Sparse Image Reconstruction by employing Adaptive Gradient Algorithm in Image Steganography

Raghu K[1] , Shaikh Mohammad Faiyyaz [2] , Siddiqui Huzaif Halim[3] ,Sachin[4], Rakesh Das[5]

[1]School of Electronics and Communication Engineering, REVA University, Karnataka, India.
[2]School of Electronics and Communication Engineering, REVA University, Karnataka, India.
[3]School of Electronics and Communication Engineering, REVA University, Karnataka, India.
[4]School of Electronics and Communication Engineering, REVA University, Karnataka, India.
[5]School of Electronics and Communication Engineering, REVA University, Karnataka, India.

[1]raghuk@reva.edu.in,[2]706fiyaz@gmail.com,[3]huzaif.hs59@gmail.com,[4]sachinvy36@gmail.com,[5]apexrakesh97@gmail.com.

Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 10 May 2021

Abstract: Image steganography is a well-known technique to transmit a secret message in the form of image from one place to another without giving even a small sense to the third party. Stego attack is a common problem in the field of image steganography. However secure is the key and the algorithm, the third party may attack/jam the secret message which is being communicated. This paper deals with solution to such stego attack problem by involving two levels of security and by employing sparse based image reconstruction technique to retrieve the jammed/corrupted secret message. In this paper, two models for image steganography is proposed by involving adaptive gradient algorithm for secret image reconstruction. The stego attacked/corrupted secret image can be completely reconstructed from its very few non-corrupted image pixels by adaptively estimating the gradient of the error function with respect to the pixels to be estimated subjected to l_1-norm for including sparsity in the transform domain of the image. Results obtained from the simulation shows that this proposed method performs better with respect to peak signal to noise ratio and computation time as compared with other conventional image filtering techniques.

Keywords: Image Steganography , LSB Substitution Method , Sparse Image Reconstruction, Adaptive Gradient Algorithm.

1. Introduction

In this current digital world, data transmission over a communication network is utmost essential. At the same time, the security of the data transmitted over the network is also equally important. Especially in some applications like forensic department, military department and telecommunications of navy and airforce sectors, the data that is being transmitted from one place to another needs to be highly secure from the third party attack. A small security bleach of any information will lead into high risks in terms of nation or our country. In fields like these, it is essential for secret communication.

Secret communication can be broadly classified into two categories as data encryption and data hiding. Data encryption is a technique of gambling or ciphering the secret message using a particular secret key such that the message will be converted to a form which cannot be decrypted by any other third party until and unless, he/she has the secret key. In data hiding techniques, the secret message may/may not be encrypted, but it will be hidden inside any other multimedia signal like video, image, audio etc. This technique fools the third party to believe that a common non-secret communication is happening between the two end-points. For example, if an image of nature is sent from one point to another point over a network, nobody will give a thought that it contains some hidden secret information, hence avoiding secret data attacks. This method of hiding a secret data inside any other multimedia signal is a well known technique called as steganography. The secret information which will be hidden can be a text, image, audio or a video, which will be of lesser data size when compared to the multimedia signal inside which the secret information needs to be hidden. This multimedia signal used for carrying hidden information is called as cover signal. An image is extensively used as cover file to carry the secret message and this technique is known as Image Steganography. The classification of steganography is as shown in Fig 1.

The are many researchers currently and previously working on developing various steganography techniques. These image steganography techniques should exhibit simple architecture/technique, high security, high data hiding capacity, good peak signal to noise ratio of the stego image and more immune to the stego attacks. Several papers have presented different algorithms and techniques for image steganography, one such famous and yet simple technique is image steganography based on LSB substitution [1]. This is a spatial domain approach for hiding the information inside the cover image. Other papers in [2] and [3], present the image steganography technique in transform domain using discrete cosine transforms, wavelet transforms etc. In recent years, [8] paper presented a novel technique for image steganography in transform domain using integer wavelet transforms with variable bit length, where the secret data was hidden in IWT coefficients of cover image and with a variable length of secret message bits per IWT coefficient of cover image.

In [2], the survey focuses on comparison study of image steganography. This paper presented the performance comparison of several image steganography algorithms both in transform and spatial domains.

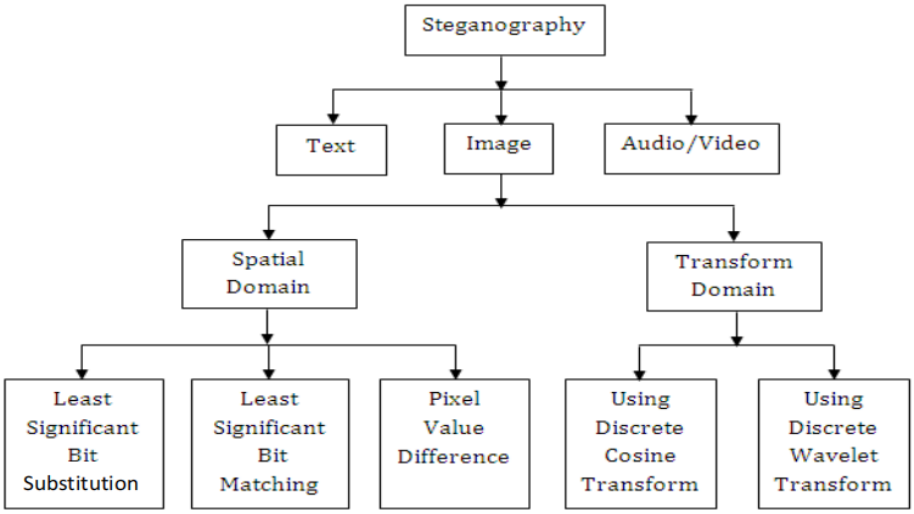

Fig 1 Classification of Steganography

In [3], the survey focuses on comparative study of image steganography; a detailed literature review on a variety of different methods, algorithms, and schemes in image steganography is conducted. In [4], the paper focuses on data hiding in transform domain with text and image as the secret information. This paper [5] presented the process of embedding the message in the image and generating a stego-image from the cover image which will be in an unpredictable format that the attacker s and eavesdroppers can't able to access the secret message inside the cover image.

Sparsity based signal reconstruction is the current hot-topic in signal processing area applied to problems such as linear regression, spectrum sensing, direction of arrival estimation [6],[7] etc. This technique of signal reconstruction can be applied for image reconstruction, where a high resolution, good quality image has to be reconstructed from a very few measured pixel samples. In Image steganography, stego attacks are the major problem, where a third party will either try to hack the secret data transmitted or will try to break the secret communication by intentionally adding noise to the cover image transmitted. In such cases, it is very much required to reconstruct the intentionally corrupted image. There comes the application sparse based image reconstruction algorithms to overcome stego attacks and also to provide an another layer of security to the transmitted secret message.

2. Sparse image reconstruction by adaptive gradient algorithm

The technique of sparsity based signal reconstruction can also be extended for image reconstruction; as image can be interpreted as 2D signal. Consider an image corrupted by salt and pepper noise, where only some of the image pixels are corrupted by salt and pepper noise whereas the remaining image pixels are non-corrupted original pixels. From these set of few non-corrupted original image pixels it is possible to reconstruct the other noisy pixels by employing sparse signal reconstruction.

The concept of sparsity can be applied in the sense that the image reconstruction is achieved from a very few samples of noiseless pixels. Also, an image is sparse in its frequency domain and sparsity based image reconstruction can be achieved. The salt and pepper noise corrupted image pixels can be easily identified, discarded and can be marked as unavailable pixels to be estimated, whereas the noiseless pixels are the available measurements [5].

A noise corrupted image of size RxS is first converted to 1D signal vector before applying sparse signal reconstruction technique. Consider **x** (Nx1**)** as the 1D array of salt and pepper noise corrupted image pixels (N=RS). Let this **x**contain M (M<N) number of noiseless pixels given by $\mathbf{y} = [x(n_1), x(n_2)\ldots..x(n_M)]^T$. Therefore, this **x** contains N-M number of noisy pixels given by $\mathbf{y_c} = [x(n_{M+1}), \ x(n_{M+2})\ldots.. \ x(n_{N-M})]^T$. From the set of measurements **y**, the algorithm needs to estimate $\mathbf{y_c}$.

Let **P** be the set of index positions of noiseless pixels in **x** given by **P** = [n_1, n_2…..n_M] and let **Q** be the set of index positions of noisy pixels in **x** given by **Q** = [n_{M+1}, n_{M+2}….. n_{N-M}]. We know that any image can be transformed into its frequency domain and vice-versa using Discrete Cosine Transform (DCT) as given in equation (1) and (2).

$$\boldsymbol{X} = \boldsymbol{\phi x} \#(1)$$
$$\boldsymbol{x} = \boldsymbol{\psi X} \#(2)$$

Where, $\boldsymbol{\phi}$(NxN)and$\boldsymbol{\psi}$(NxN)are DCT and inverse DCT matrices respectively.

The problem statement of sparse image reconstruction can be interpreted as in equation (3).

$$estimate' \boldsymbol{y_c}' \quad subjectto \min\|\boldsymbol{X}\|_1 \#(3)$$
$$estimate' \boldsymbol{y_c}' \quad s.t \min\|\boldsymbol{\phi x}\|_1 \#(4)$$

Solving this l_1-minimization problem using gradient-descent method[], we get an iterative estimation of $\mathbf{y_c}$as given in equation (5).

$$\boldsymbol{y_c}^{(m+1)} = \boldsymbol{y_c}^{(m)} - \alpha \frac{\partial\|\boldsymbol{\phi x}\|_1}{\partial \boldsymbol{y_c}}\Big|_{y_c = y_c^{(m)}} \#(5)$$

Where, m represents the particular iteration and α represents the step size of the gradient descent.

Letting $\frac{\partial\|\boldsymbol{\phi x}\|_1}{\partial \boldsymbol{y_c}}\Big|_{y_c = y_c^{(m)}} = \boldsymbol{g}^{(m)}$ which is the gradient of sparsity measure of **X** at $\mathbf{y_c}^{(m)}$ can be determined by finite difference method[]. The n_i^{th} coefficient of gradient vector $\boldsymbol{g}^{(m)}$ is then given by equation (6).

$$g^{(m)}(n_i) = \frac{\|\boldsymbol{\phi z_1}^{(m)}\|_1 - \|\boldsymbol{\phi z_2}^{(m)}\|_1}{2\Delta} \#(6)$$

Where $\mathbf{z_1}$and $\mathbf{z_2}$are the two full sets of measurements for each noisy missing pixel $n_i \epsilon \mathbf{Q}$ constructed by either increasing or decreasing the missing pixel value by Δ as given in equation (7) and (8).

$$z_1^{(m)}(n) = \begin{cases} y(n) & for n \in \boldsymbol{P} \\ y_c^{(m)}(n) + \Delta & for n \in \boldsymbol{Q} \end{cases} \#(7)$$
$$z_2^{(m)}(n) = \begin{cases} y(n) & for n \in \boldsymbol{P} \\ y_c^{(m)}(n) - \Delta & for n \in \boldsymbol{Q} \end{cases} \#(8)$$

Therefore, equation (5) reduces to equation (9):

$$\boldsymbol{y_c}^{(m+1)} = \boldsymbol{y_c}^{(m)} - \alpha \boldsymbol{g}^{(m)} \#(9)$$

Table 1. The Proposed Sparse adaptive gradient algorithm

Input Parameters: **y** ,$\boldsymbol{\phi}$, α, **P**, **Q**
Output Parameter: **x**

1. m←0
2. Initialize $\mathbf{y_c}^{(0)}$ = [**0**]
3. $\Delta \leftarrow \max_n |\boldsymbol{y}|$
4. $\boldsymbol{y_c}^{(m+1)} \leftarrow \boldsymbol{y_c}^{(m)}$
5. Repeat loop for all n
6. $z_1^{(m)}(n) = \begin{cases} y(n) & for n \in \boldsymbol{P} \\ y_c^{(m)}(n) + \Delta & for n \in \boldsymbol{Q} \end{cases}$
7. $z_2^{(m)}(n) = \begin{cases} y(n) & for n \in \boldsymbol{P} \\ y_c^{(m)}(n) - \Delta & for n \in \boldsymbol{Q} \end{cases}$
8. $endloop for all n$
9. Repeat loop for n ∈ $\boldsymbol{Q}$
10. $g^{(m)}(n_i) = \frac{\|\boldsymbol{\phi z_1}^{(m)}\|_1 - \|\boldsymbol{\phi z_2}^{(m)}\|_1}{2\Delta}$
11. $endloop for n \in \boldsymbol{Q}$
12. $\boldsymbol{y_c}^{(m+1)} = \boldsymbol{y_c}^{(m)} - \alpha \boldsymbol{g}^{(m)}$
13. m←m+1
14. repeat from step 4 until relevant stopping criteria.
15. **x** = [**y**, $\mathbf{y_c}$] (as per the original index positions **P** and **Q**).

3. The proposed methodology

Two different models for Image steganography are proposed in this paper. Model-I provides two level of security and model-II provides a way to overcome the adverse effect of stego-attack.

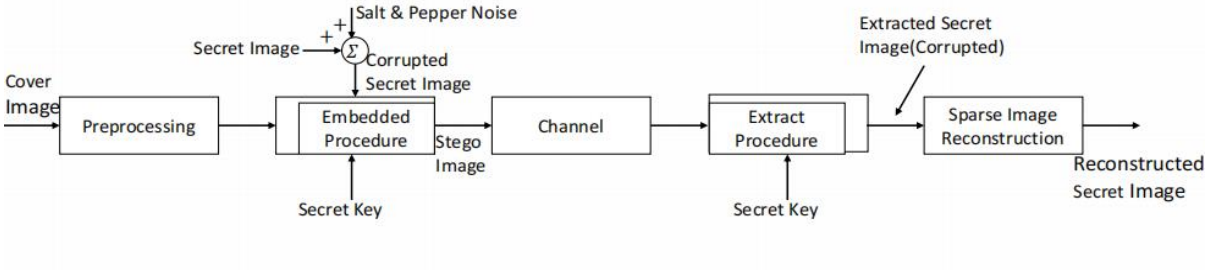

Fig 2 Model-I Image steganography

Figure 2, shows the model-I arrangement for image steganography, where the cover image is preprocessed in the first step involving image enhancement, converting 2D image pixel's array into 1D pixel blocks etc. These preprocessed 1D pixel array blocks are then used for embedding secret image data using LSB substitution technique with a bit length capacity of 2 bits/pixel [8]. In the meantime, the secret image is also preprocessed and is intentionally corrupted by salt and pepper noise at the transmitter side. This is done to provide one more level of security to the secret image. By doing this, though the third party hacks the system and gets access to the secret image, he will get the corrupted secret image and misinterpret, as it is a junk data resulting in maintaining secrecy. LSB substitution method [10], involves removing the least significant bits of each and every pixel of cover image and then substituting the same number of data bits of secret image. Repeating this embedding procedure until all the secret data bits are completely embedded inside the cover image. Re-converting the cover image pixel array blocks into 2D image will result in stego image, which will be transmitted over a communication channel.

At the receiver side, the secret image will be extracted from the cover image using LSB extraction procedure with the help of a secret key. This will result in extraction of secret image which is corrupted by salt and pepper noise at the transmitter side. From this corrupted secret image the complete high resolution noiseless secret image can be reconstructed using sparse adaptive gradient algorithm [5].

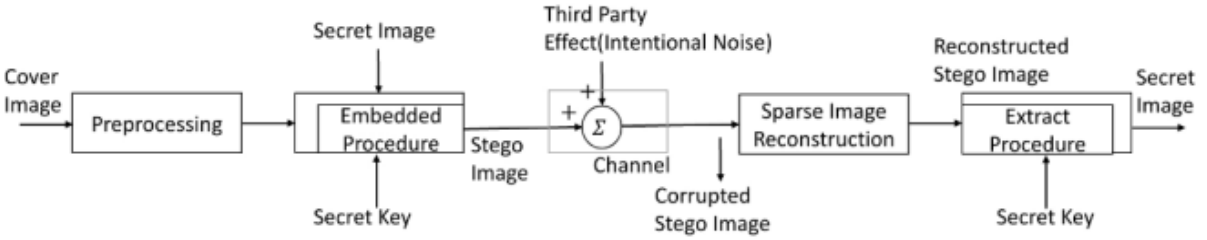

Fig 3 Model-II Image steganography

Figure 3 shows the model-II for image steganography. This model is originally deduced from the model-I. Model-II is developed to overcome the effect of stego attack. If the third party intentionally jams the secret communication by adding noise to the stego image in the channel, the hidden secret information will be corrupted or lost [11]. This attack can be overcome in the proposed model-II, as the corrupted stego image can still be reconstructed using sparse image reconstruction algorithm proposed in this paper. As the stego image is reconstructed, even the secret information hidden inside the cover image can also be reconstructed with minimum error [12].

4. Results and disscusion

MATLAB 2019 platform is used to simulate the proposed algorithm and models for image steganography. Standard color cover image (lena.png) shown in Fig 4 of size 512x512 is used for testing purpose. A 256x256 standard grey scale image (goldhill.png) shown in Fig 5 is used as secret image. The simulation is carried out for different parametric values for both model-I and model-II as presented below:

Case 1: Consider the salt and pepper noise density of 0.2. The noise corrupted secret image given as input for model-I is as shown in Fig 6 and the sparse reconstructed secret image is as shown in Fig 7. As seen from Fig 8, the stego image, after embedding the secret image into cover image, looks almost similar to cover image with a

PSNR of 38dB with respect to the cover image.

Case 2: Consider the salt and pepper noise density of 0.7. The noise corrupted secret image given as input for model-I is as shown in Fig 9 and the sparse reconstructed secret image is as shown in Fig 10. The proposed algorithm reconstructs the corrupted secret image with an average PSNR of 27dB-30dB.

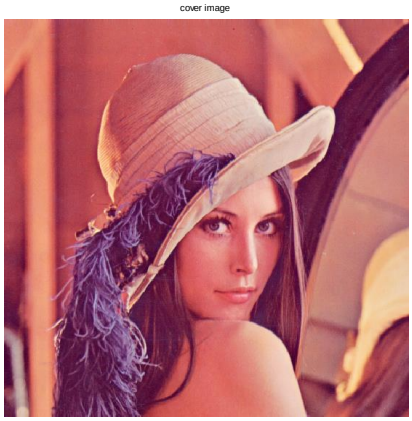

Fig 4 Test cover image (512x512)

Fig 5 Test secret image (256x256)

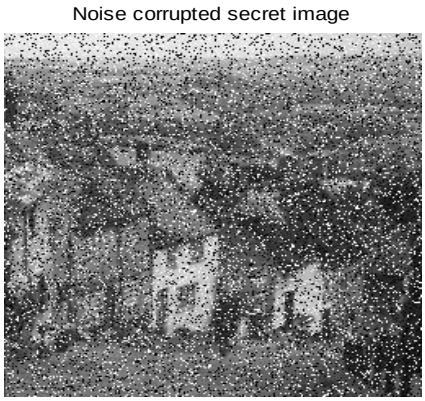

Fig 6 noise corrupted secret image with noise density=0.2

Fig 7 reconstructed secret image in case 1

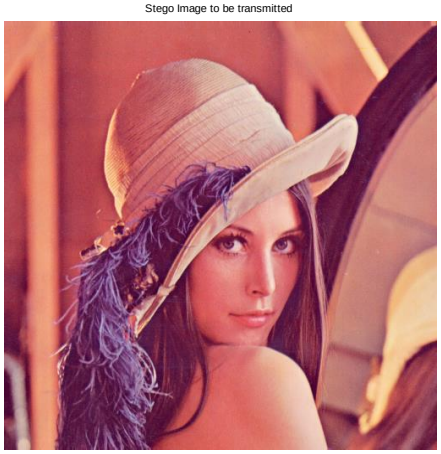

Fig 8 Stego Image after secret image embedding procedure

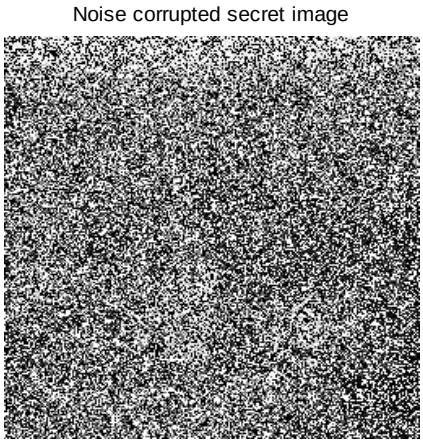

Fig 9 noise corrupted secret image with noise density=0.7

Fig 10 reconstructed secret image in case 2

Case 3: Consider a fixed amount of salt and pepper noise density of 0.2, now if the step size of the adaptive gradient algorithm is considered as $\alpha = 0.4$ & 0.6, the algorithm results in good PSNR but the computation time is considerably more for $\alpha = 0.4$ and vice versa for $\alpha = 0.6$. The reconstructed secret images for $\alpha = 0.4$ and $\alpha = 0.6$ are as shown in Fig 11 and Fig 12. As per the steepest descent algorithm[], there will be always a trade-off between computation time and PSNR.

Fig 11 reconstructed secret image for $\alpha = 0.4$

Fig 12 reconstructed secret image for $\alpha = 0.6$

Table 2 shows the comparison between computation time and PSNR for various values of algorithm step size by fixing the noise density as 0.2. As step size increases, the PSNR decreases and the computation becomes speedy. The variation of mean square error and PSNR for different noise density for fixed step size of 0.4 is given in Table 3. For a noise density of 0.8, the PSNR achieved in the reconstructed image is approximately 20dB, which means the proposed algorithm still produces an acceptable value for PSNR sufficient for visualizing the secret image at the receiver end.

Table 2 Comparison between computation time and PSNR for noise density fixed as 0.2

α	**Computation time (sec)**	**PSNR (dB)**
0.1	348.63	30.28
0.4	315.50	30.18
0.6	193.56	30.149
0.8	187.57	29.89

Table 3 Comparison between noise density and PSNR

Noise density	MSE	PSNR(dB)
0.5	9.6342	38.33
0.2	64.23	30.18
0.5	400.57	22.13
0.7	650.82	20.03
0.8	801.98	19.12

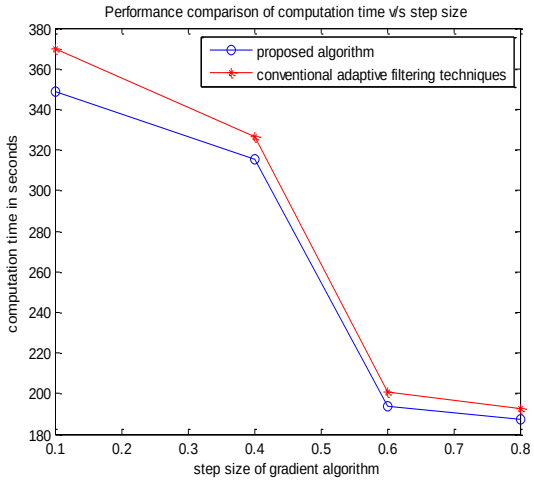

Fig 13 Performance comparison of computation time

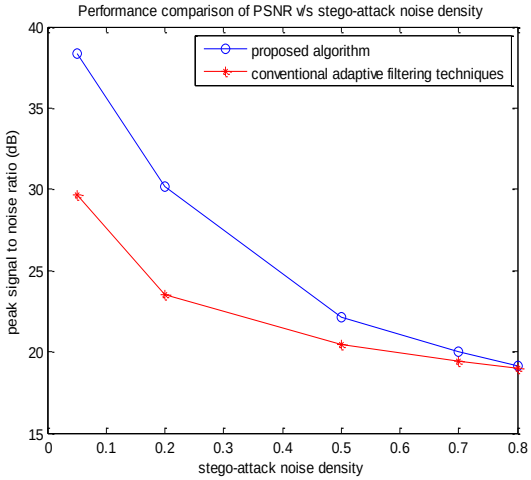

Fig 14 Performance comparison of PSNR

When compared with conventional adaptive filtering techniques for image reconstruction, the proposed sparse reconstruction algorithm in this paper shows lesser computation time with respect to step size of the gradient algorithm as shown in Fig 13. The peak signal to noise ratio curve of proposed reconstruction algorithm shows better points when compared to conventional filtering techniques [9] as shown in Fig 14. Higher the step size value, higher is the MSE value for all the different values of stego attack noise densities considered for model-II as compared in Fig 15.

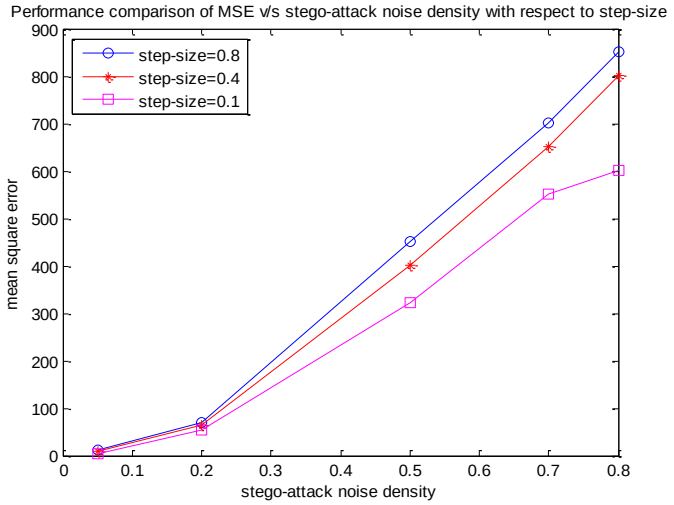

Fig 15 Performance comparison of MSE for variation in step size

5. Conclusion

In this paper, two different models for image steganography is proposed by employing sparse adaptive gradient algorithm for secret image reconstruction. Model-I is developed to provide two level of security for the secret information. Model-II is developed to overcome the effect of stego attack. Both of these models showcases better results even in the high noise density cases as presented in the results section. The PSNR achieved by the proposed reconstruction algorithm is better when compared to any other conventional adaptive filtering techniques. This paper incorporated the LSB substitution method for embedding procedure because of its simple and effective embedding procedure. Overall, on an average, the proposed models for image steganography along with the proposed algorithm for sparse image reconstruction exhibits better results and finds a good application communication field particularly in military applications.

References

1. Farah Qasim, Ahmed Alyousuf, Roshidi Din, Alaa Jabbar Qasim, “Analysis review on spatial and transform domain technique in digital steganography”, Bulletin of Electrical Engineering and Informatics, Vol. 9, No. 2, April 2020.
2. Himanshu Arora, Cheshta Bansal, Sunny Dagar, “Comparative study of Image Steganography techniques”, International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), October 2018.
3. Mohammed A. Saleh, “Image Steganography Techniques”, International Journal of Advanced Research in Computer and Communication Engineering, Vol. 7, Issue 9, September 2018.
4. Mandavilli Kavya, RamBabu M, “A Review Paper On Transform Domain Techniques Of Image Steganography In Text And Image”, International Journal of Creative Research Thoughts, Volume 6, Issue 2, April 2018.
5. Ljubiša Stankovi, Ervin Sejdi,Srdjan Stankovi, Miloš Dakovi, Irena Orovi´c, “A Tutorial on Sparse Signal Reconstruction and Its Applications in Signal Processing”, Springer: Circuits, Systems, and Signal Processing, 2018.
6. R. K and P. K. N, "Performance Evaluation & Analysis of Direction of Arrival Estimation Algorithms using ULA," 2018 International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT), Msyuru, India, 2018, pp. 1467-1473, doi: 10.1109/ICEECCOT43722.2018.9001455.
7. Raghu K and Prameela Kumari N, “On-grid Adaptive Compressive Sensing framework for Underdetermined DOA Estimation by employing Singular Value Decomposition,” International Journal of Innovative Technology and Exploring Engineering, ISSN: 2278-3075, vol. 8 Issue. 11, pp. 3076-3082, 2019.
8. Sumanth Sakkara, Akkamahadevi D H, K S Somashekhar, Raghu K, “Integer Wavelet based secret data hiding by selecting variable bit-length”, International Journal of Computer Applications (IJCA), Vol 48, No 19, 2nd Article, June 2012.
9. Raghu K, Santosh Boraganve, Yashwanth B S, Hemanth Gowda, Manikanta Yakkala, “Design and Implementation of Single/Multiple Frequency Notch Filter using Adaptive Noise Cancellor for

Communication Applications", International Journal of Future Generation Communication and Networking, Vol. 13, No. 3, (2020), pp. 1118–1127.

10. O. Elharrouss, N. Almaadeed and S. Al-Maadeed, "An image steganography approach based on k-least significant bits (k-LSB)," 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), 2020, pp. 131-135, doi: 10.1109/ICIoT48696.2020.9089566.
11. Z. Gao, L. Ding, C. Xiong, Z. Gong and Q. Xiong, "Compressive Sensing Reconstruction Based on Standardized Group Sparse Representation," 2019 IEEE International Conference on Image Processing (ICIP), 2019, pp. 2095-2099, doi: 10.1109/ICIP.2019.8803124.
12. Y. Liu, P. Huang, X. Feng and F. Li, "A reconstruction framework based on mixed sparse representations for compressive sensing," 2017 3rd IEEE International Conference on Computer and Communications (ICCC), 2017, pp. 1912-1916, doi: 10.1109/CompComm.2017.8322871.
13. W. Loedwassana, "Adaptive IIR Notch Filter with Variable Step Size Plain Gradient Algorithm based on Error Correlation governed by Gradient Accumulation," 2020 17th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), 2020, pp. 88-91, doi: 10.1109/ECTI-CON49241.2020.9158316.
14. N. Yagmur and B. B. Alagoz, "Adaptive Gradient Descent Control of Stable, First Order, Time-delay Dynamic Systems According to Time-Varying FIR Filter Model Assumption," 2019 International Artificial Intelligence and Data Processing Symposium (IDAP), 2019, pp. 1-5, doi: 10.1109/IDAP.2019.8875966.
15. A. G. Benedict, "Improved File Security System Using Multiple Image Steganography," 2019 International Conference on Data Science and Communication (IconDSC), 2019, pp. 1-5, doi: 10.1109/IconDSC.2019.8816946.