Multilingual Image Steganography Using Matrix Substitution Cipher and Combinatorial Modulo Function

Mamta Jain
Department of Information Technology
Mody University of Science and Technology
Lakshmangarh, Rajasthan, India.
Email- mamta11.jain@gmail.com

Saroj Kumar Lenka
Department of Information Technology
Mody University of Science and Technology
Lakshmangarh, Rajasthan, India.
Email- lenka.sarojkumar@gmail.com

ABSTRACT
Information security is endlessly a challenging technology of the world. Image steganography is the technique through which the terribly confidential information can be hidden in a coated image so that, it should be quite unendurable to extract the said information by the intruder or by any snooping. In this research article an innovative technique is proposed which reveals steganography along with cryptography for more robustness to secret data, highest Least Significant Bit (LSB) implanting technique, and secrets information in divergent language (national language) above and beyond the English language secret communication. Here we have arbitrarily chosen Arabic, Urdu and English languages for secret information keeping in mind that this may give strongest illusion to the intruders. This novel approach comprehends in the senders side for encryption of Arabic, Urdu and English secret information using matrix substitution cipher algorithm, embedding position in the career image by using combination function with mod calculation, dynamically insertion of the cipher text bits in the career image at 5th to 8th bit location using the position indicator value and subsequently stego image is formed and then communicated over the network and in the reverse process once again it will be decrypted at receiver side to get the secret information. In this proposed technique instead of using Arabic, Urdu alphabets and digits directly, and Unicode's of the corresponding Arabic, Urdu alphabets and digits is used. Performance analysis observed using MSE and PSNR.

Keywords
Cryptography, steganography, LSB, substitution cipher, combinatorial modulo function.

ICCCT '15, September 25-27, 2015, Allahabad, UP, India.
 ISBN 978-1-4503-3552-2/15/09…$15.00
DOI: http://dx.doi.org/10.1145/2818567.2818603

1. INTRODUCTION
In this era one of the great challenges is ensuring confidentiality of the information in the communication and its application in the real world. Information hiding and secure communication are the two important concepts for safety of information. Secrets hiding procedures should have good visual/ statistical imperceptibility and required payload property.

The former one is necessary for the safety of hidden transmission and the later ensures that a big quantity of information can be moved. The term steganography cite coat writing. Steganography, the procedure of hiding secret data in other form of communication in such a manner that an onlooker could not deduce the appearance of transmission. Steganography techniques earning appreciation with current trade desire. It comprises heterogeneous procedures of hidden communications that coat the message. For hiding the information, steganography can be classified as image and multimedia steganography. For any secret communication we can provide two kinds of security mechanisms. In cryptography the secret identical information is enciphered by a key and an algorithm and sent on the passage. An entity or intruder can identify but not thieved the content by watching that something is under transmission, without knowing the clue. But in steganography the entity or intruder will not even surmise that some secret information is on transmission.

The steganography over cryptography provides the safety and puts the extant of the data secret over World Wide Web. The proposed procedures pledge two crease of security. Former, the secrets is enciphered and later, the enciphered secrets coated into the LSB plane of carrier image, so that the robustness of steganography can be enlarged by folding it with cryptography. Hiding the data into LSB plane of carrier image does not much affect its constitution.

2. LITERATURE REVIEW
Numerous procedures are used to hide secrets inside distinguish carriers. Anderson and Petitcolas insisted that there are some limitations in steganographic methods. They suggested an information theoretic procedure using Shannon's theory for perfect secrecy [1]. In the LSB (Least Significant Byte) procedure one bit of secrets is placed at the 8th bit of every byte of the carrier file, if the entropy and correlation values of stego image and carrier image are the same after enciphering then it shows process is safe[2]. Memon et. al introduces a new method for steganography in Arabic and Urdu texts. They appraise the existence of harakaat/Araabs in Arabic and Urdu phrases. By using Reverse Fatha, secrets are

hidden in the texts. This method can be classified under feature coding procedures [3]. Swain and Lenka give a steganography approach using two square reverse ciphers. In this embedding is done at 7th bit position in selected bytes. It provides two fold security- cryptography and steganography. As compared to LSB method [2] this algorithm shows more intrusion avoidance. But in this alphabet 'q' is missing as well as digits and special characters

are not incorporate [4]. In the next method, steganography using twelve square substitution ciphers is proposed, which incorporates both alphabets and digits. Embedding is performed in the carrier image at 6th and 7th bit locations or 7th and 8th bit locations or 6th and 8th bit locations of the different pixels (bytes) by using the value of an index variable But the alphabet 'q' and some special character 'space' are not incorporate [5]. Nag et. al introduces a novelty in steganographic system based on affine encipher algorithm and inserts the secrets at the least significant bit (LSB) position in order to suggest a solid security and imperceptible ocular quality to secret data [7]. Three methodical steganography techniques are approached by Maiti et. al. for hiding secrets in coated image. They used last two least significant bits for embedding secrets in diagonal pixels of the cover image. To encrypt the secrets Symmetric and public key cryptography are used [8]. Gutte et. al introduces a technique, in this data is enciphered using Extended Substitution Algorithm. This secret cipher text is coated at two or three LSB positions of the cover image [9]. Islam et.al introduces a novel steganography technique to hide big amount of secret data. Bitmap image and filtering based algorithm using MSB bits are used for this purpose. This method uses the new technique for status checking to embed and retrieval of secrets [10]. Here we are broaching a novel approach which can be understood in following sections. In module-II the functioning of matrix substitution cipher is disclosed, in module-III the methodology of embedding, in module-IV the proposed algorithm, in module-V the simulated results, in module-VI result analysis and in module-VII the conclusion.

3. MATRIX SUBSTITUTION CIPHER

A matrix substitution cipher algorithm is proposed which includes sixteen matrixes that encrypts into multiple language secret message. It uses four 6 by 9 matrices, given in table-1. It holds the letters of the English alphabet (upper case and lower case) and another four 5 by 6 matrices used for digits and special characters of key board, as given in table-1. Here table-1 preparation description is given: In matrix-1, fifty two English alphabets and two special characters are given, in this twenty six are capital letters and twenty six are small letters. Row contains nine alphabets and column contains six alphabets. Matrix-2 is build from matrix-1 by capturing the matrix-1 fourth row to first row place and other rows follows this row. Matrix-5 is created from matrix-1 by converting the rows into columns. Matrix-6 is created from matrix-5 by capturing the matrix-5 fourth row to first row place and other rows follows this row. The same method we have followed for matrix-3 and matrix-4 as well as for matrix-7 and matrix-8 in table 1. And another eight 6 by 8 matrices arranged randomly for forty eight Arabic, Urdu alphabets and digits as given in table-2.If the plain text is English alphabets/ digits/special characters then read it from left to right. And if it is Arabic, Urdu alphabets and digits then read it from right to left. For different languages we have to follow different tables for cipher text. Use table-1 for the English alphabets/digits/special characters, otherwise refer table-2 for Arabic, Urdu alphabets and digits. If the first English alphabet's plain secret text is in matrix-1 and its corresponding secret cipher text is in same row and column position of matrix-5. The second alphabet is in matrix-2 and corresponding secret cipher text is in same row and column position of matrix-6. Similarly third alphabet correlate to matrix-1 and matrix-5, 4th alphabet correlate to matrix-2 and matrix-6, 5th alphabet concur with matrix-1 and matrix-5 and so on. The first special character (including digits), its secret plain text is in matrix-3 and secret cipher text is in same row and column position of matrix-7. For second special character (including digits), the secret plain text is in matrix-4 and secret cipher text is in same row and column position of matrix-8. For the third special character (including numbers) the secret plain text is in matrix-3 and secret cipher text is in same row and column position of matrix-7.

Table 1: Plain secret text and cipher secret text (All English alphabets, digits & special characters)

Plain Text Matrix 1	Plain Text Matrix 2	Plain Text Matrix 3	Plain Text Matrix 4
ABC D E FGHI J K LM NOPQR ST U VWXYZ@ ?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 t u v w x y z ABC D E FGHI J K LM NOPQR ST U VWXYZ@	0 1 2 3 4 5 6 7 8 9 ` $ ^ & ( ) _ { [ } ] ; : " ' \ | , . 0 1 2 3 4 5 6 7 8 9 `	$ ^ & ( ) _ { [}] ; : " ' \ | , . 0 1 2 3 4 5 6 7 8 9 `
Cipher Text Matrix 5	**Cipher Text Matrix 6**	**Cipher Text Matrix 7**	**Cipher Text Matrix 8**
A G M S Y c i o u B H N T Z d j p v C I O U @ e k q w D J P V ? f l r x E K Q W a g m s y F L R X b h n t z	D J P V ? f l r x E K Q W a g m s y F L R X b h n t z A G M S Y c i o u B H N T Z d j p v C I O U @ e k q w	0 5 ` ( } ' 1 6 ) ] \ 2 7 $ _ ; | 3 8 ^ { : , 4 9 & [ " . 0 5 ` (} ' 1 6)] \	2 7 $ _ ; | 3 8 ^ { : , 4 9 & [" . 0 5 ` (} ' 1 6)] \

Table 2: Plain text and cipher text (Arabic, Urdu alphabets & digits)

Plain Text Matrix 9	Plain Text Matrix 10	Plain Text Matrix 11	Plain Text Matrix 12
ق پ ظ ز م غ ١ ٥ ش ث ح ی ژ و ٠ ے چ ت ٨ ن ھ ع ژ ب ٩ چ ض ٣ ١ ٤ خ ڈ ذ ر ک ث ہ گ ٧ ص ۶ ل ٢ ء س ف ط	ل م چ ف ب ٧ ض ز ت ط ن ٣ ث ١ ق پ ث ش ے ذ ک ٣ ڑ س ١ ص چ ء ڈ ی غ ھ و ٢ ہ ٠ ۵ ۶ ٩ ژ گ ر ح ٨ ظ خ ع	ء ۵ ف ن ع ش ٢ غ ق ط ی ١ ۶ ص ت گ ذ خ ے ٨ م ک ب ٧ ھ پ ض ٩ ١ ث ٹ ڈ ر س ٢ ٠ ژ ح ٣ چ د ج ظ ڑ و ل ر ہ	ث ٢ ض ١ غ م گ ١ ر ح ف ب ے ق ش س خ ۵ چ ڑ و ٢ ڈ ڈ چ ٧ ٨ ز ن ڑ ک ٠ ھ ل ٹ ٣ ہ ع پ ٩ ط ی ء ۶ ظ ٹ د ص
Cipher Text Matrix 13	**Cipher Text Matrix 14**	**Cipher Text Matrix 15**	**Cipher Text Matrix 16**
ٹ۶ ڑ ذ ی ز م س ن ط ٨ چ و پ ت ٩ ہ ے ١ ۵ گ ک ڈ ٢ ج د ع ژ ٠ ب ٣ ف ظ ر خ ض ق ء ٢ ١ ص ش ل ھ ٹ غ ح ٧	ش ج ١ ط و ع ض گ ی ب ٣ ٢ ٩ ح ٧ ڑ ت ل ا ء ٢ ذ خ ے م ٠ پ س د ف ۵ ٢ ھ ڑ ص ک غ ز چ ٨ ہ ق ٹ ڈ ٹ ن ر ظ	ژ ع غ ٠ س ھ ٹ ٢ ڈ ز خ ٣ ١ ر ف ہ ٹ گ ڑ ے ذ ٢ ۶ ص ق و ٹ د ش ء ٨ ۵ ظ ک ض ط م پ ی ح ل ٧ ١ چ ج ٩ ن ب	٣ ز ک چ ٢ ٢ ن گ ھ خ پ ی ح ٠ ص ٹ غ و ذ س ط ٨ ظ ض ق م ٧ ۵ ژ ہ ١ ٩ د ٹ ڑ ٹ ۶ چ ل ء ع ر ف ڈ ش ے ب ١

Table 3: Unicode for Arabic, Urdu alphabets & digits

Characters when they occur independently	Unicode (Hex)
ا and آ	0627 and 0622
ب	0628
ٻ	067E
ت	062A
ٹ	0679
ٽ	062B
ج	062C
چ	0686
ح	062D
خ	062E
د	062F
ڈ	0688
ذ	0630
ر	0631
ڑ	0691
ز	0632
ژ	0698
س	0633
ش	0634
ص	0635
ض	0636
ط	0637
ظ	0638
ع	0639

Similarly fourth special character (including numbers) correlates to matrix-4 and matrix-8 and so on. For the Arabic, Urdu alphabets and

digits secret plain text refers to table-2. For the very first Arabic, Urdu alphabets and digits see its plain text in matrix-9 and secret cipher text is in same row and column position of matrix-13.For second Arabic, Urdu alphabets and digits see the secret plain text in matrix-10 and secret cipher text is in same row and column position of matrix-14. For the third Arabic, Urdu alphabets and digits see the secret plain text in matrix-11 and secret cipher text is in same row and column position of matrix-15. For the fourth Arabic, Urdu alphabets and digits see the secret plain text in matrix-12 and secret cipher text in same row and column position of matrix-16. Similarly fifth Arabic, Urdu alphabets and digits correspond to matrix-9 and matrix-13, 6th Arabic, Urdu alphabets and digits correlate to matrix-10 and matrix-14, 7th Arabic, Urdu alphabets and digits correlate to matrix-11 and matrix-15 and so on.

For example

English alphabets/digits/special characters secret plain text is: Ak103

Corresponding secret cipher text: AQ501

Arabic, Urdu Unicode is: 062A 0621 0644 0642

Arabic, Urdu alphabets and digits plain text is: ت ء ل ق

Its cipher text would be: ص ڈ ٹ غ

Note: In this proposed method of enciphering of Arabic, Urdu alphabets/digits, first we insert Unicode corresponding to Arabic, Urdu alphabets/digits from table 3 individually. After that Unicode will be automatically converted to Arabic, Urdu alphabets/digits. By using this mechanism we are providing one level above security for inputting Arabic, Urdu alphabets/digits.

4. METHODOLOGY OF EMBEDDING

4.1 Flowchart

First of all the information to be hidden will be checked, which may be either the combination of English alphabets/digits/special characters or Arabic, Urdu alphabets/digits. If the plain text is English alphabets/digits/special characters then perform encryption using table 1 of matrix substitution cipher algorithm. Otherwise for Arabic, Urdu alphabets/digits use table 2 for encryption. After that apply combinatorial mod function on 8-bit block of cipher text for finding the embedding location in cover image. For English alphabets/digits/special characters read cipher text from left to right direction for embedding in 5th or 6th or 7th or 8th bit LSB position of cover image. And for Arabic, Urdu alphabets/digits read cipher text from right to left direction for embedding. After getting the stego image transmits it to the recipient. Recipient uses reverse operation to get the secret plain text from stego image.

4.2 Embedding Technique

Embedding process involves implanting the secret cipher text within the cover image by replacing the 5th or 6th or 7th or 8th bit of every pixel of cover image with the secret cipher text bit. The accessing of the above said LSB's in the cover image is explained below.

Step 1- Divide the secret cipher message bits into 8 bits blocks. Also divide the cover image into bytes.

Step 2- Now calculate the embedding location(5th or 6th or 7th or 8th bit) in every pixel(byte) of coat image for hiding the secret cipher data bits.

i) Calculate the total number of 8-bit secret cipher message blocks (B1, B2, B3,……Bk)

ii) Now combinatorial mod function is used to calculate the

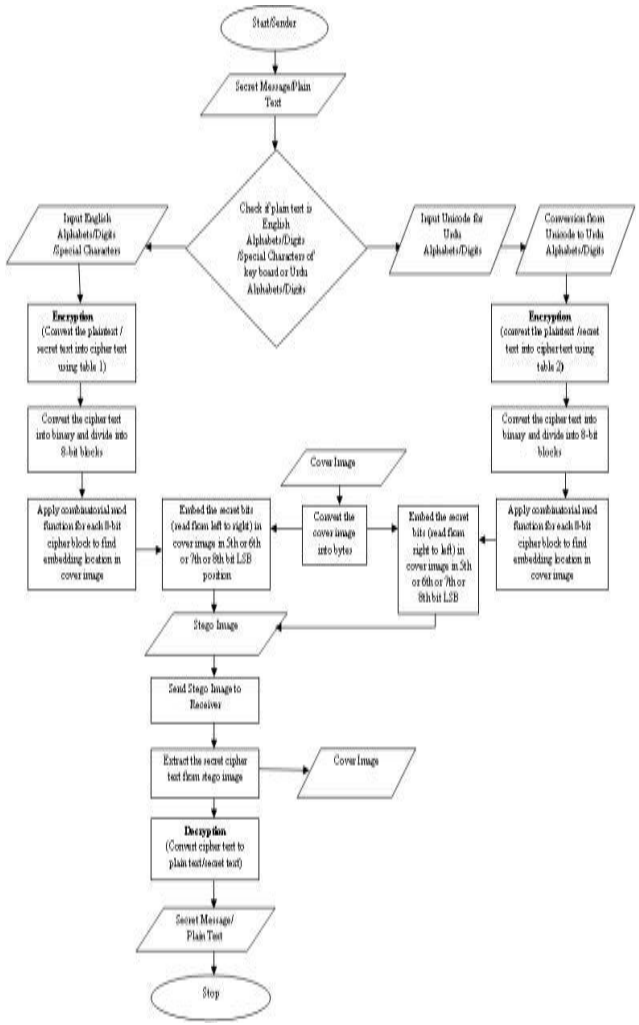

Figure 1. Flow chart of proposed algorithm

iii) embedding location in cover image.

Calculate the value of combination function for all message bits in one block.

$$A_i = nCr_i$$

Step 2- Now calculate the embedding location(5th or 6th or 7th or 8th bit) in every pixel(byte) of coat image for hiding the secret cipher data bits.

iv)Calculate the total number of 8-bit secret cipher message blocks (B1, B2, B3,……Bk)

v) Now combinatorial mod function is used to calculate the embedding location in cover image.

Calculate the value of combination function for all message bits in one block.

$$A_i = nCr_i$$

Here

n=Total no of secret cipher bits in one block C= Combination function

r= Position value of secret cipher bits (i=1 to 8),

For English alphabets/digits/special characters secret bit will be read

from left to right, and for Arabic, Urdu alphabets/digits secret bit will be read from right to left.

Repeat this process for each block up to Bk, After that calculate Mi= Ai-Si

Here

Ai= Calculated combination function for each message bit in one block

Si = ith secret message bit in one block (i=1 to 8), For English alphabets/digits/special characters secret bit will be read from left to right, and for Arabic, Urdu alphabets/digits secret bit will be read from right to left.

Repeat this process for each block up to Bk After that apply mod function to calculate the position indicator value for embedding location in cover image.

$$Li = Mi \bmod 4$$

If Li=0, then embedding location is 5th bit LSB position in cover image pixel (byte).

If Li=1, then embedding location is 6th bit LSB position in cover image pixel (byte).

If Li=2, then embedding location is 7th bit LSB position in cover image pixel (byte).

If Li=3, then embedding location is 8th bit LSB position in cover image pixel (byte).

Repeat this process for each block up to B_k

Step 3- Now implant the secret cipher bits in the corresponding location in cover image.

As instance suppose the secret cipher text is: 10101101 11001010. From table 4 we can see the embedding location of cipher secret bits in cover image bytes. More over the image features representing bytes should not be altered. In JPEG images (> mega bytes) maximum of 100 bytes carrying the image characteristics, image may be damaged by modification of these bytes.

Table 4: Embedding location in cover image bytes

Cover File byte	**Secret cipher bits (8bit/block) Si**	**Combinatorial Function operation (A_i= nCr_i)**	**Calculate Mi= Ai- Si**	**Calculate mod function (L_i=M_i mod 4)**	**Embed-ding location**
Byte A	1(Block 1)	8	7	3	$_8$th
Byte B	0(Block 1)	28	28	0	$_5$th
Byte C	1(Block 1)	56	55	3	$_8$th
Byte D	0(Block 1)	70	70	2	$_7$th
Byte E	1(Block 1)	56	55	3	$_8$th
Byte F	1(Block 1)	28	27	3	$_8$th
Byte G	0(Block 1)	8	8	0	$_5$th
Byte H	1(Block 1)	1	0	0	$_5$th
Byte I	1(Block 2)	8	7	3	$_8$th
Byte J	1(Block 2)	28	27	3	$_8$th
Byte K	0(Block 2)	56	56	0	$_5$th
Byte L	0(Block 2)	70	70	2	$_7$th
ByteM	1(Block 2)	56	55	3	$_8$th
Byte N	0(Block 2)	28	28	0	$_5$th
Byte O	1(Block 2)	8	7	3	$_8$th
Byte P	0(Block 2)	1	1	1	$_6$th
So on					

5. PROPOSED ALGORITHM

5.1 Sender Side Algorithm

Step-1: Check the secret message is English alphabets/digits/special characters or Arabic, Urdu alphabets/digits. If it is Arabic, Urdu alphabets/digits insert Unicode individually to corresponding Arabic, Urdu alphabets/digits. And convert it into Arabic, Urdu alphabets/digits.

Step-2: Apply the matrix substitution cipher algorithm on different language secret message to get the cipher text.

Step-3: Divide the whole secret cipher information into blocks of 8-bits.

Step-4: Take the coat image and transform it into bytes. The length of cover image is adequate enough to coat the cipher text.

Step-5: The first hundred bytes brings the image features. Next to store the information like number of secret cipher blocks and the start index of each block as well as start index of cover image bytes and position where embedding is being done, reserve from 101^{th} byte up to 5000^{th} byte. Then start from 5001^{th} byte onwards up to the last byte or up to a desired byte depending upon the length of your secret message.

Step-6: Implant the cipher text (one bit) into the coat n image (one byte) as considered in the embedding process.

Step-7: Embed number of secret cipher blocks and the start index of each block as well as start index of cover image bytes and position where embedding is being done in the reserved pixels i.e. pixel number 101 to 5000, using 5^{th} to 8^{th} bits of all those pixels.

Step-8: Now get the stego image and stop.

5.2 Receiver side algorithm

Step-1: Accept the stego image by the recipient.

Step-2: Repossess number of secret encipher blocks and the start index of every block as well as start index of coat image bytes and location where implanting has been done in the reserved pixels i.e. pixel number 101 to 5000, from 5th to 8th bits of all those pixels.

Step-3: Retrieve cipher text blocks from stego image using step-2.

Step-4: Concatenate all these secret message blocks, and got the secret cipher message.

Step-5: Apply the matrix substitution cipher algorithm on encipher text of different lingual secret data to decrypt it to get the secret plain text.

Step-6: Stop.

The demanded length of the cover file for embedding secret cipher is n bytes of the secret data. Here one bit of cipher is being hide in every pixel depending on some predetermined conditions. So one byte of cipher can be board in 8 bytes of cover image. Thus for n byte secret cipher text, a cover image of 8n bytes length required. Following characteristics are required for any steganographic technique: (i) must be able to coat a quantity amount of payload, (ii) must not be unguarded to profound search strikes, (iii) the indignity in, quality of the stego image must not be perceptible and (iv) must assure at least two folds of security. The given broached algorithm owns all these features.

6. SIMULATED RESULTS

The simulation and experimentation has been done using MATLAB for multilingual image steganography. To implement this GUI is being used to make convenient for user to handle it. Resultant simulated outcome is being displayed in figure 2.The clause peak signal-to-noise ratio is a technical terminology that defines the ratio between the maximum power of a signal and the power of damaged noise. The representation/quality of the signal is affected due to corrupted noise. An important index to readjust the quality of reformation of steganographic images is peak signal to noise ratio.

Figure 2. (a) Screenshot of the mechanism at sender after enciphering and implanting (English alphabets/digits/special characters).

Figure 2. (b) Screenshots of the mechanism at recipient after retrieving secret data and calculated PSNR & MSE data (English alphabets/Digits/special characters).

Figure 2. (c) Screenshots of the mechanism at sender with Unicode after enciphering and implanting (Arabic, Urdu alphabets/Digits).

Figure 2. (d) Screenshots of the mechanism at recipient side after retrieving secret data and calculated PSNR & MSE data(Arabic, Urdu alphabets/Digits).

The original cover image acts like a signal, and the noise is the defect included by some steganography mechanism. The PSNR at divergent payloads for English alphabets/digits/special characters and Arabic, Urdu alphabets/digits for same image is given in table 5 and 6 respectively. PSNR is calculated in decibels (dB). PSNR values less than 30 dB indicate a very low quality, i.e., twist caused by implanting can be clear. A high quality stego image should aspire for 40 dB and above [6].

PSNR outcome is defined by the mean square error (MSE) for two P×Q monochrome images, Where x as well as y are image coordinates, SGxy (stego image) and CVxy (cover image), one of the images is approved a noisy surmise of the other is defined as:

$$M.S.E = \frac{1}{PQ} \sum_{x=1}^{P} \sum_{y=1}^{Q} \left[SG_{xy} - CV_{xy} \right]$$

$$PSNR = 10 \log 10 \left\{ \frac{CVmax^2}{M.S.E} \right\}$$

Where CVmax = the maximum 255 pixel value, for 8-bit cover images. [6]

7. RESULT ANALYSIS

In this paper result is analyzed by embedding secret information either in 5th or 6th or 7th or 8th bit position, which directly depends on the value of the combinatorial mod function and position indicator. This shows the dynamicity of the proposed algorithm at run time. Here we are giving two fold security, former encrypting the secret plain text and after embedding the secret cipher text. The used enciphering algorithm is matrix substitution cipher algorithm. This technique has multi-exchange capability which is less vulnerable to frequency analysis attack and encrypted meaage attacks. The proposed algorithm is giving novelty for multilingual secret communication between multi communities. Here we are using secret message either in English alphabets/digits/special characters or Arabic, Urdu alphabets/digits. So that it provides more payloads too. If we are comparing this algorithm with other LSB cipher methods, it shows better intrusion avoidance in terms of randomness of secret bit insertion position.Using table 5 and 6, it is being observed that for cover image of size 10.8 KB(Leena.jpg) and secret cipher of size 14 bytes, the proposed method gives the MSE & PSNR Value 0.0005 & 80.56 respectively for English alphabets/digits/ special characters. And for the Arabic, Urdu alphabets/digits, MSE & PSNR values are 0.0012 & 77.09 respectively. Comparison of results of the existing techniques on the basis of PSNR and MSE values is shown in table 7.

Table 5: Observed MSE & PSNR value for different size (English alphabets/digits/special Characters) payloads

Image	Cover Image size(KB)	Size of cipher implanted (Bytes)	MSE (Mean Square Error)	PSNR (in decibles)
Leena.jpg	10.8	128	0.0054	70.77
Leena.jpg	10.8	64	0.0027	73.78
Leena.jpg	10.8	32	0.0013	76.96
Leena.jpg	10.8	14	0.0005	80.56
Leena.jpg	10.8	12	0.0005	81.04
Leena.jpg	10.8	8	0.0004	82.01

Table 6: Observed MSE & PSNR value for different size (Arabic, Urdu alphabets/digits) payloads

Image	Cover Image size(KB)	Size of cipher implanted (Bytes)	MSE (Mean Square Error)	PSNR (in decibles)
Leena.jpg	10.8	14	0.0012	77.09
Leena.jpg	10.8	12	0.0010	78.21
Leena.jpg	10.8	8	0.0007	79.45

Table 7. Comparison with schemes proposed by other Researchers

Scheme	Observed PSNR (in dB)	MSE	Imperceptibility/Quality
Gandharba Swain, Saroj Kumar Lenka[5]	74.41	0.0025	Good
Amitava Nag, Jyoti Prakash Singh, Srabani Khan,Saswati Ghosh[7]	30.48	0.0012	Not Good
R.S. Gutte, Y.D.Chincholkar and P.U. Lahane[9]	73.40	0.0030	Good
Md. Rashedul Islam, Ayasha Siddiqa, Md. Palash Uddin, Ashis Kumar Mandal and Md. Delowar Hossain[10]	74.39	0.0024	Good
Our Proposed Method	82.01	0.0004	Better

8. CONCLUSIONS

Proposed technique describes the image steganography through Arabic, Urdu and English languages using matrix substitution cipher and combinatorial modulo function. This proposed method provides two levels of security. We have calculated the embedding capacity and measured performance. It has been observed that the proposed method have better imperceptibility for the combination of Arabic, Urdu and English languages scripts. The stego-images do not produce any visual marks to be suspected. The estimated PSNR and MSE value for the proposed scheme is quite better than the all other methods published so far. So the proposed method have very much high image embedding capacity in terms of multi lingual secret data into the cover image is concerned. It can also be referred to devise new algorithms how to send different language secret text or image in audio as well as video applications.

9. REFERENCES

[1] Anderson, R.J., and Petitcolas, F.A.P.1998. *On The Limits of steganography*. IEEE Journal of selected Areas in communication, 16(4), pp. 474-481, Special Issue on Copyright & Privacy protection. ISSN 0733-8716.

[2] Younes, M. A. B., and Jantan, A. 2008. *A New Steganography Approach for Image Encryption Exchange by using the LSB insertion*. IJCSNS International Journal of Computer Science & Network Security, Vol. 8, No. 6 , pp. 247-254.

[3] Memon, J. A., and Kazi K. K. H. 2008. *Evaluation of steganography for Urdu /arabictext*. Journal of Theoretical and Applied Information Technology, pp. 232-237.

[4] Swain, G., and Lenka, S. K. 2010. *A Technique for Secure Communication using Message Dependent Steganography*. Special issue of IJCCT, Vol. 2, No. 12.

[5] Swain, G., and Lenka, S. K. 2011. *Steganography using the Twelve Square Substitution Cipher and Index Variable.* IEEE Conference on Image Processing, pp. 84- 88.

[6] Li, B., et al. 2011. *A survey on image steganography and steganalysis*. Journal of Information Hiding and Multimedia Signal Processing, Vol. 2, No. 2, pp. 142-172.

[7] Nag, A., Singh, J. P., Khan, S., and Ghosh, S.2011. *A Weighted Location Based LSB Image Steganography Technique.* Springer ACC 2011, Part II, CCIS 191, pp. 620–627.

[8] Maiti, C., Baksi, D., Zamider, I., Gorai, P., and Kisku, D.R. 2011. *Data Hiding in Images Using Some Efficient Steganography Techniques*. Springer SIP 2011, CCIS 260, pp. 195–203.

[9] Gutte, R.S., Chincholkar, Y.D., and Lahane, P.U.2013. *Steganography for two and three lsbs using extended substitution algorithm*. ICTACT Journal on communication technology, vol. 4, pp. 685-690, issue 01.

[10] Islam, M. R., Siddiqa, A., Uddin, M.P., Manda, A.K. and Hossain, M.D. 2014. *An Efficient Filtering Based Approach Improving LSB Image Steganography using Status Bit along with AES Cryptography*. IEEE Conference on Informatics, Electronics & Vision.