Comparison of Steganography at One LSB and Two LSB Positions

R. S. Gutte
Department of E& TC, Sinhgad College of Engineering, Pune, Maharashtra, India.

Y. D. Chincholkar
Department of E& TC, Sinhgad College of Engineering, Pune, Maharashtra, India.

ABSTRACT
The use of Internet has been extensively increased. Sometimes, it is needed to keep the information secret and secure without attracting the attention of unauthorized person. Here, we proposed Text Steganography method along with cryptography for secret communication. It uses a simple method of steganography which is the data hiding at LSB positions. We compared the data hiding at one LSB and two LSB positions and evaluated the performance parameters like Standard Deviation, MSE and Entropy etc. The hiding of data at LSB positions is not fixed therefore it is a stronger approach. The data is encrypted using Extended Square Substitution Algorithm. It covers all the alphabets, special characters and mathematical symbols like µ, ß, þ, Ø. Each pixel of the image is considered as a byte. The encrypted text is then embedded at LSB positions of each pixel and the carrier image after embedding the data is called Stego image. The stego image is then transmitted and the secret data is then successfully extracted at the receiver. The MATLAB has been used for implementation.

General Terms
Cryptography,Extended Square Substitution Algorithm, Entropy, LSB method, MSE, Standard Deviation, Steganography.

Keywords
Extended square substitution cipher algorithm.

1. INTRODUCTION
The Steganography is a technique of hiding the secret data into a carrier, such as a ditital image, audio, video etc. Here, we implemented the text steganography. The word steganography is basically a Greek word. It is the combination of two words stegos and grafia. Stegos means to cover and grafia means writing. We can find many evidents of the Steganography in the history. The people in Rome and Greece used to carve the message on the wooden pieces and this writing would be then covered with the wax. The secret messages written on thin pieces of silk would be rolled on a small ball and then the ball would be swallowed by the army messenger. The common example of the steganography is, writing secret message on a paper with onion juice or ammonia salts and the secret message can be then exposed by heating the paper. The various type of the Steganography are text, image, audio or video steganography as per the type of the carrier. The steganography should be strong enough to hide the secret data securely and it should not change the basic properties of the carrier. The proposed method is stronger. Also, there is less threat of changing the basic characteristics of the carrier as we are using the LSB method. It is the age of the internet as we get the service just on a click. We use the internet for searching information, downloading and uploading of multimedia, to check E-mails, E-banking, Online reservations, therefore it is oftenly needed to keep the data secret without attention of hackers. Various Cryptographic algorithms has been used for security purpose but the main disadvantage of Cryptography is that, it attracts the attention of the third party as the encrypted data is visible to anyone and steganography avoids it, as the data is hidden behind a carrier. The secret data is firstly encrypted and then embedded using the LSB method. Therefore it gives a double layered security to the secret information.

Rest of the paper is arranged as; section 2 gives the brief overview of existing approaches. Section 3 covers the cryptography algorithm; Section 4 gives a detail explanation about data embedding procedures. Section 5 illustrates proposed algorithm, the results has been displayed in Section 6. Insection 7 the future scopeand the conclusions based on comparisons between our results and others results have been discussed.

2. BRIEF REVIEW OF EXISTING APPROACHES
Many authors suggested various methods of the steganography, a brief review of that will be taken. The most important thing is, while doing the steganography is that, the visible properties of the carrier should not be much changed. Least Significant Bit (LSB) method is the simplest method of steganography. The changes at the LSB positions of the carrier may not be noticeable because of the imperfect sensitivity of the human eyes[1]. The binary secret data replaces the least significant bit of an image. The embedding of the information at LSB position does not make significant change in the color of the pixel. The LSB method usually does not increase the file size, entropy and correlation values before embedding and after embedding the data therefore the process is a secure one[2][3]. Abbas Cheddad, Joan Condell et al. gave the brief review of digital image stegagraphy and compared Steganography, Watermarking and Encryption. Also, they elaborated some of the applications of the steganography such as Smart Identity cards, Medical Imaging Systems, Copyright. They also provided a brief survey about Steganography methods such as Steganography exploiting the image format, steganography inimage spatial domain, Steganography in image frequency domain, Adaptive Steganography [4]**Error! Reference source not found.**.

Ross J. Anderson and Fabien A.P. Petitcolas presented the limitations of steganography and gave contrast of variousdisciplines of cryptography and traffic security [5]. H. Motameni and his colleagues presented an approach of embedding the secret message at dark corners to use the carrier efficiently without making any visible effect on the image quality [6].Another way of inserting the secret message in frequency domain was proposed by Po Yuch Chen and

Hung Ju Lin. They used Discrete Wavelet Transform method for it. In this method the embedding should be done at high frequency coefficients [7]. P. Mohan Kumar and D. Roopa proposed The Block Matching method. As per this method one can use block matching procedure to search the highest similarity block for each block of the secret image and embed in LSBs of the carrier image [8]. Hardik J. Patel and Preeti K. Dave proposed LSB based image steganography means hiding secret image into another image. They presented the results of binarised data embedding at one, two and four LSBs they also did the statistical analysis with Histograms. They found that the insertion of secret data at one LSB position of the carrier provides good image quality but the less capacity whereas inserting data at four LSBs gives increased capacity but the degraded image quality [9]. S. Gurusubramani and his colleagues introduced the concept of Multi Layer Data Security (MLDS) [10].

Lisa M Marvel and Charles G Boncelet proposed to hide at the inherent noise places [11]. Another Method named as Two way block matching for image in Image steganography was proposed by Ran-Zan Wang and Yeh-shun Chen [12]. Xinpeng Zhang and his colleagues proposed an approach called "multibit assignment steganography for palette images", secret data can be embedded at the same coloured pixels of the gregarious pallette images [13]. Weiming Zhang, Xinpeng Zhang and Shuozhong Wang presented a method for implementing plus minus steganography [14]. When the secret message is hidden into a carrier image, It changes statistics of natural images [15]. If we avoid data embedding at the bits those carry the image features then it would make minimum effect on image features. H. Rifa-Pous and J. Rifa presented a steganographic protocol based on hamming code [16]. Paresh Marwaha et al. proposed a method called Visual Cryptographic Steganography in an image which uses a block or a grid cipher for cryptography and This cipher Containing the data is mapped in a 3-D matrix of RGB [17]. Mohammad Shirali-Shahreza presented an application of Text steganography for mobile phones for hiding the secret text data of SMS in MMS message [18].

Authors in [19] presented a method of Text steganography using the six square substitution algorithm and it was consisting of only the alphabets. The twelve square substitution algorithm covered alphabets as well as the special characters [20][21]. but the alphabet 'q' was missing andsome symbols like µ, Þ, ß, Ø, ×, ð, þ, ø, ÷, ¯, *ƒ* etc were not considered. Here, the missing alphabets 'q' as well as the above mentioned symbols are included. The proposed technique uses both cryptography and steganography. Therefore,it provides double layered security. The Extended Square Algorithm was implemented for various image formats using one bit LSB and two bit LSB method.

The Steganography Process canbe described using the following block diagram in Fig 1. The encryption of the secret message is done using a new cipher algorithm called extended square substitutioncipher algorithm, and then this cipher text is inserted at LSB places. For data embedding at one bit LSB may be at 6th or 7th or 8th position and it is notfixed. Whereas the data embedding at two LSB position uses 7th, 8th or 6th, 7th or 6th, 8th positions as per the variable value. The variable value can be 0 or 1 or 2.

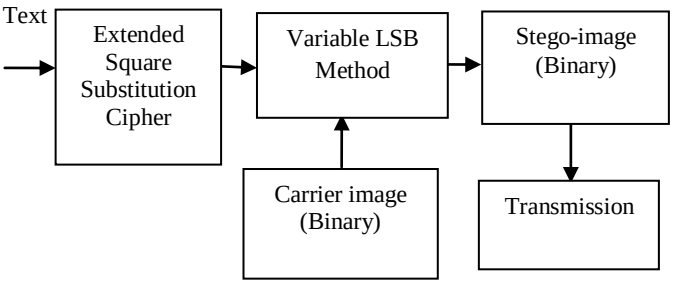

Fig 1: Steganography Process

After embedding the stego-image is sent to the receiver and receiver retrieves the cipher text from the said locations and then decrypts by using the extended square cipher algorithm to get the secret message.

3. EXTENDED SQUARE SUBSTITUTION CIPHER

Gandharba Swain and Saroj Kumar Lenka presented Square Substitution algorithms, The Six square substitution algorithm could cover only alphabets and its further improved version Twelve Square Substitution Cipher Algorithm covered alphabets as well as some special characters but it could not cover the alphabet q and some special symbols like µ, Þ, ß, Ø, ×, ð, þ, ø, ÷,(space) , ¯, *ƒ* [20] [21].

The Extended Square Substitution Cipher Algorithm includes numerals and special characters. It encrypts capital as well as small alphabets, digits and special characters. There are 9 by 6 matrices each arranged in a square, as shown in Table-1. Each of the 9 by 6 matrices contains the letters of the alphabet and another 12 by 6 matrices arranged in squares for digits and special characters and mathematical symbols, as shown in Table-2. All the special characters and digits are included in this table. Now we will discuss about the arrangement of the table. There are 54 letters arranged in the Table 1. Alphabet "q" is also included along with the letters like @, ? to have a square like arrangement of 54 letters. Each table is so arranged that, the plain text letter and its encryption letter should not be the same. Square-1, 2, 3, 4 indicates the plain text and their corresponding encryption in Square-5, 6, 7, 8.

Table 2 covers all the digits, special characters and mathematical symbols. Square-7, 8, 9, 10 covers all the numerals and special characters from a standard laptop and are arranged in 6 rows and 12 columns and their encryption text is in square 11, 12, 13 and 14 respectively.

While extracting the secret message, if the special characters and digits appeared it is referred to Table-2 and if the capital or small alphabet appears then it is referred to Table-1. Now we will see the working of this algorithm. This can be elaborated using an example.

Supposeone word 'India +91'. Its first alphabet is 'I'. Therefore, it is referred to table-1 and this capital alphabet is referred to square-1. Its corresponding row and column is calculated.

Table 1: Plain Text and Cipher Text (Alphabets)

Square-1	Square-2	Square-3	Square-4
a X b W c V d U e f T g S h R i Q j k P l O m N Y M o p L q K r J s I t u H v G w F x E y z D @ C ? B n A Z	a X f T k p u P z L b g H l D q v @ c W h S m r w O ? K d i G Y C s x n e V j R o t y N Z J F B U Q M I E A	s t u v w x y z A B C D E F G H I J K L M N O P Q R S T U V X W Y Z @ ? a b c d e f g h i j k l m n o p q r	s B K T a j t C L U b k u D M V c l V E N X d m w F o W e n y G P Y f O x H Q Z g p z I R @ h q A J S ? i r
Square-5	**Square-6**	**Square-7**	**Square-8**
T U V X a b c d e W Y Z @ ? f g h i s t u v O P Q R S K L j M k l m n N o p q r A B C D E F G H I J w x y z	T U V X W Y Z @ ? a b c d e f g h i j k l m n o p q r s t u v w x y z A B C D E F G H I J K L M N O P Q R S	Y H Q Z g p z I R @ h q A J S ? i r v E N X d m w F o s B K T a j t C L U b k u D M V c l W e n y G P x f O	j k l m n o p q r s t u v w x y z A B C D E F G H I J K L M N O P Q R S T U V X W Y Z @ ? a b c d e f g h i

Table 2: Plain Text and Cipher Text (Digits and Special Characters)

Square-7	Square-8	Square-9	Square-10
0 1 2 3 4 5 6 7 µ ß þ ð 8 9 ` ~ ! " # $ … « » ± % ^ & * ( ) _ - ¼ ½ ¾ Þ + = { [}] ; : Ø × ø ÷ ' ‘ \ | < , > . © ™ ® ° ¶ / ƒ † • ¹ ³ ² ¦ ¯ ñ	8 9 ` ~ ! " # $ … « » ± % ^ & * ( ) _ - ¼ ½ ¾ Þ + = { [}] ; : Ø × ø ÷ ' ‘ \ | < , > . © ™ ® ° ¶ / ƒ † • ¹ ³ ² ¦ ¯ ñ 0 1 2 3 4 5 6 7 µ ß þ ð	% ^ & * ( ) _ - ¼ ½ ¾ Þ + = { [}] ; : Ø × ø ÷ ' ‘ \ | < , > . © ™ ® ° ¶ / ƒ † • ¹ ³ ² ¦ ¯ ñ 0 1 2 3 4 5 6 7 µ ß þ ð 8 9 ` ~ ! " # $ …« » ±	+ = { [ ] ; : Ø × ø ÷ ' ‘ \ | < , > . © ™ ® ° ¶ / ƒ † • ¹ ³ ² ¦ ¯ ñ 0 1 2 3 4 5 6 7 µ ß þ ð 8 9 ` ~ ! " # $ …« » ± % ^ & * ( ) _ - ¼ ½ ¾ Þ
Square-11	**Square-12**	**Square-13**	**Square-14**
8 9 ` ~ ! " # $ … « » ± % ^ & * ( ) _ - ¼ ½ ¾ Þ + = { [}] ; : Ø × ø ÷ ' ‘ \ | < , > . © ™ ® ° ¶ / ƒ † • ¹ ³ ² ¦ ¯ ñ 0 1 2 3 4 5 6 7 µ ß þ ð	% ^ & * ( ) _ - ¼ ½ ¾ Þ + = { [}] ; : Ø × ø ÷ ' ‘ \ | < , > . © ™ ® ° ¶ / ƒ † • ¹ ³ ² ¦ ¯ ñ 0 1 2 3 4 5 6 7 µ ß þ ð 8 9 ` ~ ! " # $ … « » ±	+ = { [}] ; : Ø × ø ÷ ' ‘ \ | < , > . © ™ ® ° ¶ / ƒ † • ¹ ³ ² ¦ ¯ ñ 0 1 2 3 4 5 6 7 µ ß þ ð 8 9 ` ~ ! " # $ … « » ± % ^ & * ( ) _ - ¼ ½ ¾ Þ	' ‘ \ | < , > . © ™ ® ° ¶ / ƒ † • ¹ ³ ² ¦ ¯ ñ 0 1 2 3 4 5 6 7 µ ß þ ð 8 9 ` ~ ! " # $ … « » ± % ^ & * ( ) _ - ¼ ½ ¾ Þ + = { [}] ; : Ø × ø ÷

Its location is at 4th row and 8thcolumn then this alphabet ‘I’ is replaced with the alphabet having same row and column in Square-5 and its encryption text will be ‘n’. The next alphabet is ‘n’ therefore it is referred to first table and Square-2. Its corresponding row and column is calculated then it is replaced with the alphabet having same row and column position in Square-6 and its corresponding encryption text will be ‘A’. The next three letters are not the alphabets therefore they will be referred to table-2. The first letter is a space. Its location is 6th row and 3rdcolumn and its encryption text will be the ‘¦’, which is at the same location in the Square-11. The next symbol is ‘+’ and its encryption text will be ‘<’. This procedure repeats till the last letter comes. The following examples can illustrate the working of the algorithm:

i. *Plain text*: India +91
   Cipher text: nAuhT'^9

ii. *Plain text*: The proposed algorithm covers the mathematical symbols like µ, ß, þ, ð, ½, , ×, Ø, ©, ™.
   Ciphertext:
   YlD2YkFxJmBu2nucPigGcG2aFZLky2Hbe2nUp?
   BynNuknu2yzGVFnj2uueL2…•2«•2»•2±•2×•2•2™
   •2©•2²•2¦³

The algorithm is able to hide all the alphabets as well as special characters and mathematical symbols.

4. DATA EMBEDDING AND INDEX VARIABLE

The process of embedding message into an image can be explained as: Firstly, the carrier image is transformed into binary form. Onlyred plane out of Red, Blue and Green has been taken to insert the secret message in color image. Each pixel value is then converted into 8 bits. Each cipher text of the secret message is converted into bytes. Binarised bits of the cipher text are inserted into the carrier image. The process of inserting the data at LSB position is random and depends on variable x. Supposean image is n byte long. Divide it by 8. That much data can be hidden into that image when we are inserting the data at only one LSB of carrier image. The data sent through two LSB positions method is double than sending the data through one LSB. The data embedding at one LSB position depends upon a variable x. The x takes the values 0, 1, 2. When x=0, eight bit binary cipher text is embedded at 6thbit locations of first eight pixels of the carrier image. If x=1 next eight bit cipher text is embedded at 7th bit location at next eight pixels and when x=2, next eight bit cipher text is embedded at 8thbit location at next eight pixels. The insertion of the data at two LSB positions also depends on the variable x and the binarised text will be embedded at

two LSB positions of the carrier image pixel. The variable x takes the values 0, 1, 2, 3. If the value x=0, eight bit binary cipher text is embedded at $6^{th}$and 7^{th}bit locations of first four binary pixel value of the carrier image. If x=1 next eight bit cipher text is embedded at $7^{th}$and 8^{th}bit locations at next four binary pixel value and for x=2,next eight bit cipher text is embedded at $6^{th}$and 8^{th}bit locations at next four binary pixel value.For example, suppose alphabet 'A' is a cipher. Its ASCII value is 65. Its binary value is 01000001.First two bits from left are 01; second pair is 00, third 00 and fourth 01. If value of x=1, then to hide this eight bit data at every two LSBs of the binary pixel value, four subsequent pixels are required. Suppose we call those subsequent pixels as p, q, r, s; then the first pair '01'is inserted atat $7^{th}$and 8^{th}bit location of pixel p. The second pair '00' is insert at $7^{th}$and 8^{th} bit location of q and so on. Table-3 illustrates this concept.

Table 3: LSB Selection using Index Variable for two bit data embedding

Cipher Text	Binary pixels	Variable x	Insert	LSB positions
A (01000001)	p	1	01	7^{th} ,8^{th}
	q	1	00	7^{th} ,8^{th}
	r	1	00	7^{th} ,8^{th}
	s	1	01	7^{th} ,8^{th}
B (01100010)	t	0	01	6^{th} ,7^{th}
	u	0	10	6^{th} ,7^{th}
	v	0	00	6^{th} ,7^{th}
	w	0	10	6^{th} ,7^{th}

The Table-4 illustrates the scheme for Steganography at one bit LSB position of carrier image pixel. The binarised ASCII value of alphabet 'A'is inserted at one LSB position of eight carrier image pixels. Now it is clear that the data embedding at one LSB position takes eight consecutive pixels of the carrier image whereas the text data embedding at two LSB positions need only four consecutive pixels two hide the alphabet 'A'.

Table 4: LSB Selection using Index Variable for one bit data embedding

Cipher Text	Binary pixels	Variable x	Insert	LSB positions
A (01000001)	p	1	0	7^{th}
	q	0	1	6^{th}
	r	2	0	8^{th}
	s	1	0	7^{th}
	t	0	0	6^{th}
	u	2	0	8^{th}
	v	1	0	7^{th}
	w	0	1	6^{th}

5. THE PROPOSED ALGORITHM

The common process for both one LSB steganography and two LSB can be understood using following flowchart. The pixel values of the Carrier image is converted into binary. Plain text is encrypted using extended square Substitution Cipher. The cipher of the plain text is its substitution from the corresponding square. Every Cipher has its ASCII value. This ASCII value is then converted into binary format. The length of the carrier image is then checked. If it is able to conceal the secret message then the binary cipher is embedded into it.The resultant image is transmitted and the plain text is retrieved by applying the reverse procedure. The flow chart of the proposed algorithm is shown below.

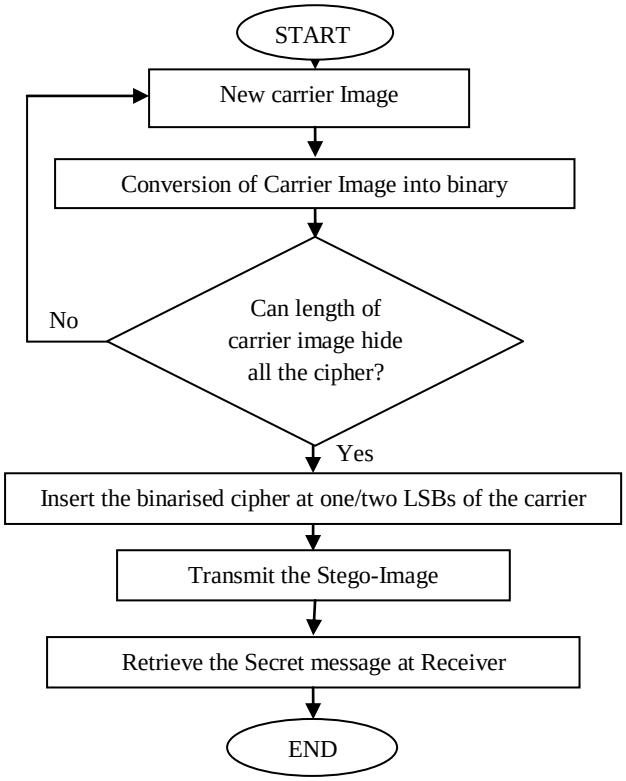

Fig 2: Flowchart of Proposed Algorithm

6. RESULTS

The plain text in example ii has been considered for encryption and the graphical user interface for two LSB and one LSB have been shown in Fig 3 and 4 respectively. The length of the plain text is 90 characters. Table- 5 shows image parameters for steganography at one LSB and Two LSB positions.Theresults for JPEG and BMP image formats have been verified and the proposed method works fine. Images a, b, c are in the JPEG format and their corresponding stego-images are d, e, f. The images g, h, i are in BMP format and their corresponding stego-images are j, k, l as shown in Fig 5.The statistical analysis for these images has been shown in Table-6. The image parameters like Mean, Standard Deviationand Entropy before embedding and after embedding the text have been calculated. From this statistical analysis it is clear that inserting data at two LSB positions hardly changes the carrier image parameters also the quality of the image is retained.

Table 5:Image parameters for Steganography at one and two LSB positions (Lena.bmp image)

Image Para-Meters	One LSB Method		Two LSB Method	
	Before	After	Before	After
Mean	95.6564	95.6564	95.6564	95.6563
Std. Devi.	10.2422	10.2422	10.2422	10.2422
Entropy	7.2338	7.2338	7.2338	7.2338
MSE	0.0013885		0.00085449	

Table 6:Image parameters for different image formats for two LSB Steganography

Before Embedding				After Embedding				MSE
Image	Mean	Std Devi.	Entropy	Image	Mean	Std. Devi.	Entropy	
a	84.5954	9.5236	7.7161	d	84.5961	9.5236	7.7163	0.002088
b	121.8739	10.2359	7.2845	e	121.8735	10.2359	7.2845	0.00331
c	120.4513	10.7926	7.4439	f	120.4504	10.7926	7.4441	0.0057
g	48.0961	8.9234	6.4817	j	48.0959	8.9234	6.4824	0.00052
h	116.4993	10.339	7.8136	k	116.4992	10.339	7.8136	0.0012
i	82.9008	9.4916	7.5051	l	82.9011	9.4916	7.505	0.0007

7. CONCLUSIONS

This secret communication system is based on both Cryptography and Steganography. We successfully verified the steganography at one LSB and two LSB positions and it is clear from the study that inserting the data at two LSB position does not change image parameters like Mean, Standard deviation, Entropy in much extent. Therefore, it retains the image quality similar to that of one bit LSB scheme. The amount of data sent through steganography at two LSB is double than that of one LSB scheme. This system is able to conceal all types of alphabets (small as well as capital), special characters and mathematical symbols. The variable x takes values as 0, 1, 2and 3. Embedding the cipher at two LSBs is decided by variable x. As the LSB in each pixel are not same but decided according to variable value, it is stronger approach and helps in minimizing the error.

8. ACKNOWLEDGEMENT

Both the authors work under Pune University. They are thankful to the teachers and management of Sinhgad college of Engineering and Dnyanganga College of Engineering for permitting them to pursue their research work.

9. REFERENCES

[1] Gurusubramani, T. Prabahar Godwin James, Venkatesh "Enhancing the Impregnability of Text Messages at Multiple Levels" Proceedings published in International Journal of Computer Applications (IJCA) 2012,pp.28-31.

[2] Mohammad Ali Bani Younes and Aman Jantan, "A New Steganography Approach for Image Encryption Exchange by using the LSB insertion", International Journal of Computer Science and Network Security, Vol 8, No 6,2008, pp. 247-254.

[3] Joachim J. Eggers, R.Bauml and Bernd Girod, "A Communications Approach to image steganography", Proc. Of SPIE Volume 4675, San Jose, Ca, 2002, pp. 1-12.

[4] Abbas Cheddad, Joan CondellKevinCurran, PaulMcKevitt "Digital image steganography: Survey and analysis of current methods", Elsevier Journal of Signal Processing 2010, pp.727–752.

[5] Ross J. Anderson and Fabian A.P. Petitcolas, "On The Limits of steganography", IEEE Journal of selected Areas in communication, Vol.16, No.4, 1998, pp. 474-481.

[6] H. Motameni, M.Norouzi, M.Jahandar. and A. Hatami, "Labeling method in Steganography", Proc. of world academy of science, engineering and technology, Vol. 24, 2007, pp.349-354.

[7] Po Yuch Chen and Hung Ju Lin, "A DWT Based Approach for Image Steganography", International journal of Applied Science and Engineering, Vol.4, No.3, 2006, pp. 275-290.

[8] P.Mohan Kumar and D.Roopa, "An Image Steganography Framework with Improved Tamper Proofing", Asian Journal of Information Technology, Vol. 6, No.10, 2007, pp.1023-1029.

[9] Hardik J. Patel and Preeti K. Dave, "Least Significant Bits Based Steganography Technique", International Journal of Electronics Communication and Computer Engineering (IJECCE-2012) pp.44-50.

[10] Gurusubramani, T. Prabahar Godwin James, Venkatesh "Enhancing the Impregnability of Text Messages at Multiple Levels" Proceedings published in International Journal of Computer Applications (IJCA) 2012,pp.28-31.

[11] Lisa M. Marvel and Charles G. Boncelet, "Spread Spectrum Image Steganography", IEEE Transactions on Image Processing, Vol. 8, No. 8, 1999, pp.1075-1083.

[12] Ran-Zan Wang and Yeh-Shun Chen, "High Payload Image Steganography Using two-Way Block Matching", IEEE Signal Processing letters, Vol. 13, No.3, 2006, pp161-164.

[13] Xinpeng Zhang, Shuozhong Wang and Zhenyu Zhou, "Multibit Assignment Steganography in Palette Images",IEEE Signal Processing Transactions, Vol.15, 2008, pp. 553-556.

[14] Weiming Zhang, Xinpeng Zhang and Shuozhong Wang, "A Double layered Plus-Minus One data Embedding Scheme", IEEE Signal Processing Letters, Vol. 14, No.11, 2007. pp. 848-851.

[15] Alvaro Martin, Guillermo Sapiro and Gadiel Seroussi, "Is steganography Natural", IEEE Transactions on Image processing, Vol. 14, No. 12, 2005. pp. 2040-2050.
[16] H. Rifa-Pous and J. Rifa, "Product Perfect Codes and Steganography", Digital Signal Processing, Vol.19, 2009, pp. 764-769.
[17] Piyush Marwaha, Paresh Marwaha, "Visual Cryptographic Steganography in images", Second IEEE conference on Computing, Communication and Networking Technologies 2010,PP. 193-206.
[18] Mohammad Shirali-Shahreza, "Steganography in MMS" Multitopic Conference, INMIC IEEE International 2007,pp.1-4.S.
[19] Gandharba Swain, Saroj Kumar Lenka, "Better Steganography using the Six Square Cipher Algorithm", Proc. of International Conference on Advances and Emerging Trends in Computing Technologies (ICAET-2010), Chennai, India, 2010, pp.334-338.
[20] Gandharba Swain and Saroj Kumar Lenka, "Steganography Using the Twelve Square Substitution Cipher and an Index Variable", IEEE transactions on Image Processing, 2011, pp. 84-88.
[21] R.S. Gutte, Y.D. Chincholkar, "The Twelve Square Substitution Cipher Algorithm based Steganography using MATLAB", Proc. of National level Conference on Emerging Trends in Electronics & Telecommunication at MITCOE, Pune, India, 2011, pp. 44-49.

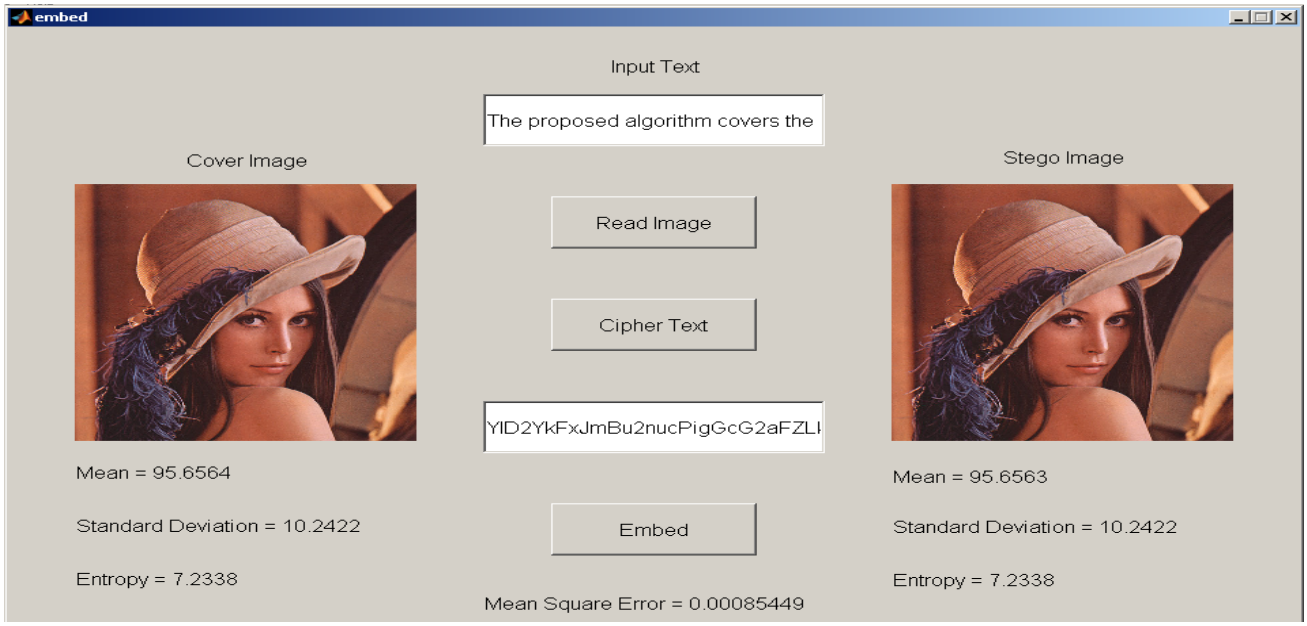

Fig 3: Steganography at Two LSB graphical user interface consisting of plain text and its cipher text of example ii.

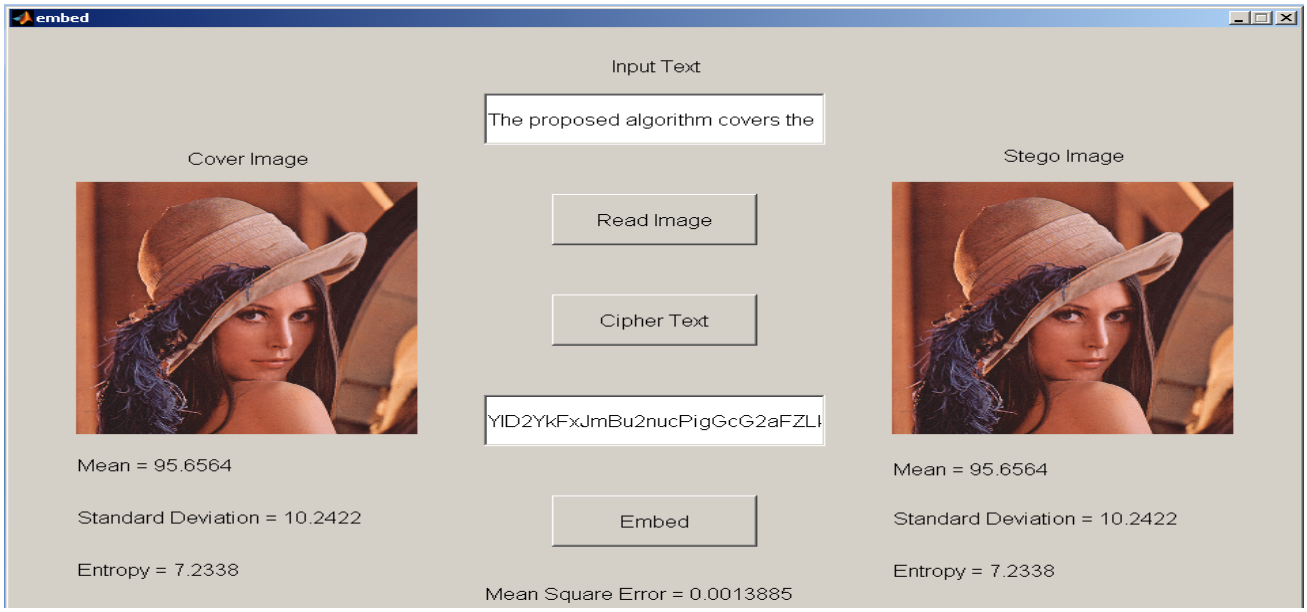

Fig 4: Steganography at one LSB graphical user interface consisting of plain text and its cipher text of example ii.

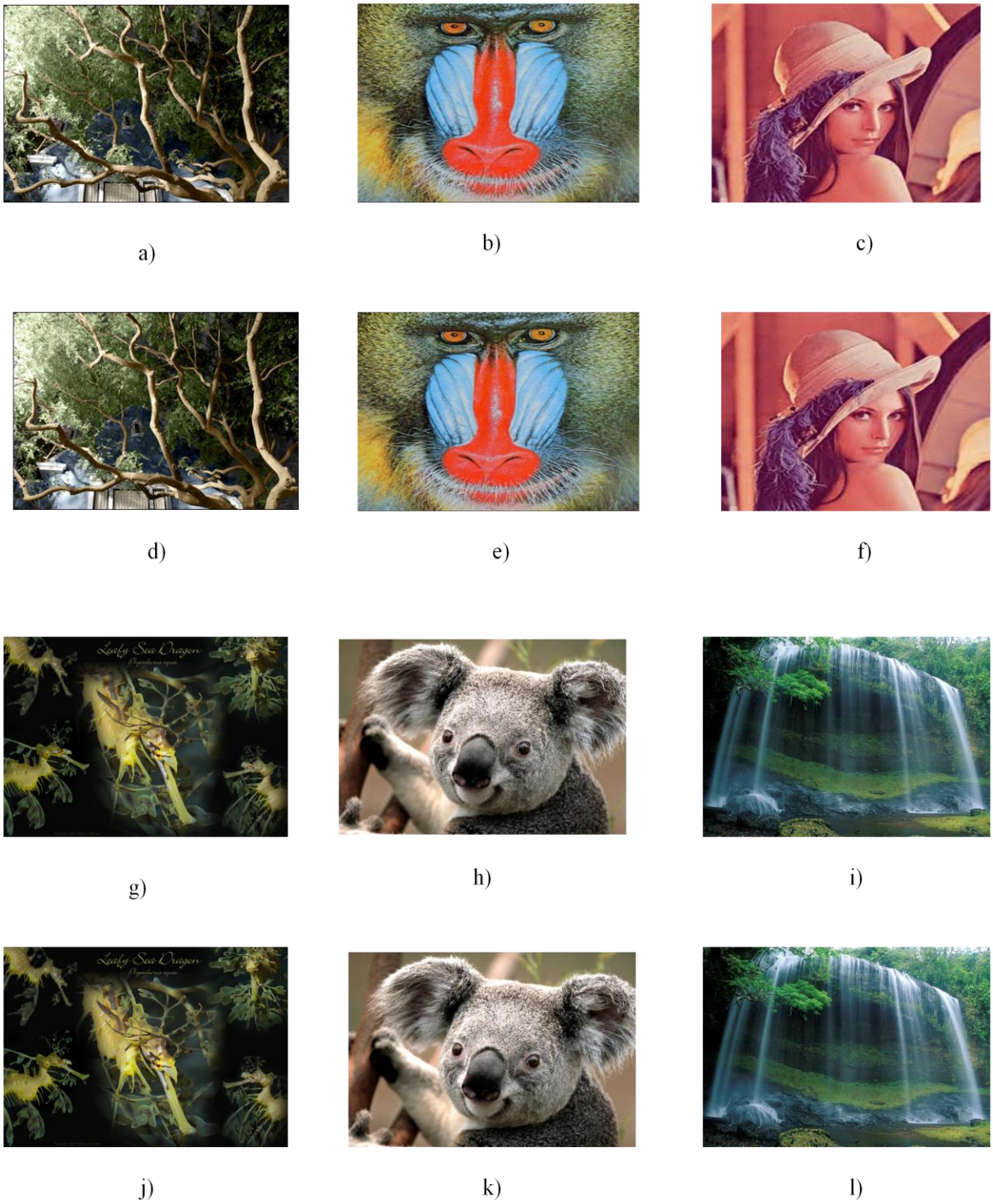

Fig 5: Verification the algorithm on different Image Formats (before embedding- a, b, c, g, h, i; after embedding- d, e, f, j, k, l)