N.F. & Jajodia, S. “Exploring Steganography: Seeing the Unseen”, Computer Journal, 1998.

[3] Peng R, Varshney PK. A human visual system-driven image segmentation algorithm. J Vis Commun Image R. 2015; 26:66–79.

[4] Parah SA, Sheikh JA, Hafz AM, Bhat GM. Data hiding in scrambled images: a new double layer security data hiding technique. Comput Electr Eng. 2014; 40:70–82

[5] Kanan HR, Nazeri B. A novel image steganography scheme with high embedding capacity and tunable visual image

quality based on a genetic algorithm. Expert Syst Appl. 2014; 41:6123–30.

[6] Valarmathi, Nawaz GMK. Secure data transfer through audio signal with LSA R. Indian Journal of Science and Technology. 2015 Jan; 8(1):17–22.

[7] Digital image steganography using nine-pixel diferencing and modifed LSB substitution gandharba swain. Indian Journal of Science and Technology. 2014 Sep; 7(9):1444–50.

[8] Swain G. Digital image steganography using nine-pixel differencing and modifed LSB substitution. Indian Journal of Science and Technology. 2014; 7(9):1444–50.

[9] Wang, S., Yang, B., & Niu, X. (2010). A secure steganography method based on genetic algorithm. Journal of Information Hiding and Multimedia Signal Processing, 1(1), 28–35.

[10] Hamidreza Rashidy Kanan , Bahram Nazeri, "A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm" Expert Systems with Applications 41 (2014) 6123–6130.

[11] Chin-Chen Changa, Yi-Pei Hsiehb, Chia-Hsuan Lin, "Sharing secrets in stego imageswith authentication" Pattern Recognition 41 (2008) 3130 – 3137

[12] Cheng-Hsing Yang, Cheng-Ta Huang, Shiuh-JengWang, "Reversible Steganography Based on SideMatch and Hit Pattern for VQ-Compressed Images" Fifth International Conference on Information Assurance and Security, 2009.

[13] Chia-Chun Wu, Shang-Juh Kao and Min-Shiang Hwang, "A High Quality Image Sharing with Steganography and Adaptive Authentication Scheme" 2012.

[14] lanca E. Carvajal-Gamez, Francisco J. Gallegos-Funes , Alberto J. Rosales-Silva, "Color local complexity estimation based steganographic (CLCES) method" Expert Systems with Applications 40 (2013) 1132–1142.

[15] Kolsoom Shahryari, Mehrdad Gholami. "High Capacity Secure Image Steganography Based on Contourlet Transform" Advances in Computer Science: an International Journal, Vol. 2, Issue 4, No.5, September 2013.