RESEARCH ARTICLE

STEGANOGRAPHY USING COMBINED ALGORITHM OF LSB AND XOR FOR DATA SECURITY.

Inder kumar[1] and Saravana kumar[2].
1. PG Scholar, Department of Computer Science, Christ University, Bengaluru, India.
2. Associate Professor, Department of Computer Science, Christ University, Bengaluru, India.

....

Manuscript Info	*Abstract*
....	....
Manuscript History	Steganography is the technique used to hide the information within a medium (image, audio, and video). This technique has been applied using different approaches (algorithm) such as Least Significant Bit algorithm, spatial algorithm, XOR algorithm, etc. All the algorithms have pros and cons when compared with each other. In order to give a highly efficient, secured and optimum algorithm, the combined LSB and XOR algorithm has been developed. This algorithm uses two algorithms i.e. Least Significant Bit (LSB) and Exclusive OR (XOR). Initially, the pixel values of an image (which is going to encrypt the message) and the message is been found, then all the 2nd LSB of the image is XORed with pixel value of the message and replaced with the LSB of the image. After the completion of above approach, information is sent to the particular end-user. The end-user for decryption has to take the 2nd LSB values of the encrypted image and XOR it with the LSB of the encrypted image. This approach is more efficient, secured and easy to use and understand.

....

Introduction:-
Steganography in Greek means 'steganos' means 'covered or secret' and 'graphy' means 'writing or drawing', general it means 'covered writing'. It is the art and science of secret communication. The main goal of Steganography is to hide information within a medium (image / text). It helps in hiding the importance of the secret message. There are there major components of steganography: a) cover message (steganos), b) secret message (writing) and c) secret key.

The most common reasons is that, intruders are able to gain illegal access of information and can misuse the information. It's not only limited to information or communication, it also applies on computer network because internet is the only medium to exchange information. The main reason to provide security is to maintain the confidentiality, integrity, availability and also to stop the illegal use of information. Most common way to stop this is to implement Steganography and cryptography. Image Steganography is an important area in the field of Data Security. As the demand of security and privacy

Increases, need of hiding their secret information is very important. If a user wants to send a private information to another person with security, he can send it through image Steganography.

Corresponding Author:- Inder Kumar.
Address:- PG Scholar, Department of Computer Science, Christ University, Bengaluru, India.

During the Steganography process, the sender has to select the appropriate message carrier (i.e. image, video, audio, text) and select the secret messages with the robust password. The effective Steganography algorithm must be selected which is able to encode the message in more secure way. Then the respective person can send the Stego file through the appropriate medium.

Literature Survey:-
Steganography technique is most commonly used in hiding the existence of information whereas cryptography is a technique which is used to keep the content of information secret. Both are complement to each other. [1]
The basic need in today's world is communication. Everyone wants to keep the private information of work to be secret and safe. We use human pathways in our daily life for transferring and sharing information Using internet or telephonically, but at a certain level it's not safe. [2]
Steganography and Cryptography are two methods which could be used to share information in a concealed manner. Cryptography includes message which is in encrypted form guarded by an encryption key which is known by sender and receiver only. But in cryptography it's always clear to intermediate person that the message is in encrypted form, but in Steganography the secret message is hidden within the cover image so that it couldn't be clearer to any intermediate person. The cover image containing the secret message is then transferred to the recipient. The recipient is able to extract the message with the help of retrieving process and secret key provided by the sender. [3]
The transfer of data through internet has made it easier to send the data accurately and fast to the destination, but in order to transfer the data securely to the destination without any modifications, there are many approaches like Steganography. [4]
The LSB technique is used to hide the secret image bits in the cover image to obtain the stego image. The stego image is transformed from spatial domain to the frequency domain using DCT. [5]

Problem Statement:-
The illegal use of information is increasing, in-order to secure the secret information we can use cryptography or Steganography technique. There are many image Steganography and cryptography algorithms has been already developed such as Least Significant Bit, Random Scattered (RS), Most Significant Bit (MSB) but LSB is most frequently used because it simply inserts the bit of secret message with the LSB of image. LSB is very easy, due to this detection of secret message is also easy. We need to develop an advanced version of LSB algorithms which is more secure than LSB.

Existing System:-
LSB is simple and most commonly used image Steganography algorithm. LSB is basically follow insertion process in which last bit is simply replaced by the bit of secret message.

At first, original image called cover image (I) is converted into 8-bit stream but if we are using a 24-bit image then it can also be divided into 3 block of 8-bit of red, green and blue color component. Then LSB or last bit of each 8-bit block is replaced with the bit of secret message/image sequentially or randomly using a pseudo-random generator with the help of stego-key.
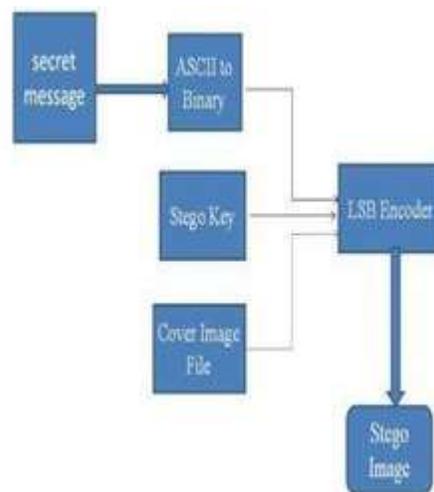
Fig 4.1:- LSB Insertion flowchart
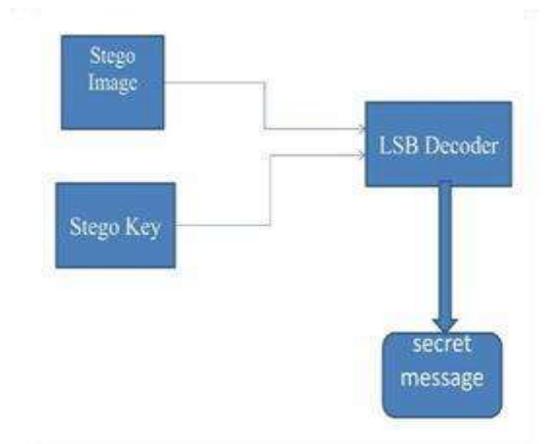
Fig 4.2:- LSB Extraction flowchart

In LSB Algorithm, only **Proposed System:-**
Least Significant Bit is replaced by Information bit but in Advanced LSB, least significant bit is not directly changed. It will change with the help of second least significant bit and the information bit.

Advanced L S B a n d X O R encryption Algorithm
1. Find the pixel value of cover image.
2. Find all 2nd LSB of the cover image
3. Find the binary value of message to be hidden.
4. Perform the operation with the help of rules between the value 2nd LSB of each pixel and bits of message.
5. Find the resultant value of LSB.

Advanced LSB and XOR decryption Algorithm
1. Find the pixel value of the stego image
2. Find all the LSB and 2nd LSB of stego image
3. Perform the operation with the help of rules between the values.
4. Find the resultant bits of image.
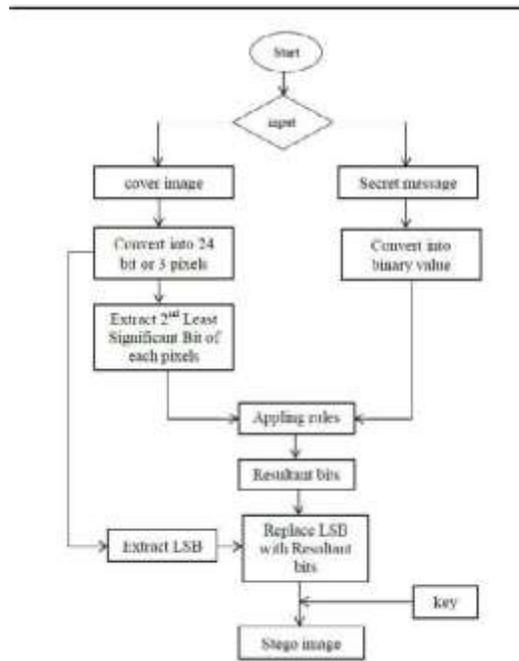
Fig 4.2:- LSB + XOR flowchart

Methodology:-

Suppose the value of three pixels of cover image is:

11010011 01100101 00111010
01110101 10101100 11011001
10010001 10101001 10110011

Suppose we want to hide 'A'. Binary value of A is 01000001

Table 6.1:- Hide Message and Calculation of the LSB

2nd LSB	Bits	Resultant
of cover	of	LSB to be
image	Message to	replaced
	be	with
	encrypted	LSB of
	[A]	cover
		Image
1	0	0
0	1	0
1	0	0
0	0	1
0	0	1
0	0	1
0	0	1
0	0	1
1	1	1

1101001**0** 0110010**0** 0011101**0**
0111010**1** 1010110**1** 1101100**1**
1001000**1** 1010100**1** 1011001**1**

Results:-

Text Encryption and Decryption using combined LSB and XOR algorithm
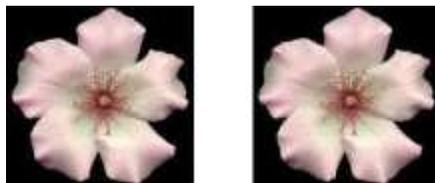
Original Image Message encrypted Image (stego Img)

Message decrypted Image

Fig 7.1 Text Encryption and Decryption using combined LSB and XOR algorithm (Flower)

Original Image

Message encrypted

Image (stego Img)

Message decrypted Image

Fig 7.2:- Text Encryption and Decryption using combined LSB and XOR algorithm (Leaf)

Original Image

Message encrypted
Image (stego Img)

Message decrypted Image

Fig 7.3:- Text Encryption and Decryption using combined LSB and XOR algorithm (Bear)

Table 7.1:- Encryption and Decryption values

Slno	Cover	Stego	Original
	Image	image	image
1	66806	66863	66806
2	30700	30757	30700
3	18600	18657	18600
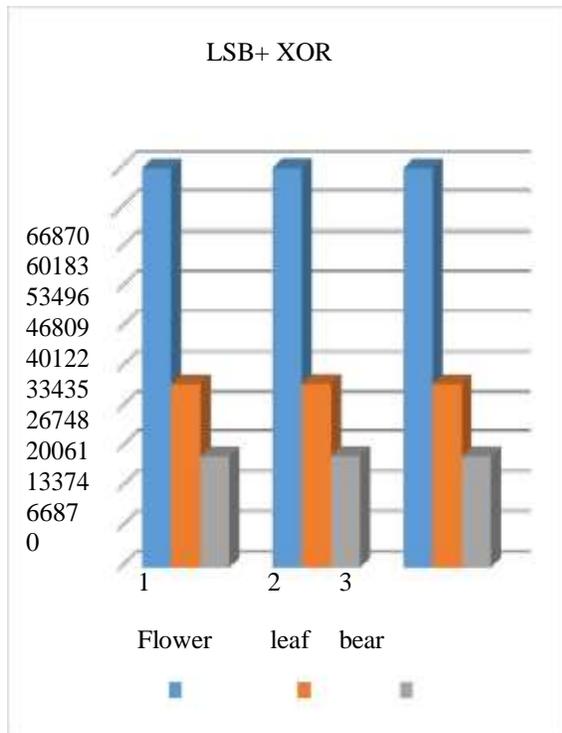
Fig 7.4:- Graphical representation of the combined LSB and XOR algorithm for text encryption/decryption

Table 7.2:- Comparison between the three algorithms

Slno	LSB	XOR	LSB+XOR
1	233561	116752	66863
2	155726	51238	30757
3	110066	38867	18657
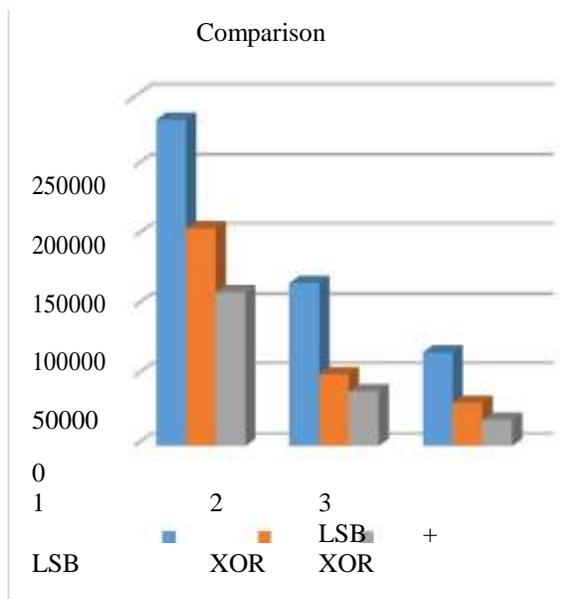
Fig 7.5:- Graphical representation for comparing LSB, XOR and LSB+XOR for text encryption/decryption

Image Encryption and Decryption using combined LSB and XOR algorithm

Cover image   Stego image

Cover image   Stego image

Cover image   Stego image
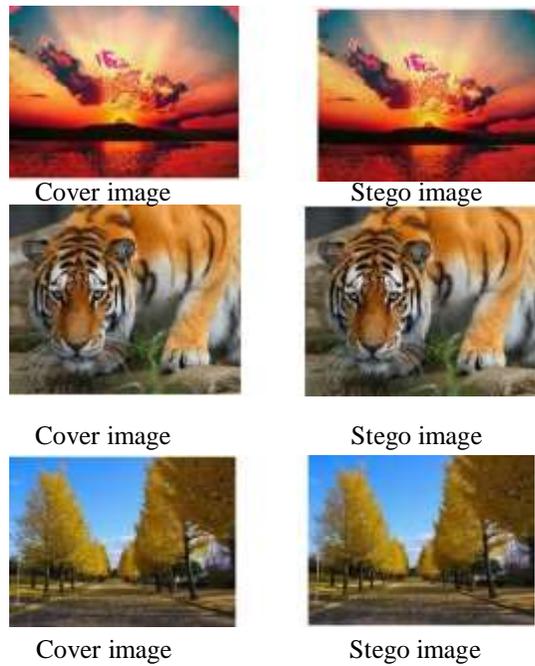
Fig 7.6:- Image Encryption and Decryption using combined LSB and XOR algorithm

Table 7.3 Encryption and Decryption values

Slno	Cover image	Stego image	Original image
1	66806	66903	66806
2	147456	147553	147456
3	150528	150625	150528
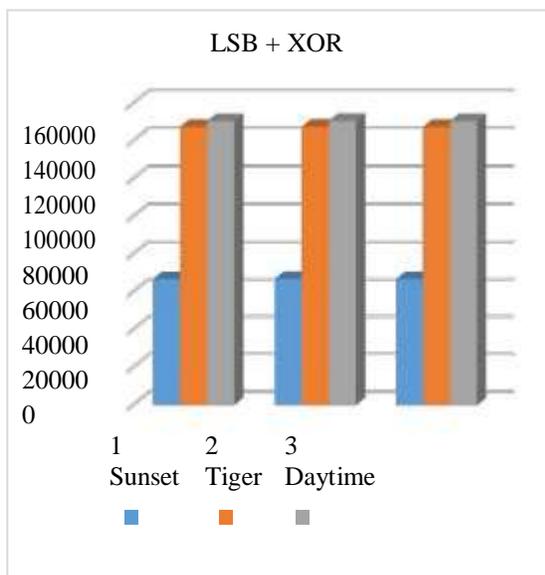
Table 7.4 Comparison between the three algorithms

Slno	Cover Image	Stego image	Original image
1	233501	116700	66806
2	446123	229670	147456
3	450187	231622	150528
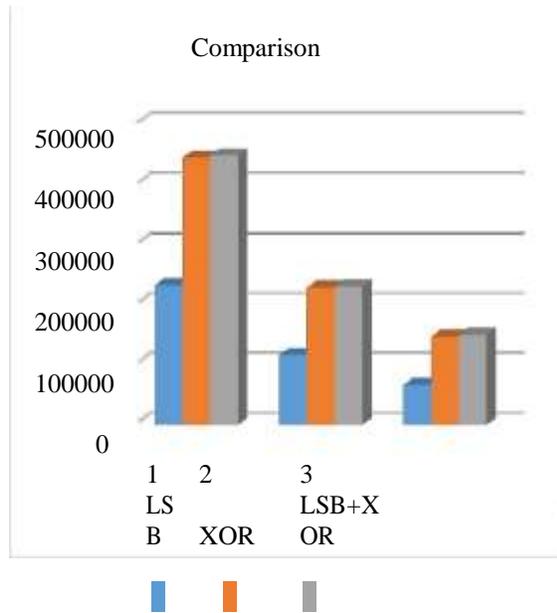
Fig 7.8:- Graphical representation for comparing LSB, XOR and LSB+XOR for text encryption/decryption

Conclusion:-

This paper work provides increased security and protects the hidden message from External (stego) attacks. There is negligible change in the image resolution when we embed the message into the image and the image is protected with the personal password. The Least Significant Bit and the XOR algorithms were used to give faster and reliable results and moderate for comparing both the algorithm's efficiency with the enhanced version.

The major limitation is, it is designed for bit map images (.bmp).

The future work is to extend the used for the different types of image formats like

Jpg, .png, etc. in the future. The security using LSB Algorithm is good but we can improve the level to certain extent by varying the carriers as well as using different keys for encryption and decryption.

Fig 7.7:- Graphical representation of the combined LSB and XOR algorithm for image encryption/decryption

References:-

1. Shilpa Gupta, Geeta Gujral and Neha Aggarwal **"**Enhanced Least Significant Bit algorithm For Image Steganography**"** International Journal of Computational Engineering & Management, Vol. 15 Issue 4, July 2012 ISSN: 2230-7893**,** www.IJCEM.org
2. Ramanpreet Kaur, Baljit Singh, Ishpreet Singh "A Comparative Study of Combination of Different Bit Positions In Image Steganography" International Journal of Modern Engineering Research Vol.2, Issue.5, Sep-Oct. 2012, ISSN: 2249- 6645, www.ijmer.com
3. Gandharba Swain and Saroj Kumar Lenka "A Technique for Secret Communication Using a New Block Cipher with Dynamic Steganography" International Journal of Security and Its Applications Vol. 6, No. 2, April, 2012
4. Savita and Mamta Juneja "A Review on Image Steganography" International Journal of Scientific & Engineering Research, Volume 4, Issue 5, May-2013ISSN 2229-5518
5. Shamim Ahmed Laskar and Kattamanchi Hemachandran "High Capacity data hiding using LSB Steganography and Encryption" International Journal of Database Management Systems (IJDMS) Vol.4, No.6, December 2012
6. Y. Benlcouiri , M. C. Ismaili, A. Azizi "Securing Images by Secret Key Steganography" Applied Mathematical Sciences, Vol. 6, 2012, no. 111, 5513 – 5523
7. Dr. Mohammed Abbas Fadhil Al-Husainy "Message Segmentation to Enhance the Security of LSB Image Steganography" International Journal of Advanced Computer Science and Applications, Vol. 3, No. 3, 2012
8. J. K. Mandal and Debashis Das "Colour Image Steganography Based on Pixel Value Differencing in Spatial Domain" International Journal of Information Sciences and Techniques (IJIST) Vol.2, No.4, July 2012
9. Suvarna Patil and Gadendra Singh Chandel "Performance Analysis of Steganography Based on 5-Wavelet Families by 4 Levels -DWT" International Journal of Advance Research in Computer Science and Management Studies Volume 1, Issue 7, December 2013 ISSN: 2321-7782 (Online)
10. Anil Kumar and Rohini Sharma "A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique" International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 7, July 2013 ISSN: 2277 128X