Efficient and Multilevel Secured Image Steganography using LSB and RSA Encryption Algorithm

Ganga Verma [1] ,Prof. Vikram Rajpoot[2]

[1]Mtech. scholar , [2]Research Guide ,

Department of Computer Science and Engineering, LNCT College Bhopal

Abstract – Image steganography the domain where we deal with the information security transmit through images. The images are being processed in such a way that the information is being hidden behind image without compromising with the quality of image, because if it loose its quality than the original image, anyone can predict some information is hidden in the image or some processing has been done with images. If someone trying to predict hidden information he can with some efforts, so we need another security layer to protect this information. This work concentrating to increase the security level so that the information is being hidden behind image must not be revealed without access to the authorized person. The proposed approach is than compared for robustness using Peak Signal to Noise Ratio(PSNR) and Mean Square Error(MSE), and found much better than the previous algorithm. For Security of the information being hidden is achieved using RSA Algorithm.

Keywords - RSA Encryption, Steganography, Image Processing, Information Security.

I. INTRODUCTION

With progressions in computerized communication innovation and the development of computer power and memory storage, the troubles in ensuring users privacy turned out to be progressively testing. The degrees to which people acknowledge privacy contrast starting with one individual then onto the next. Different strategies have been examined and created to ensure individual privacy. Encryption is presumably the most clear one, and afterward comes steganography. Encryption fits commotion and is for the most part observed while steganography isn't recognizable.

Interest from established researchers has escalated in the previous couple of years in connection to steganography. This displays itself in the foundation of new devoted meetings and books, expanded subsidizing from protection services, and the introduction of different business organizations. Obviously that in a couple of nations, the blossoming worry that prompts this liberality is because of the far reaching neurosis of culprits and terrorists who could possibly utilize this technique to impart. In this manner, financing in those nations was one-sided towards counter-attacking steganography and paid little worry to upgrading the privacy of people.

Such an exertion ejected into an open fight that has two unequal camps, one for making steganography algorithms to reinforcement the human requirement for privacy and another camp discovering approaches to vanquish the recently created techniques, steganalysis.

The various sorts of steganography systems are substitution, transform domain, spread spectrum, statistical and distortion strategies and cover generation techniques. Substitution methodologies supplant the minimum critical bits of each pixel in the cover record with bits from the secret report. The transform domain system technique hides secret information in the transform domain (like frequency domain) by changing the least significant coefficients of the cover file. Most research in the category of transform domain encoding is centered around on exploiting redundancies in Discrete Cosine Transform (DCT) [13]. This strategy is generally utilized for JPEG images in order to pack images. Changing countless does not deliver any obvious modifications but rather brings about a lot of changes in compression rates. In this way the installing limit of the DCT procedure is less contrasted with LSB strategy. Spread range procedures spread hidden data over various transfer speeds [1].

It is the act of encoding/implanting secret data in a way with the end goal that the presence of the data is undetectable. The first records can be alluded to as cover content, cover image, or cover sound. Subsequent to embeddings the secret message it is alluded to as stego-medium. A stego-key is utilized for concealing/encoding procedure to confine discovery or extraction of the embedded information.

Image steganography is a strategy which is utilized to shroud secret message inside an image. The paired bits of secret of message are hidden in the double of image and this somewhat influences the powers of shading or brilliance which isn't recognizable by exposed human eyes [8]. There are numerous algorithms which are utilized for image steganography yet some of them are exceptionally perplexing while some of them are basic.

As expressed before, images are the most mainstream cover objects utilized for steganography. In the area of

advanced images a wide range of image document positions exist, a large portion of them for particular applications. For these diverse image document positions, distinctive steganographic algorithms exist.

A straightforward image steganographic model contains a unique image, called cover (I) image in which secret segment secret message/image (M) is hidden and a stego key (K) which is utilized to shroud the data and additionally to separate. The motivation behind utilizing stego key is to give security. At long last, after the steganographic procedure, an image is acquired called stego-image (S) in which pixel esteem is not the same as the pixel estimation of unique image yet these progressions is minor to the point that it can't be effortlessly recognize by human eyes.

In the above model figure 1.1, work f demonstrates any image steganographic algorithm. LSB image steganography algorithm is used which is used to supplant the Least Significant Bits (LSB) of the image in which secret message is to be hidden called cover image with the Most Significant Bits (MSB) of secret message to be hidden without changing the truthful property of the cover image basically.

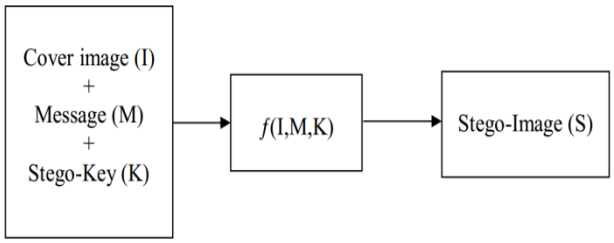

Figure 1.1 Simple Steganographic Model.

II. RSA ENCRYPTION ALGORITHM

The rising development of information communication strategy and electronic transaction over the web has made framework security to end up plainly the most essential issue over the system. To give present day security features, open private key cryptosystems are utilized. One of such cryptosystem is RSA algorithm. In spite of the fact that calculation in RSA takes additional time by if the message to be scrambled is created randomly then RSA will end up being to be great cryptography algorithm for system security [7].

For the better working of RSA based cryptosystem the framework has the general population key for decryption and the user will have the gadget containing the private key alloted to the user. What's more, rather than entering the secret key the user will simply need to embed the gadget to the framework and the framework will do the cross checking of the watchword for that specific client and permit get to in like manner [8].

1. Public-key encryption.

In RSA, encryption keys are made open while the decryption keys are kept private, so just the individual with the right decryption key can decipher a scrambled message. Everybody has their own particular encryption and comparing decryption keys. The keys are made such that the decryption key can't be effectively concluded from people in general encryption key.

2. Digital signatures.

The beneficiary may need to check that a transmitted message is really started from the sender, and didn't simply originate from verification. This is finished with the assistance of the sender's decryption key, and later the mark can be checked by anybody, utilizing the relating open encryption key. Marks hence can't be replicated. Additionally, Also, no signer can later deny having signed the message.

The various steps involved in RSA algorithm are :

A. Finding large prime numbers

The first step of the algorithm, is to search 'n' where ‘n’ is the product of two prime numbers ‘p’ & ‘q’. The number ‘n’ will be revealed in the encryption and decryption keys, but the numbers ‘p’ and ‘q’ will not be explicitly shown. The prime numbers ‘p’ and ‘q’ should be large such that it will be very difficult to derive from ‘n’.

$$n = p \times q \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots Eq.1$$

B. Finding the public key (e)

Choose a number ‘e’ such that ‘e’ is co-prime to $\varphi(n)$, where $\varphi(n)$ is the Euler’s totient function that counts the number of positive integers less than or equal to ‘n’ that are relatively prime to ‘n’ i.e.

$$\varphi(n) = (p-1)(q-1) \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots Eq.2$$

$$Gcd\big(e, \varphi(n)\big) = 1 \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots Eq.3$$

where, $1 < e < \varphi(n)$

C. Determine the private key (d)

Determine the private key ‘d such that‘d’ is the multiplicative inverse of the public

key ‘e’ i.e.

$$d^{-1} = e\left(mod\big(\varphi(n)\big)\right) \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots Eq.4$$

D. Encryption

Let ‘m’ be the message (integer type) that is to be encrypted using public key ‘e’ to give the encrypted message as ‘c’ where ‘c’ is calculated as

$$c = m^e\big(mod(n)\big) \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots Eq.5$$

E. Decryption

The decrypted message 'm' is found out using the private key'd' and is calculated

as:

$$m = c^d \left(mod(n)\right) \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots Eq.6$$

III. PROPOSED METHODOLOGY

The usage of proposed is based on Least Significant Bit (LSB) as one of the steganography systems alongside RSA encryption algorithm to improve the security level of image stenography [8]. The minimum noteworthy piece (as such, the eighth piece) of a few or the greater part of the bytes inside an image is changed to a touch of the secret message [7].

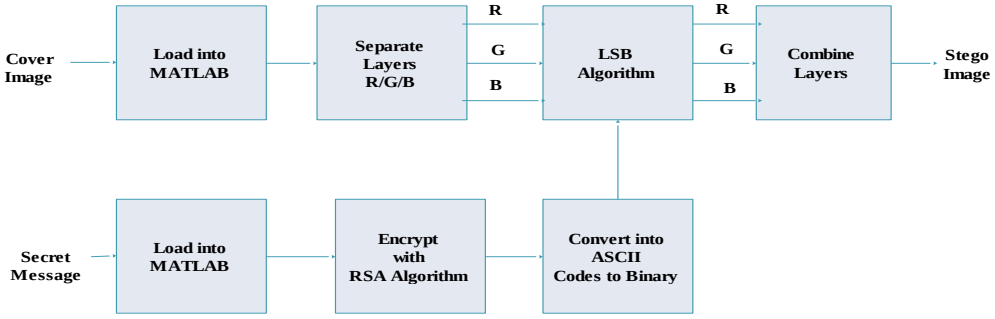

Figure 3.1 Block diagram of water marking process.

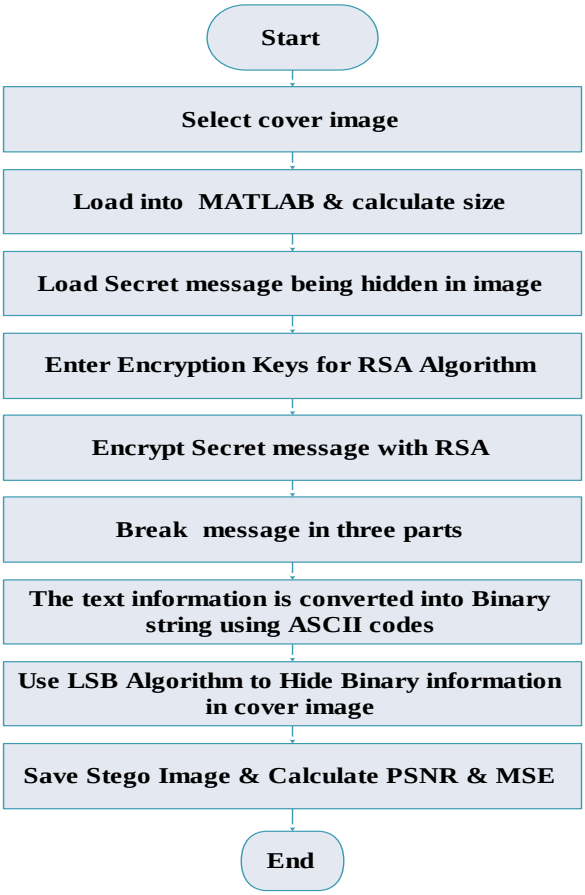

Figure 3.2 water marking process flow.

Increasing diminishing the incentive by changing the LSB does not change the presence of the image; much so the resultant stego image looks relatively same as the cover image. Figure 3.1 piece chart of water checking process has are portioned in two sections.

Two inputs are Cover image and secret message to be embedded in it and a stego image output.

First cover image is loaded into Matlab environment. Then separate layers of RGB image apply LSB algorithm on cover image. now load secret message in to Matlab first encrypt it with RSA encryption algorithm then convert encrypted secret message in to ASCII to binary code now using LSB algorithm embed text with cover image. Combine layers of cover image. finally we will have highly encrypted stego image. the process flow of proposed work has given in figure 3.2.

Figure 3.3 demonstrated the block diagram of image retrieval process to get the secret information from stego image.

First stego image has loaded into Matlab environment the separate layers of stego image read hidden information using LSB algorithm. Decrypt retrieved information with RSA decryption algorithm. The process flow of information retrieval has given in figure 3.4.

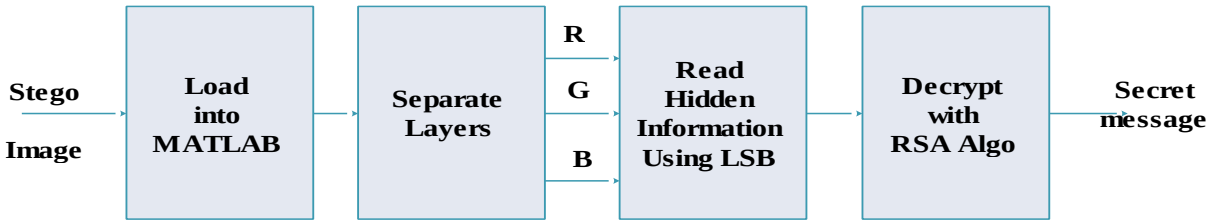

Figure 3.3 block diagram of retrieval process

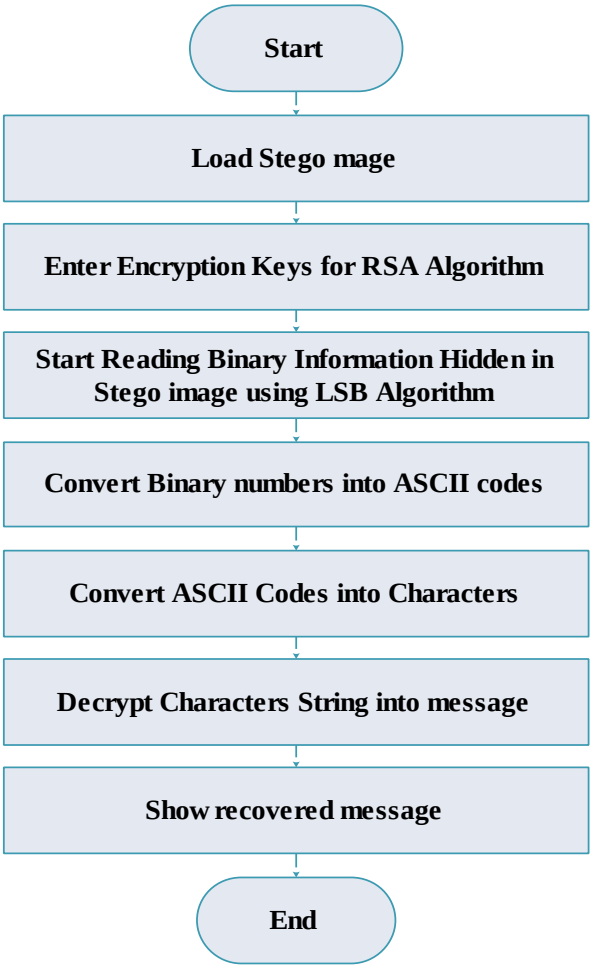

Figure 3.4 : Retrieval Process flow.

IV. EXPERIMENTAL RESULTS

Implementation and synthesis of proposed work has done on Matlab 11a. As an execution measure for image contortion because of hiding of message, the outstanding peak-signal-to noise ratio (PSNR), which is classified under contrast mutilation measurements, can be connected to stego images. Table 1 illustrated Peak Signal to Noise Ratio (PSNR) of Different Images with Variable Length Texts. for Lena, Baboon, Airplane image.

Fig.4.1 shows PSNR Curve for test images in dp on vertical axis and text size on horizontal axis. table 2 lists Mean Square Error (MSE) of Different Images with Variable Length Texts and figure 4.2 shows corresponding MSE Chart.

Test image Original Cover Images (a) Lena, (b) Baboon, (c) Airplane are given in figure 4.3. and corresponding Stego Images (a) Lena, (b) Baboon, (c) Airplane are shown in figure 4.4.

Comparison of Peak Signal to Noise Ratio (PSNR) in dB with Previous Methodology for All Images are given in table 3. 4.5 PSNR Comparison for Lena Image, fig.4.6 PSNR Comparison for Baboon Image. fig.4.6 PSNR Comparison For Airplane Image with previous methodology. Comparison of Mean Square Error (MSE) with Previous Methodology for All Images. are given in table 4 , and graphical comparison of MSE are demonstrated in figure 4.7, figure 4.8, figure 4.9 and fig. 4.10 respectively.

Table 1: Peak Signal to Noise Ratio (PSNR) of Different Images with Variable Length Texts

Image	PSNR (in dB) with Different Text Length				
	100	200	300	400	500
Lena	75.5314	78.261	80.421	81.4716	82.4115
Baboon	75.5636	78.7055	80.2816	81.4582	82.4375
Airplane	75.426	78.3918	80.2708	81.5205	82.5318

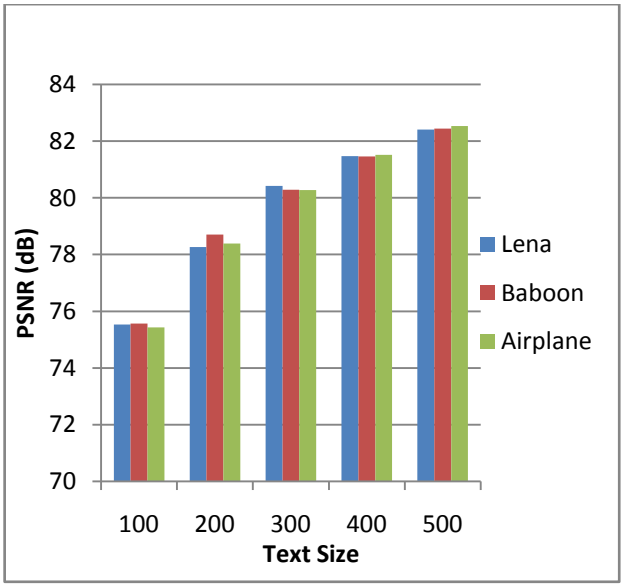

Fig 4.1. PSNR Curve.

Table 2: Mean Square Error (MSE) of Different Images with Variable Length Texts.

Image	MSE with Different Text Length				
	100	200	300	400	500
Lena	0.0018	0.001	0.00063	0.0005	0.0004
Baboon	0.0018	0.000943	0.00061	0.0005	0.0004
Airplane	0.0019	0.0009	0.0006	0.0005	0.0004

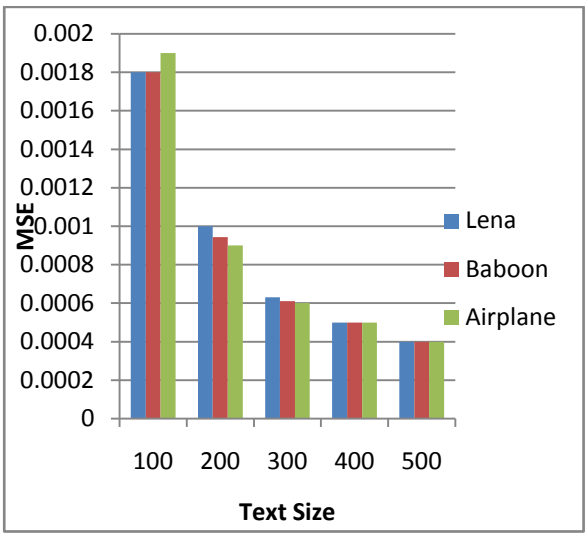

Fig.4.2 MSE Chart.

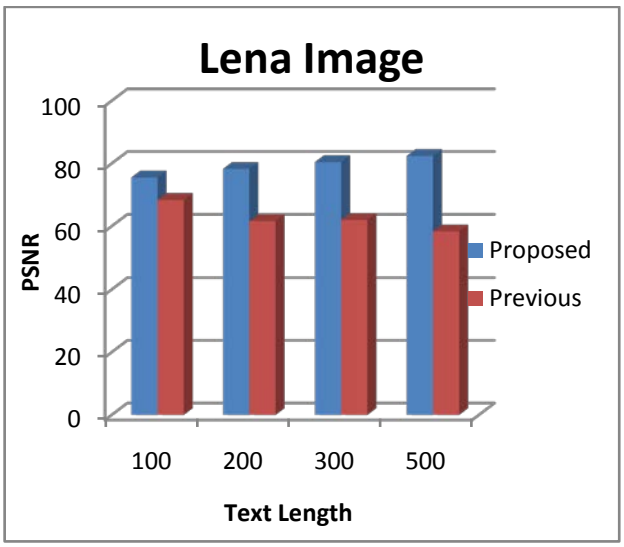

Fig.4.5 PSNR Comparison For Lena Image.

Fig.4.3 Original Cover Images (a) Lena, (b) Baboon, (c) Airplane.

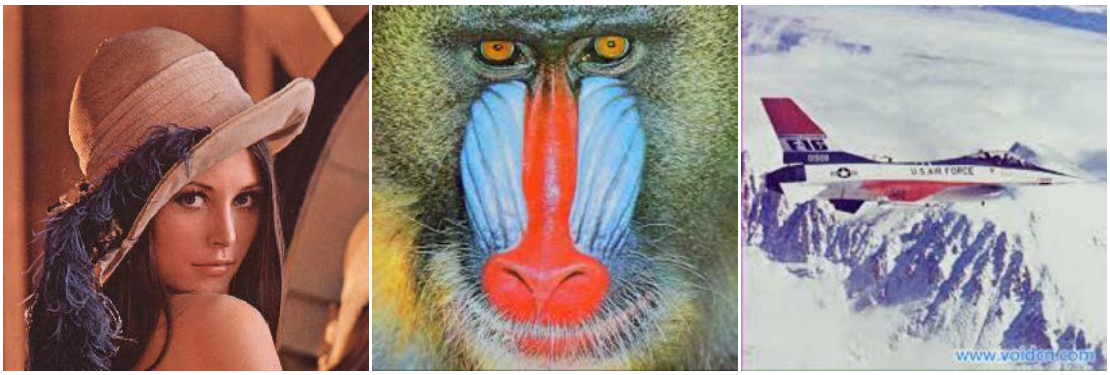

Fig.4.4 Stego Images (a) Lena, (b) Baboon, (c) Airplane.

Table 3: Comparison of Peak Signal to Noise Ratio (PSNR) in dB with Previous Methodology for All Images

Text Length	*Lena*		*Baboon*		*Airplane*	
	Proposed Methodology	*Previous Methodology*	*Proposed Methodology*	*Previous Methodology*	*Proposed Methodology*	*Previous Methodology*
100	**75.5314**	68.3805	**75.5636**	67.8384	**75.426**	67.5661
200	**78.2610**	61.5978	**78.7055**	59.3079	**78.3918**	59.6853
300	**80.4210**	61.9719	**80.2816**	59.3925	**80.2708**	60.0582
500	**82.4115**	58.3005	**82.4375**	56.1872	**82.5318**	56.4357

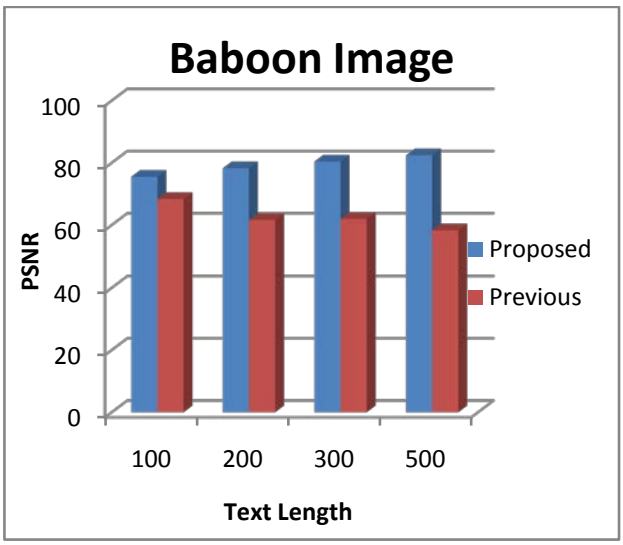

Fig.4.6 PSNR Comparison for Baboon Image.

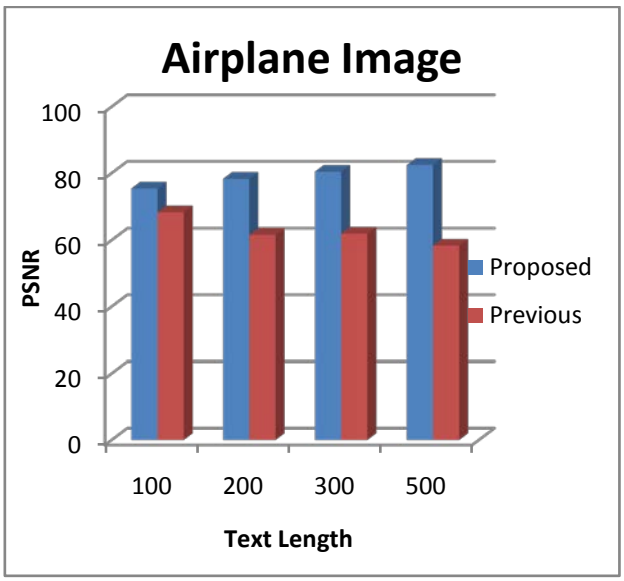

Fig.4.7 PSNR Comparison for Airplane Image.

Table 4: Comparison of Mean Square Error (MSE) with Previous Methodology for All Images.

Text Length	*Lena*		*Baboon*		*Airplane*	
	Proposed Methodology	*Previous Methodology*	*Proposed Methodology*	*Previous Methodology*	*Proposed Methodology*	*Previous Methodology*
100	**0.0018**	0.0094	**0.0019**	0.0115	**0.0019**	0.0115
200	**0.0010**	0.0450	**0.0009**	0.0690	**0.0009**	0.0690
300	**0.0006**	0.0413	**0.0006**	0.0582	**0.0006**	0.0582
500	**0.0004**	0.0962	**0.0004**	0.1477	**0.0004**	0.1477

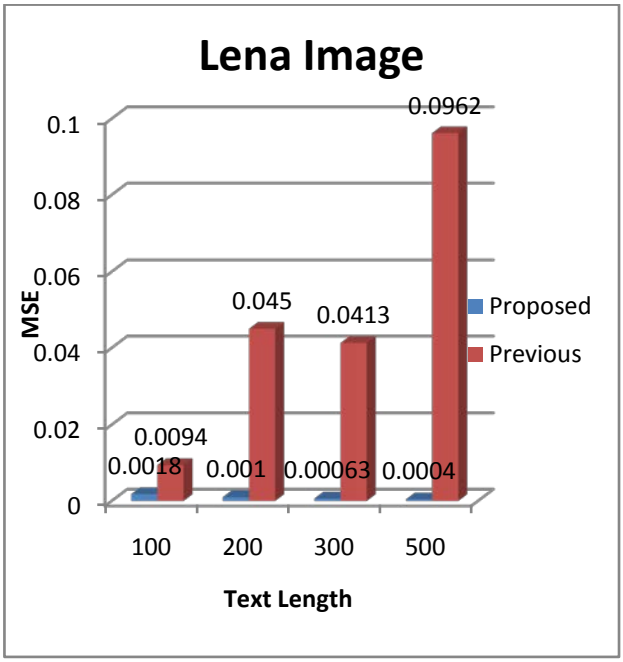

Fig.4.8 MSE Comparison for Lena Image.

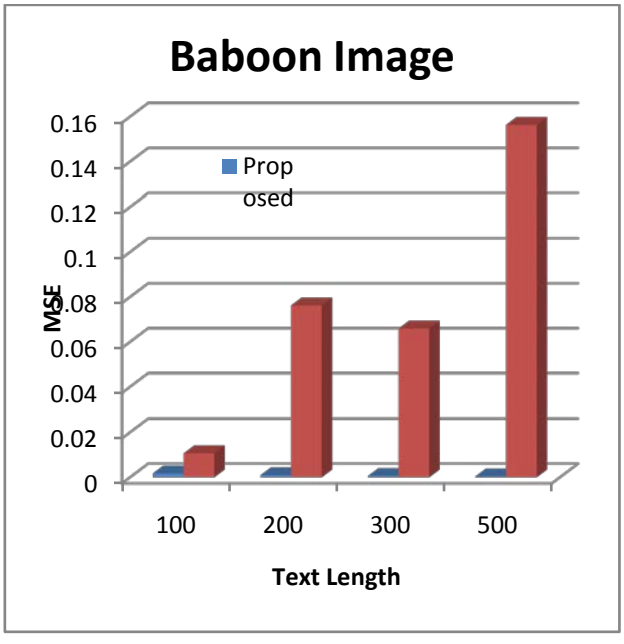

Fig.4.9 MSE Comparison for Baboon Image.

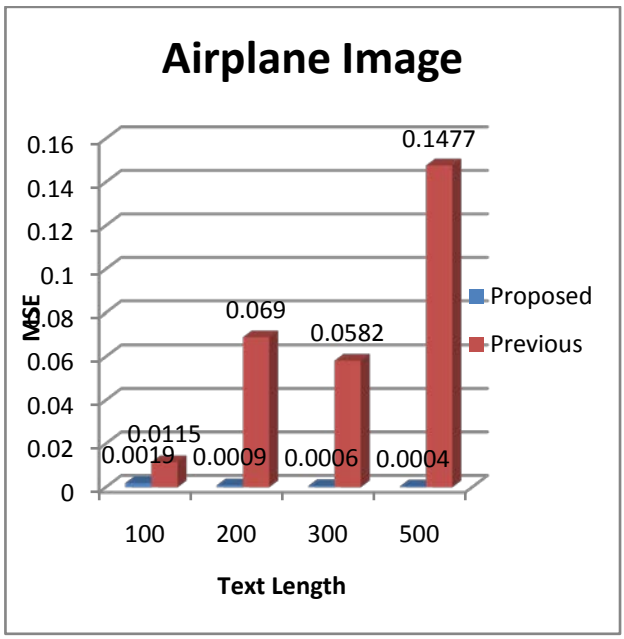

Fig.4.10 MSE Comparison For Airplane Image.

V. CONCLUSION AND FUTURE SCOPE

An image encryption system has been developed using RSA encryption algorithm as the cryptographic algorithm. it can be seen that most of the time in improved LSB insertion operation less number of bits are changed in comparison of existing LSB algorithm, due to which the process of detecting existence of hidden information becomes difficult and if someone is able to find then he cannot be able to use because it would be in encrypted form due to RSA encryption algorithm.

Now a days, image steganography is broadly used in steganography field. So there is lot to do as per research is concerned. both the algorithm image encryption using improved LSB and RSA encryption can be able to reduce the space and time complexity and to increase the level of encryption and security.

REFERENCES

[1] G. S. Charan, Nithin Kumar S S V, Karthikeyan B, Vaithiyanathan V and Divya Lakshmi K, "A novel LSB based image steganography with multi-level encryption," 2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore, 2015, pp. 1-5.

[2] S. Islam and P. Gupta, "Robust Edge Based Image Steganography through Pixel Intensity Adjustment," 2014 IEEE Intl Conf on High Performance Computing and Communications, 2014 IEEE 6th Intl Symp on Cyberspace Safety and Security, 2014 IEEE 11th Intl Conf on Embedded Software and Syst (HPCC,CSS,ICESS), Paris, 2014, pp. 771-777.

[3] M. M. Sadek, M. G. M. Mostafa and A. S. Khalifa, "A skin-tone block-map algorithm for efficient image steganography," 2014 9th International Conference on Informatics and Systems, Cairo, 2014, pp. DEKM-27-DEKM-32.

[4] A. K. Bairagi, S. Mondal and R. Debnath, "A robust RGB channel based image steganography technique using a secret key," Computer and Information Technology (ICCIT), 2013 16th International Conference on, Khulna, 2014, pp. 81-87.

[5] R. Kumar and S. Chand, "A new image steganography technique based on similarity in secret message," Confluence 2013: The Next Generation Information Technology Summit (4th International Conference), Noida, 2013, pp. 376-379.

[6] H. Hajizadeh, A. Ayatollahi and S. Mirzakuchaki, "A new high capacity and EMD-based image steganography scheme in spatial domain," 2013 21st Iranian Conference on Electrical Engineering (ICEE), Mashhad, 2013, pp. 1-6.

[7] P. H. Gani and M. Abdurohman, "Selective encryption of video MPEG use RSA algorithm," 2014 The 1st International Conference on Information Technology, Computer, and Electrical Engineering, Semarang, 2014, pp. 124-128.

[8] C. Patsakis, "Recovering RSA private keys on implementations with tampered LSBs," 2013 International Conference on Security and Cryptography (SECRYPT), Reykjavik, Iceland, 2013, pp. 1-8.

[9] Singla,D., Juneja,M. ”New information hiding technique using Features of image”, Journal of Emerging Technology in Web Intelligence, 6(2),pp.237-242.

[10] Mainberger,M.,Schmaltz,c.,Berg,M.,Weickert,J.,Backes,M. ”Diffusion-based image compression in steganography” 7432 LNCS (PART 2),pp.219-228.

[11] Udit Budddia and Deepak Kundur, “Digital video steganalysis exploiting collusion Sensitivity”,IEEE, 1(4):502-516, 2006.

[12] Provos, N. & Honeyman, P. ;“Hide and Seek: An introduction to steganography”, Security and Privacy, Vol.1, pp.32-44, 2003.

[13] Gomathymeenakshi,M., Sruthi, S .,Karthikeyan,B .,N ayana, M.

[14] ”An efficient arithmetic coding data compression with steganography”, in 2013 IEEE International Conference on Emerging Trends in Computing and Nanotechnology,ICE-CCN 2013 6528520,pp. 342-345.

[15] Lin, Y.-K. “A data hiding scheme based upon DCT coefficient modification”, Computer Standards and Interfaces 36(5),pp.855- 862.