Highly Secure Image Steganography using LSB and Public Key Encryption Algorithm

Palak Chouriya[1], Prof. Khushboo Verma[2]

[1]*MTech. Scholar,* [2]*Research Guide*

Department of Computer Science and Engg, Bansal Institute of Science and Technology, Bhopal

Abstract - Security of information in the era of communication is getting worse due to the black hat practices of information stealing to make profit even compromising with the privacy of humans using various online platform and social networking portals. One of the kinds of such information is text, which is quite sensitive information of anyone like bio, passwords, contacts, call logs, messages and many more. The things more prone to get hacked when shared with someone. To make sharing of such information can be made secured more than the sharing of information directly. And the way is image steganography. Image steganography makes the information sharing so secure that no one can even predict that some kind of confidential information is with any image. If someone predicted and try to extract this information he/she cannot without the algorithm to decode it. This research work based on the method of development which increases the embedding algorithm more secures than any other method out there. So this works utilizing the LSB algorithm along with the public key encryption (PKE) method to secure data being hidden with cover image. The efficiency of proposed approach is compared using 3 figure of merits which are Mean Square Error(MSE), Peak Signal to Noise Ratio(PSNR) and Normalized Cross Correlation (NCC) found much better than the previous algorithm. For Security of the information being hidden is achieved using Public Key Encryption Algorithm.

Keywords - Public Key Encryption, Steganography, Image Processing, Information Security.

I. INTRODUCTION

Nowadays individuals exchange information straightforwardly using the existing communication technologies such as a local area network, a wide area network or simply the Internet. This information can be very sensitive and need to be protected against any intruder who can intercept them during the communication phase. Therefore, transferring sensible information cannot be solely relied on the existing communication technologies channels. There is need of a robust technique to protect the information and ensure that they cannot be detected by other parties.

Cryptography is used to encrypt information based on some mathematical formulas. It is widely used to protect information exchanged over the Internet. World Wide Web (WWW) and e-mail are both public channels for transferring information. However, both technologies are vulnerable to attacks and exchanged information can be detected relatively easily. In cryptography the secret information is modified using some public and private keys and become unreadable (e.g., encryption). They are then sent over the public channels to the destination where the original information would be retrieved using the corresponding keys (e.g., decryption). This technique does not prevent against hacker’s attacks who can intercept the decrypted information and apply their own techniques to retrieve the secret information. Therefore, it is necessary to find another methodology to protect the information exchanged safely over public channels without raising suspicions. This methodology is known as steganography and has become very popular in the last decade.

Steganography is the art of concealing sensible information into digital media (i.e., images, audio, text). It is a mechanism that completely differs from cryptography. In fact, in cryptography the information is modified but still can be seen in this unreadable format once sent over the networks, whereas in steganography the information is simply embedded into a digital support and cannot be noticed as long as the quality of the carrier is not deteriorated.

Steganography hides information into a digital media called cover object which can be a video clip, a digital image, an audio file or simply a text. This digital media is called respectively a cover image, a cover audio, a cover video, and a cover text. Once the information is embedded in that cover it is called a stego-object. If the cover is an image or an audio file, then the result of embedding the information in the cover is referred to as stego-image or stego-audio respectively.

In a good steganography algorithm, there are five vital features that should be considered. The first one is the capacity payload which refers to the amount of secret information that a stego-cover can carry before the distortions become noticeable. The second feature is the un-detectability which means that the existence of the secret information should be undetectable whenever the stego-object is detected and analyzed. Other features that should be considered are: invisibility, security and robustness.

Many research works have been conducted on image steganography-based algorithms. One of the oldest algorithms is the Least Significant Bit (LSB), where redundant bits of the stego-image are replaced by the covert information bits. The modification is done in the spatial domain of the image. Although the LSB algorithm is the simplest technique to hide information into a digital image, it is however the less efficient one as it causes obvious distortion of the stego-image. To enhance the performance and to achieve robustness and security a highly secure image Steganography using LSB and public key encryption algorithm has presented in this examination.

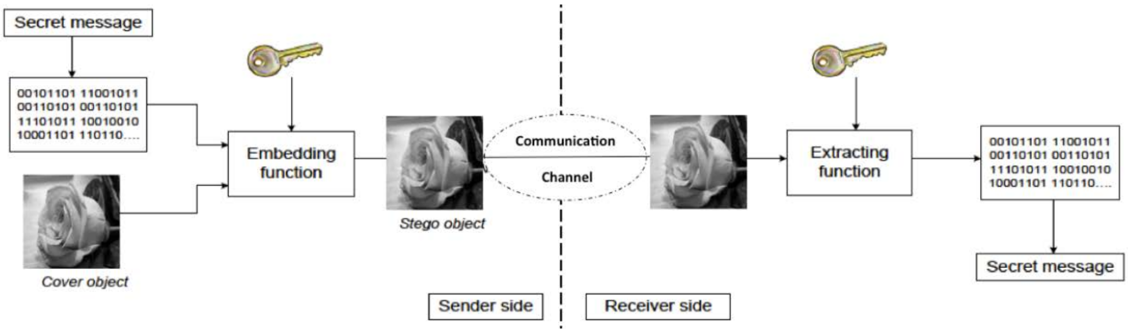


Fig. 1.1 Illustration of Steganography Process.

An illustration of the steganography process to embed and extract a message is presented in Figure 1.1. This example uses an image as the cover object to carry bits of the secret message. At the sender's side, the secret message is embedded into the cover image by using some embedding function and the stego-image can be parameterized by a stego-key. Then the stego-image is sent over a communication channel to the receiver. The communication channel can be any type of transmission technologies that exist such as the Internet or E-mail. Then at the receiver's side the secret message is extracted using the extracting function. In addition, the extracting function uses the shared stego-key if it was used in the embedding phase.

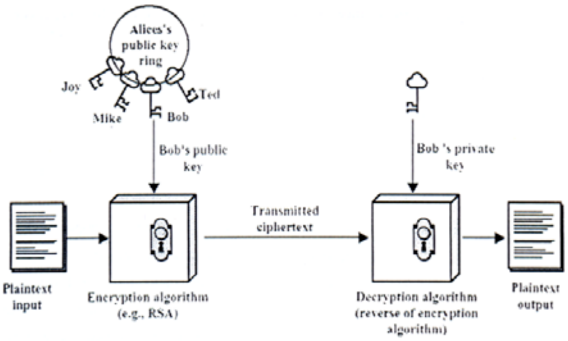
II. PUBLIC KEY ENCRYPTION (PKE) ALGORITHM

Public-Key Algorithms are symmetric, that is to say the key that is used to encrypt the message is different from the key used to decrypt the message. The encryption key, known as the Public key is used to encrypt a message, but the message can only be decoded by the person that has the decryption key, known as the private key.

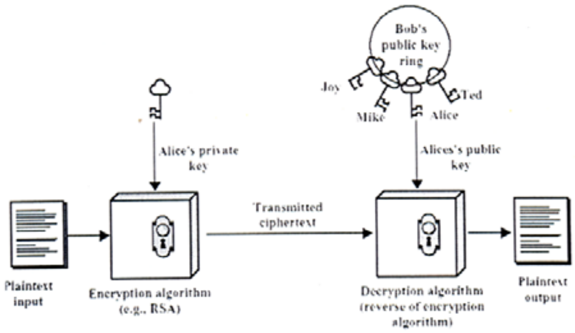
This type of encryption has a number of advantages over traditional symmetric Ciphers. It means that the recipient can make their public key widely available- anyone wanting to send them a message uses the algorithm and the recipient's public key to do so. An eavesdropper may have both the algorithm and the public key, but will still not be able to decrypt the message. Only the recipient, with the private key can decrypt the message.

A advantage of public-key algorithm is that they are more computationally intensive than symmetric algorithms, and therefore encryption and decryption take longer. This may not be significant for a short text message, but certainly is for bulk data encryption.

In order to decrypt a message, Bob (the recipient) has to know the key. However, it may be difficult for Alice (the sender) to tell Bob what the key is. If they simply agree on a key bye-mail for example, Eve could be listening in on their e-mail conversation and thus also learn what the key is. Public key cryptography was invented to solve this problem.



(a) Encryption.



(b) Authentication.

Fig. 2.1 Public- key Encryption.

When using public-key cryptography, Alice and Bob both have their own key pairs. A key pair consists of a public key and a private-key. If the public-key is used to encrypt something, then it can be decrypted only using the private-key. And similarly, if the private-key is used to encrypt something, then it can be decrypted only using the public key. It is not possible to figure out what the private-key is given only the public-key, or vice versa.

This makes it possible for Alice and Bob to simply send their public keys to one another, even if the channel they are using to do so is insecure. It is no problem that Eve now gets a copy of the public keys. If Alice wants to send a secret message to Bob, she encrypts the message using Bob's public key. Bob then takes his private key to decrypt the message. Since Eve does not have a copy of Bob's private key, she cannot decrypt the message. Of course this means that Bob has to carefully guard his private key. With public key cryptography it is thus possible for two people who have never met to securely exchange messages. Figure 2.1 illustrates the public-key encryption process.

III. PROPOSED METHODOLOGY

An image steganography employ to hide information inside an image. It manipulates image features to hide messages a highly secure image Steganography using LSB and public key encryption algorithm has proposed in this research examination. The LSB steganography algorithm is one of the oldest steganography algorithms that embeds the message bits into the stego-image used in proposed work. It is an outstanding information hiding system utilized broadly as a result of its straightforwardness. It leads to modify to the least significant bit of the stego-image (text embedded image) pixels, which change just the tone of the colour. This change is so slight that the human eye may not notice it. The least significant bit of image pixels hides the message bits into the image pixels either in a sequential or randomized fashion. It creates a replacing path for the least significant bits of the image with the message bits. If the path is randomly generated then the pseudo random number generator PRNG is utilized. The PRNG should be seeded with some stego-key that is shared between the sender and receiver. In this way the message bits will be spread over the stego-image. Fig. 3.1 shows the block representation of proposed Steganography model embedding process. A Lena image is taken as a cover image to execute proposed examination work. First to select the pixels a path is created. On the basis of a stego-key these selected pixels are choose in random fashion . A pixel is chosen from the cover image based on the path for each bit of the secret message then replace the least significant bit of the cover pixel with the bit of the secret message. The algorithm hides the length of the secret message alongside the message itself.

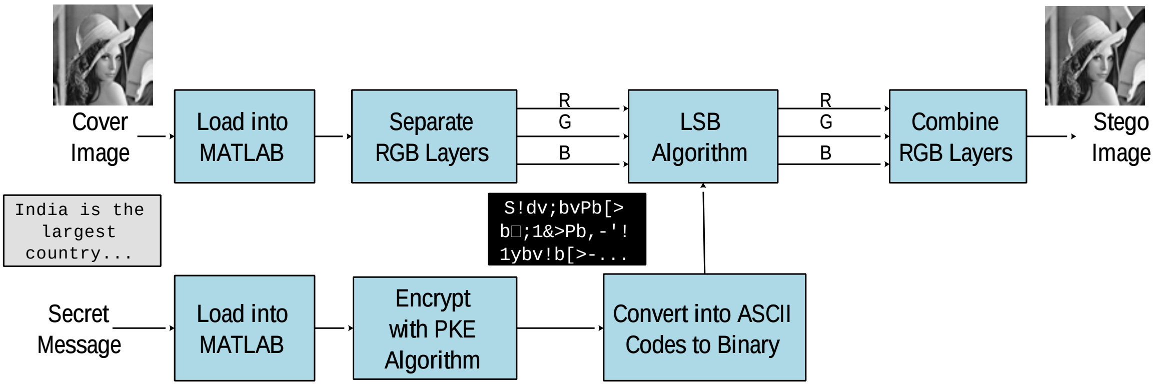

Cover Image
Load into MATLAB
Separate RGB Layers
R
G
B
LSB Algorithm
R
G
B
Combine RGB Layers
Stego Image
India is the largest country...
S!dv;bvPb[> b□;1&>Pb,-'! 1ybv!b[>-...
Secret Message
Load into MATLAB
Encrypt with PKE Algorithm
Convert into ASCII Codes to Binary

Fig.3.1 Block Diagram of Proposed Steganography Model Embedding Process.

Fig. 3.2 shows the block representation of proposed Steganography model retrieval process. The extraction stage is the opposite of the embedding stage. At the receiver side the way is made based on the stego-key. First the length of the secret message is recovered by retrieving the LSB of the pixels. At that point the pixels are crossed based on the way and minimum noteworthy bit of every pixel is retrieved. This procedure of traversing every one of the pixels proceeds until achieving the end of the message length.

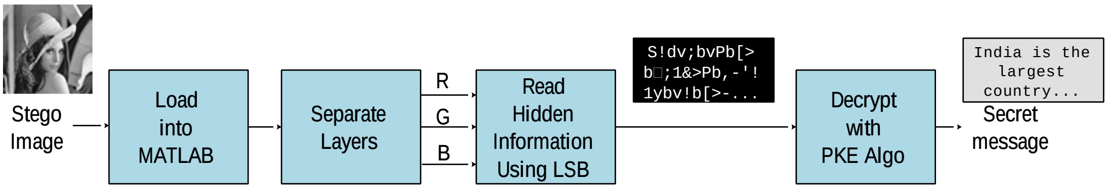

Stego Image
Load into MATLAB
Separate Layers
R
G
B
Read Hidden Information Using LSB
S!dv;bvPb[> b□;1&>Pb,-'! 1ybv!b[>-...
Decrypt with PKE Algo
India is the largest country...
Secret message

Fig.3.2 Block Diagram of Proposed Steganography Model Retrieval Process.

Fig. 3.3 shows the process flow of execution of proposed work in MATLAB simulation environment. A step by step execution of proposed algorithm is show with the help of flow chart in this Fig.

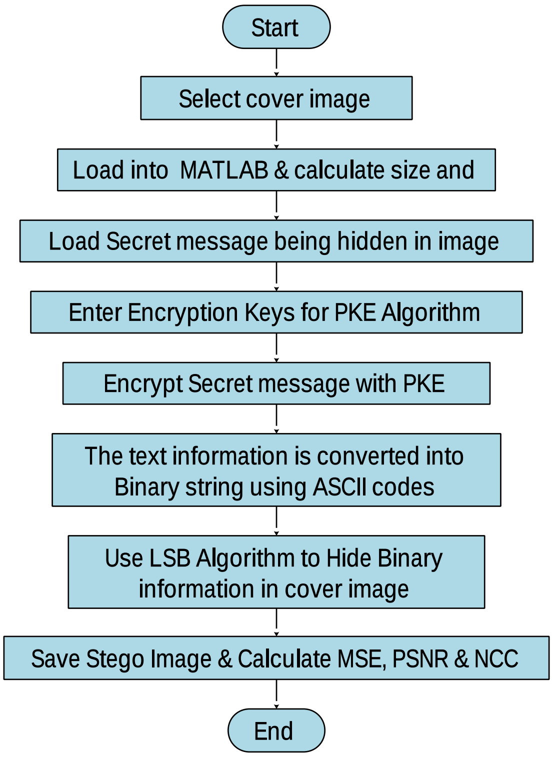

Start
Select cover image
Load into MATLAB & calculate size and
Load Secret message being hidden in image
Enter Encryption Keys for PKE Algorithm
Encrypt Secret message with PKE
The text information is converted into Binary string using ASCII codes
Use LSB Algorithm to Hide Binary information in cover image
Save Stego Image & Calculate MSE, PSNR & NCC
End

Fig.3.3 Flow Chart of Steganography Embedding Process

Step 1: Start execution in MATLAB image processing environment.

Step 2: Select Lena image as a cover image.

Step 3: Load image in to MATLAB and calculate its size.

Step 4: Load secret message being hidden in cover image.

Step 5: Enter encryption key for public key encryption algorithm.

Step 6: Encrypt secret message with PKE.

Step 7: The text information is converted into Binary string using ASCII codes.

Step 8: Use LSB Algorithm to Hide Binary information in cover image.

Step 9: Save Stego image and calculate MSE, PSNR, & NCC.

Step 10: End encryption process.

Fig. 3.4 shows the information retrieval process of proposed algorithm in retrieval process is inverse to embedding process. The steps of retrieval process are as follows.

Step 1: Start process with MATLAB image processing

Step 2: Load Stego image in MATLAB image processing proposed algorithm.

Step 3: Define public and private keys for PKE Algorithm.

Step 4: Convert binary numbers ASCII codes.

Step 5: Convert ASCII codes into Character.

Step 6: Decrypt characters Strings into message.

Step 7: Shows recovered message.

Step 8: End process.

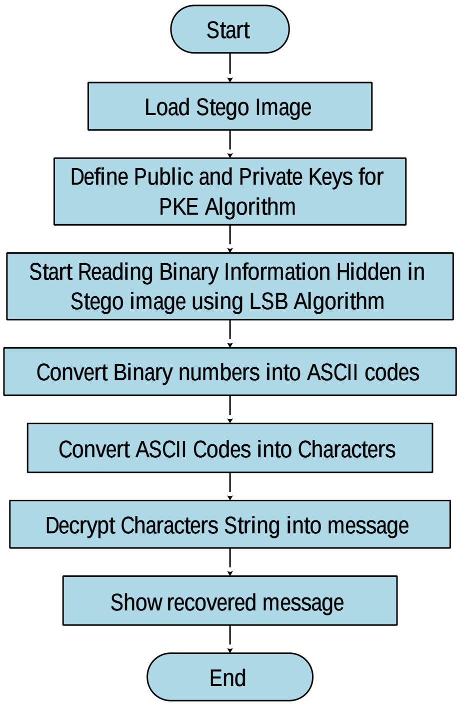

Start
Load Stego Image
Define Public and Private Keys for PKE Algorithm
Start Reading Binary Information Hidden in Stego image using LSB Algorithm
Convert Binary numbers into ASCII codes
Convert ASCII Codes into Characters
Decrypt Characters String into message
Show recovered message
End

Fig.3.4 Flow Chart of Steganography Retrieval Process.

IV. EXPERIMENTAL RESULTS

The implementation execution and simulation of proposed algorithm has completed in MATLAB image processing simulation environment. The LSB substitutes a secret message’s bit with the cover image least significant bit. Because this method introduces asymmetry artifacts to the stego-image, that makes it weak against steganalysis techniques. To overcome this public key encryption algorithm is used. First the text is compressed and encrypted using stego-key1. Compression and encryption are used to reduce the amount of data required to be hidden in a cover image and to increase security respectively. The compression and encryption will only be used for implementing an application. Fig. 4.1 shows the Original secret message.

```
India is the largest country in the
South Asia Region, located primarily in
the center of South Asia, and shares
International borders with Pakistan to
the north-west, China and Nepal to the
north, Bhutan to the north-east, and
Bangladesh and Myanmar are to the east.
Sri Lanka lies to the south, Maldives to
the south-west and has maritime boundary
8 Indonesia to the south-east of India
in the Indian Ocean. The Republic of
India is the seventh largest country in
the world by area and, with over a
billion people, is second only to China
in population, although its much higher
birth-rate makes it
```

Fig. 4.1 Original Secret Message.

Using compression will decrease number secret bits which lead to decrease number of modified pixels. The compression algorithm used is deflate. Deflate is one of most commonly method adopting lossless compression technique.

Afterward, PKE encryption technique is used to encrypt the compressed text. This sort of encryption has various points of interest over conventional symmetric Ciphers. It implies that the beneficiary can make their open key broadly accessible anybody needing to send them a message utilizes the algorithm and the beneficiary's open key to do as such. An eavesdropper may have both the algorithm and the general public key, however still not able to decode the message. Only the receiver, with the private key can decode the message. Fig. 4.2 Shows the encrypted secret message after public key encryption (PKE) using pk1 = 11 and pk2 = 13.

```
S!dv;bvPb□[>b ;1&>P□b,-'!□1ybv!b□[>-
'□[bAPv;bE>&v-!cb -,;□>db1v;1v
ybv!b□[>b,>!□>1b-w-
'□[bAPv;cb;!dbP[;1>PbS!□>1!;□v-!; b -
1d>1Pb%v□[b□;DvP□;!b□-b□[>b!-
1□[o%>P□cbY[v!;b;!dbN>; b□-b□[>b!-
1□[cbB['□;!b□-b□[>b!-1□[o>;P□cb;!dbB;!&
;d>P[b;!dbMy;!;1b;1>b□-b□[>b>;P□T1vb6;!D;b
v>Pb□-b□[>bP-'□[cbM; dvO>Pb□-b□[>bP-
'□[o%>P□b;!db[;Pb;1v□v>b -'!d;1yb8bS!d-
!>Pv;b□-b□[>bP-'□[o>;P□b-
wbS!dv;bv!b□[>bS!dv;!b(,>;!TbH[>bE>'  v,b-
wbS!dv;bvPb□[>bP>O>!□[b ;1&>P□b,-
'!□1ybv!b□[>b%-1 db yb;1>;b;!dcb%v□[b-O>1b;b
v  v-!b>- >cbvPbP>,-!db-! yb□-bY[v!;bv!b-'
;□v-!cb; □[-'&[bv□Pb',[b[v&[>1b
v1□[o1;□>b;D>Pbv
```

Fig.4.2 Encrypted Secret Message after Public Key Encryption (PKE) using pk1 = 11 and pk2 = 13.

Table 1 shows the experimental results cover images and respective stego images. In table 1 Lena, Barbara, Sailboat, Airplane, House images are taken as a Test image or cover image and their respective Stego image. Table 2 shows the performance analysis of proposed algorithm for same test images in terms of Mean Square Error (MSE) with respect their previous results. The graphical analysis of proposed algorithm is shown in Fig. 4.3 in terms of Mean Square Error (MSE).

Table 1. Experimental Results Cover Images and Respective Stego Images.

Test Images	*Cover Image*	*Stego Image*
Lena		
Barbara		
Sailboat		
Airplane		
House		

Table 2: Performance of Mean Square Error(MSE) for Different Images

Test Images	***MSE***	
	Previous [1]	***Proposed***
Lena	0.27	0.0003
Barbara	0.27	0.0003
Sailboat	0.27	0.0003
Airplane	0.27	0.0003
House	0.27	0.0003

The PSNR Peak Signal to Noise Ratio (PSNR) Performance of in dB for 1 Lena, Barbara, Sailboat, Airplane, House images are shown in Table 3 and its corresponding graphical representation is shown in Fig. 4.4.

Table 3: Performance of Peak Signal to Noise Ratio (PSNR) in dB for Different Images

Test Images	***PSNR (in dB)***	
	Previous [1]	***Proposed***
Lena	53.46	83.24
Barbara	53.65	83.17
Sailboat	53.78	83.18
Airplane	52.91	83.13
House	53.05	83.32

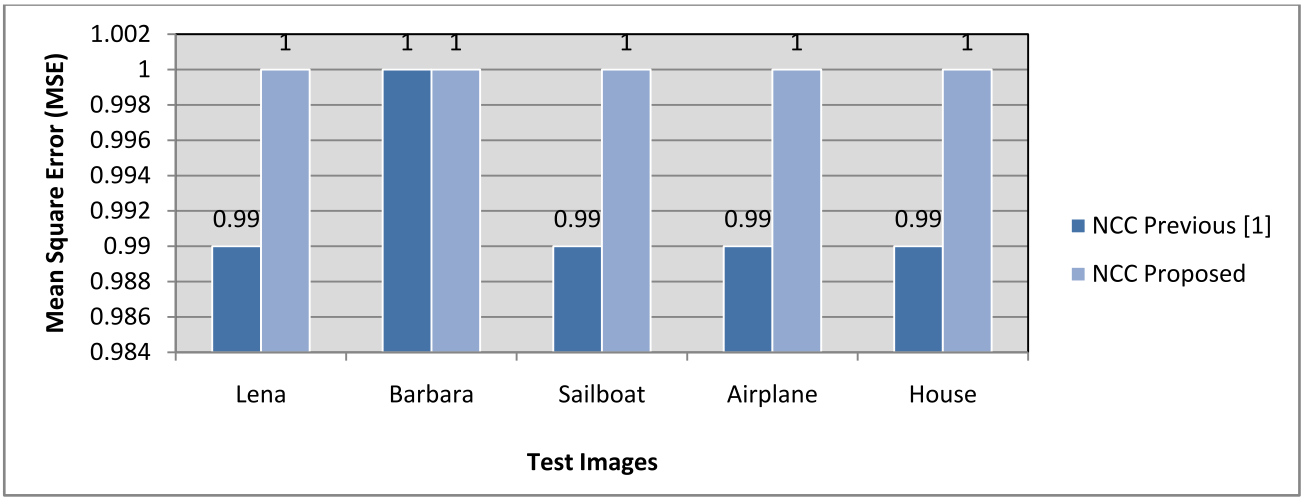


Fig.4.3 Graphical Comparison of Mean Square Error (MSE).

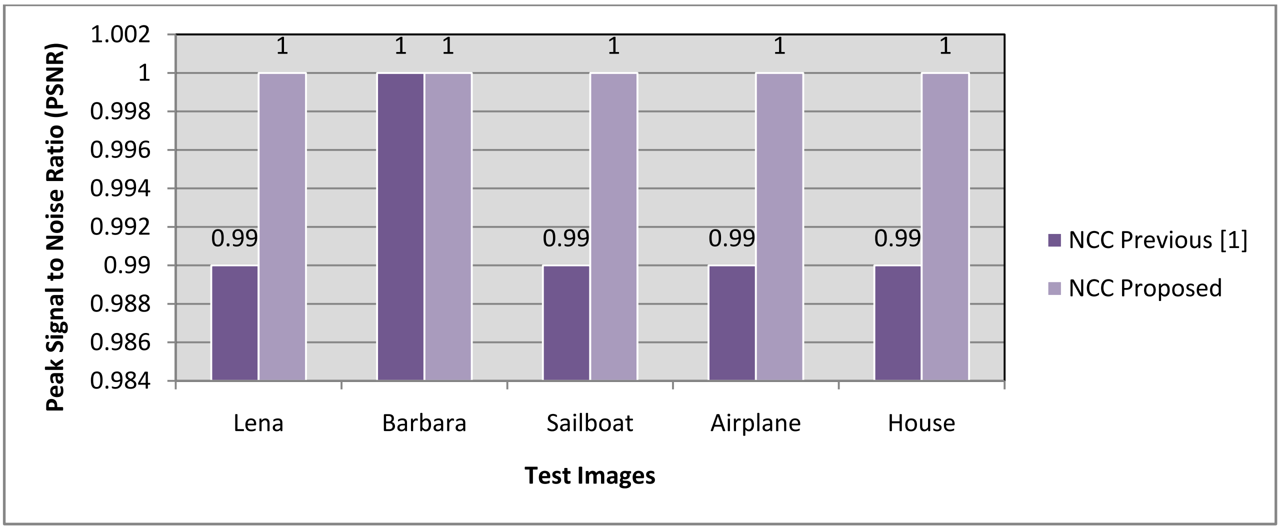


Fig.4.4 Graphical Comparison of Peak Signal to Noise Ratio (PSNR).

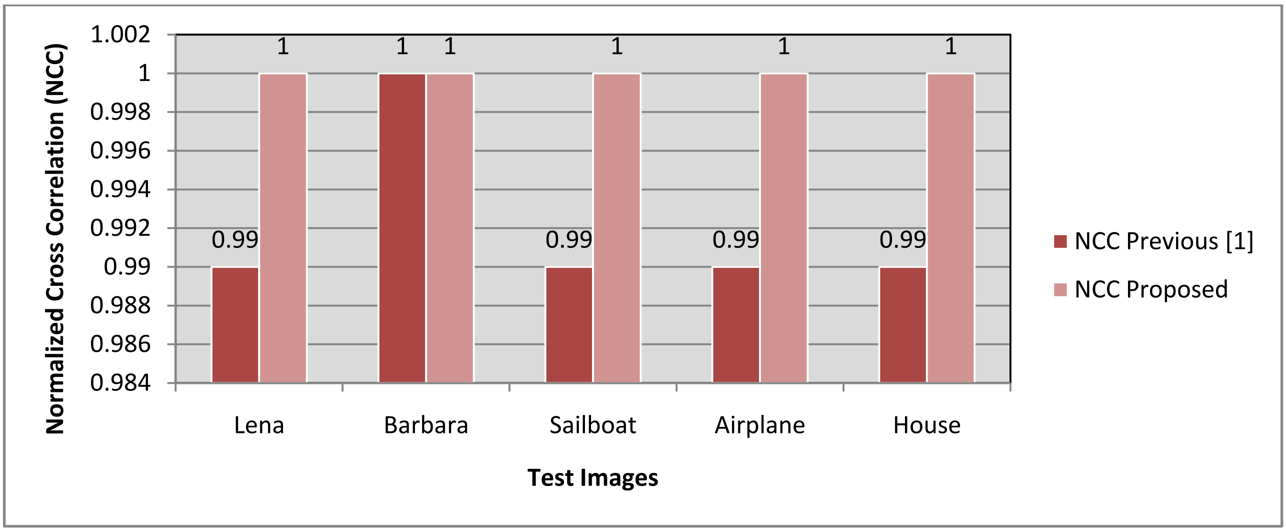


Fig.4.5 Graphical Comparison of Normalized Cross Correlation (NCC).

Performance of Normalized Cross Correlation (NCC) for Lena, Barbara, Sailboat, Airplane, House images are shown in table 4 and its graphical representation is shown in Fig. 4.5.

Table 4: Performance of Normalized Cross Correlation (NCC) for Different Images.

Test Images	***NCC***	
	Previous [1]	***Proposed***
Lena	0.99	1.00
Barbara	1.00	1.00
Sailboat	0.99	1.00
Airplane	0.99	1.00
House	0.99	1.00

V. CONCLUSION AND FUTURE SCOPES

In this research work overview and background about steganography are presented. Images are the most preferred type for holding secret messages the existing algorithms of symmetric key and public key cryptography are also studied for secure image steganography. Image Steganography in spatial domain involves direct manipulation of the pixel's bits to embed secret message. Researches on Steganography in spatial domain are very active and there is space for improvement. This examination work proposed a highly secure image steganography using LSB and public key encryption algorithm in MATLAB image processing environment. LSB is the most recognized algorithm in image steganography in spatial domain. The Least Significant Bits of the image pixels are modified to match the secret bits. To validate the performance of proposed approach an examination of results are carried out in terms of MSE, PSNR and NCC and compared with previous base results. It is found that proposed work has better performance against previous one. As perceived the robustness of the proposed method based on LSB using PKE still need to improve since it works in spatial domain. For future work, concentration should be on applying the proposed technique in transform domain to improve the robustness.

REFERENCES

[1] E. Emad, A. Safey, A. Refaat, Z. Osama, E. Sayed and E. Mohamed, "A secure image steganography algorithm based on least significant bit and integer wavelet transform," in Journal of Systems Engineering and Electronics, vol. 29, no. 3, pp. 639-649, June 2018.

[2] S. E. El-Khamy, N. Korany and M. H. El-Sherif, "Robust image hiding in audio based on integer wavelet transform and Chaotic maps hopping," 2017 34th National Radio Science Conference (NRSC), Alexandria, 2017, pp. 205-212.

[3] K. A. Al-Afandy, O. S. Faragallah, A. Elmhalawy, E. M. El-Rabaie and G. M. El-Banby, "High security data hiding using image cropping and LSB least significant bit steganography," 2016 4th IEEE International Colloquium on Information Science and Technology (CiSt), Tangier, 2016, pp. 400-404.

[4] G. Sugandhi and C. P. Subha, "Efficient steganography using least significant bit and encryption technique," 2016 10th International Conference on Intelligent Systems and Control (ISCO), Coimbatore, 2016, pp. 1-6.

[5] P. W. Adi, F. Z. Rahmanti and N. A. Abu, "High quality image steganography on integer Haar Wavelet Transform using modulus function," 2015 International Conference on Science in Information Technology (ICSITech), Yogyakarta, 2015, pp. 79-84.

[6] S. Sharma and U. Kumar, "Performance improvement of IWT BPCS image Steganography," 2015 4th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions), Noida, 2015, pp. 1-5.

[7] S. Lavania, P. S. Matey and V. Thanikaiselvan, "Real-time implementation of steganography in medical images using integer wavelet transform," 2014 IEEE International Conference on Computational Intelligence and Computing Research, Coimbatore, 2014, pp. 1-5.

[8] Kaur S, bansal S, Bansal R K. "Steganography and classification of image steganography techniques". Proc. of International Conference on Computing for Sustainable Global Development, 2014: 870 – 875.

[9] Thanikaiselvan v, Arulmozhivarman P. , "High security image steganography using iwt and graph theory". Proc. of International Conference on Signal and Image Processing Applications, 2013: 337 – 342.

[10] Hemalatha S, Renuka A, Acharya U D, et al. "A secure image steganography technique using integer wavelet transform". Proc. of World Congress on Information and Communication Technologies, 2012: 755 – 758.

[11] El safy r o, zayed h h, el dessouki A, "An adaptive steganographic technique based on integer wavelet transform" Proc. of International Conference on Networking and Media Convergence, 2009: 111 – 117.

[12] Prabakaran G, Bhavani R, "A modified secure digital image steganography based on discrete wavelet transform" Proc. of International Conference on Computing, Electronics and Electrical Technologies, 2012: 1096 – 1100.