DATA HIDING IN ENCRYPTED IMAGES USING BLOCK SMOOTHNESS & SCAN TECHNIQUE

[1]Kamal Kishor Joshi, [2]Santosh Kumar Mishra ,[3]Asheesh Kumar ,[4]Vinod Nirala, [5]VaibhavBansal

[1]Assistant Professor,[2]Associate Professor,[3]Assistant Professor, [4]Assistant Professor,[5]Lecturar

[1]CSE Department at JBIT Dehradun,[2] CSE Department at JBIT Dehradun,[3]CSE Department at JBIT Dehradun,

[4]Mechanical Department at JBIT Dehradun,[5]CSE Department at JBIT Dehradun

Abstract: Reversible information covering up is a strategy that is utilized to shroud information inside a picture. The information is covered up such that the correct or unique information isn't obvious. The concealed information can be recovered as and when required. There are a few strategies that are utilized as a part of reversible information concealing methods like Watermarking, Lossless inserting and encryption.

In the information covering up in encoded pictures we implanted the information in the scrambled picture and afterward after we utilize a few calculations for instance Randomized XOR system, Flipping bit procedure, Bit length exhausting strategy, Modified SCAN calculation.

By utilizing every one of these systems we accomplish the lossless picture and the first information. We likewise utilize the pixel rearranging strategy for enhancing the security of our information and we utilize the idea of piece smoothness for enhancing the entropy of the picture or we can state the irregularity of the picture. So we can state that we accomplish the reversible information.

***Index Terms* -Flipping bit technique, Bit length expanding technique, SCAN algorithm, Stenography, Cryptography, Watermarking**

I. INTRODUCTION

A. Steganography and Watermarking

In this day and age, it is effectively to deliver advanced data by different means. Creation of such data has turned out to be extremely convenient as well as exceptionally shoddy. Subsequently, this data can likewise be conveyed to anybody without much measure of cost. This causes to disperse the data boundless number of times with boundless duplicates of the data. Sharing and dispersion of data is helpful and fundamental on one hand however then again it has genuine downsides when the data is touchy or limited by the rights. For instance, copyright information can't be shared without consent, which can't be taken care while disseminating the data indiscriminately. Keeping in mind the end goal to confine such unlawful dispersion of data, some sort of systems is fundamental. Steganography and watermarking bring an assortment of essential procedures how to hide primary data in an imperceptible or potentially in irremovable path in picture, sound and video information. Watermarking and steganography are fundamental parts of fasts creating territory of data covering up.

B. Steganography versus Watermarking

There are noteworthy, however limit contrasts amongst steganography and watermarking. Let 'd' be the coveted picture, sound and video information 'm' be some message inserted into data 'd' and 'd' be the information got in the wake of applying the message m into 'd'. The fundamental objective of steganography is to conceal a message m in some picture, sound or video (cover) information d, to get new information d', for all intents and purposes very much like from d, by individuals, such that a busybody cannot recognize the nearness of m in d'.

The principle objective of watermarking is to hide a message m in some sound or video (cover) information d, to get new information d', fundamentally the same as from d, by individuals, such that a busybody cannot evacuate or replacement.

The objective of steganography is to cover a message in balanced correspondences and the objective of watermarking is to shroud message in one-to-numerous interchanges.

C. Steganography/Watermarking versus Cryptography

Since steganography and watermarking both include some message to be covered up in the first information, they appear to be like cryptographic exercises, nonetheless they are not. There is critical distinction between steganography/watermarking and cryptography in spite of the fact that the motivation behind both these methods is to give classified correspondence. Cryptography disguise the substance of the message from an aggressor, yet not the being of the message. Steganography/watermarking even cover the very presence of the message in the liaise information. Thusly, split the framework is diverse for cryptosystems and stegosystems (watermarking frameworks).

A cryptographic framework is crushed when the assailant can read the private message. Shattering of a steganography/watermarking framework has two phases:

a) The aggressor can identify that steganography/watermarking has been utilized.

b) The assailant can read, adjust or isolate the disguised message.

A steganography/watermarking framework is considered as unreliable as of now if the location of steganography/watermarking is conceivable.

II. PROPOSED METHODOLOGY

A. Data hiding technique

In the proposed philosophy we talk about the modules of making the systems for information stowing away. To begin with we will examine how we inserted the information into the picture through figureIn this system a cover picture is scrambled then after we accomplish an encoded picture assume in the encoded picture we have taken a pixel in second line and third section.

Let the pixel (2,3) computerized esteem =124 then after we will change over the pixel (2,3) advanced an incentive into the twofold (0,0,1,1,1,1,1) at that point we will supplant and alter the parallel and change over it into decimal again now let the new computerized estimation of pixel (2,3) is 147.

Assume we need to inserted the information 'War' in pixel (2, 3). To begin with we will change over it into ASCII then after we will change over it into parallel

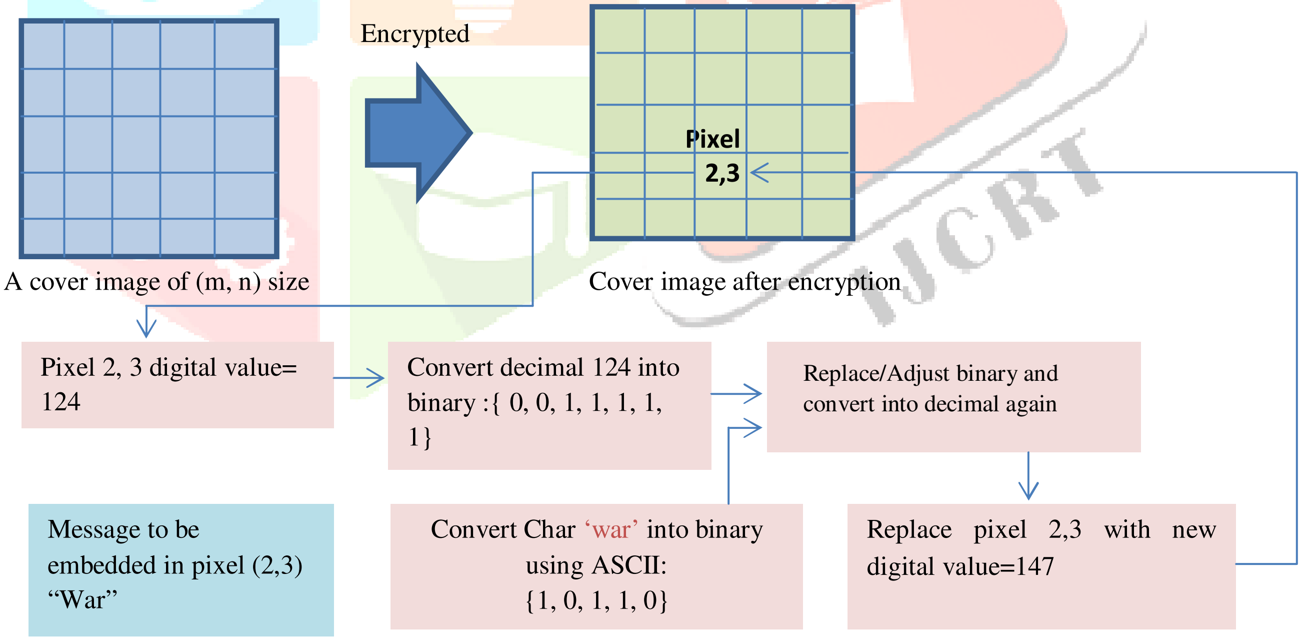
Encrypted
Pixel
2,3
A cover image of (m, n) size
Cover image after encryption
Pixel 2, 3 digital value= 124
Convert decimal 124 into binary :{ 0, 0, 1, 1, 1, 1, 1}
Replace/Adjust binary and convert into decimal again
Message to be embedded in pixel (2,3) “War”
Convert Char ‘war’ into binary using ASCII: {1, 0, 1, 1, 0}
Replace pixel 2,3 with new digital value=147

Fig 1. Data hiding technique

B. Base Code Methodology

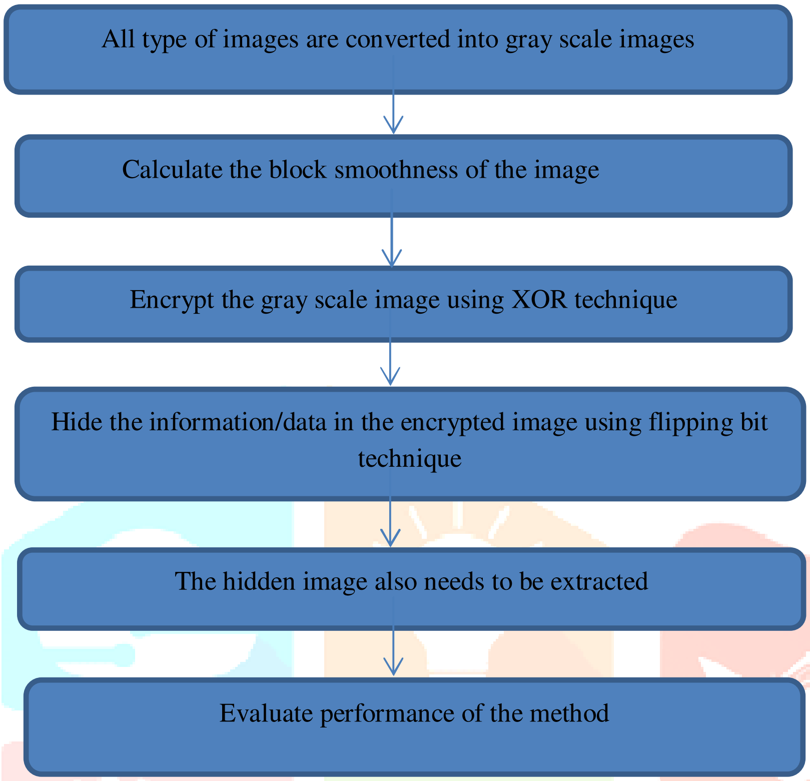
All type of images are converted into gray scale images
Calculate the block smoothness of the image
Encrypt the gray scale image using XOR technique
Hide the information/data in the encrypted image using flipping bit technique
The hidden image also needs to be extracted
Evaluate performance of the method

Fig 2. Base code methodology

In the base code strategy first we will change over the first hued picture into the dim scale picture then after we compute the piece smoothness of the picture then after encode the dim scale picture utilizing XOR system then after we conceal the data/information in scrambled picture utilizing flipping bit procedure. At the beneficiary end we separate the concealed picture. Finally we assess the execution of the strategy

1) Error rate

2) Peak Signal to Noise Ratio

PSNR is most effectively characterized through the mean squared error(MSE). Given a noise-free m*n monochrome picture *I* and its noisy estimation *K*, MSE is defined as:[4]

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

The PSNR is defined as:[4]

$$PSNR = 10\ \log_{10}(MAX_I^2)/(MSE)$$

$$PSNR = 20\ \log_{10}(MAX_I)/\sqrt{(MSE)}$$

$PSNR = 20\log_{10}(MAX_I)$ -10 $\log_{10}$ (MSE)

C. Modified Code Methodology

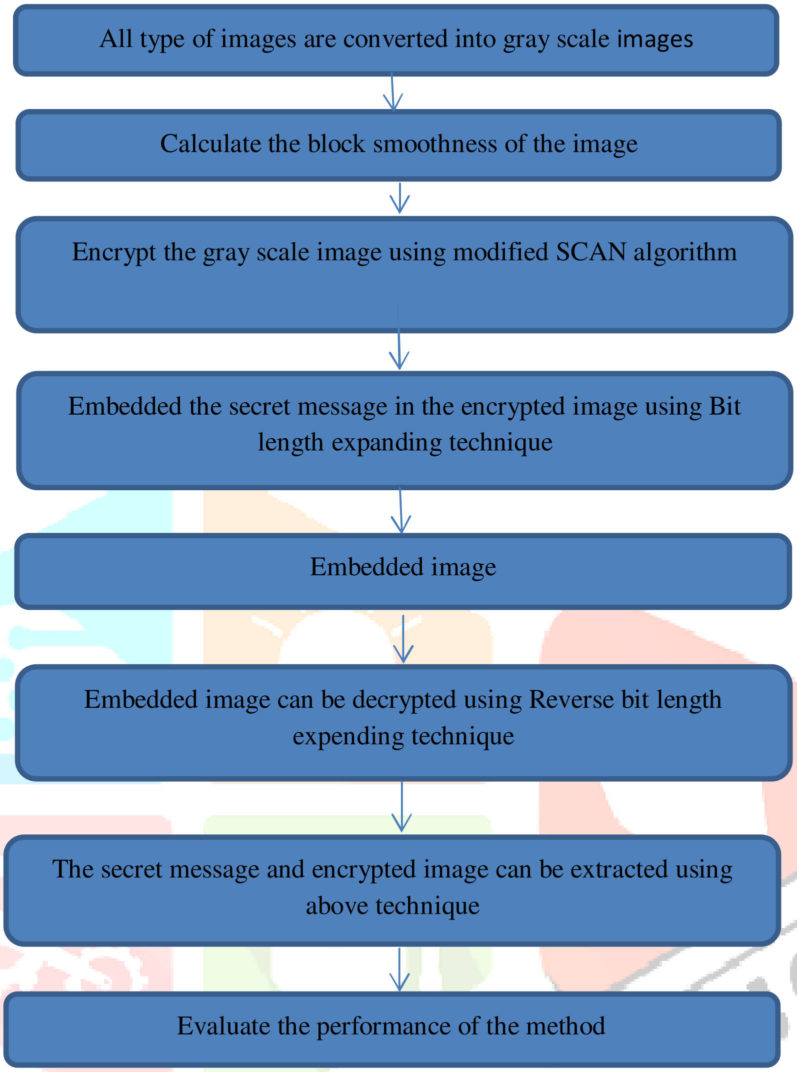
All type of images are converted into gray scale images
Calculate the block smoothness of the image
Encrypt the gray scale image using modified SCAN algorithm
Embedded the secret message in the encrypted image using Bit length expanding technique
Embedded image
Embedded image can be decrypted using Reverse bit length expending technique
The secret message and encrypted image can be extracted using above technique
Evaluate the performance of the method

Fig 3. Modified code methodology

In the altered code approach we utilize the changed SCAN calculation procedure for scramble the picture then after implanted the mystery message into encoded picture utilizing Bit length exhausting strategy. After the inserting of picture we utilize the switch bit length expanding procedure to extricate the mystery message and the scrambled picture then after we assess the execution of the strategy.

III. IMPLEMENTATION

A. Steps used in implementation

The following steps are used in the implementation that are given in the figure

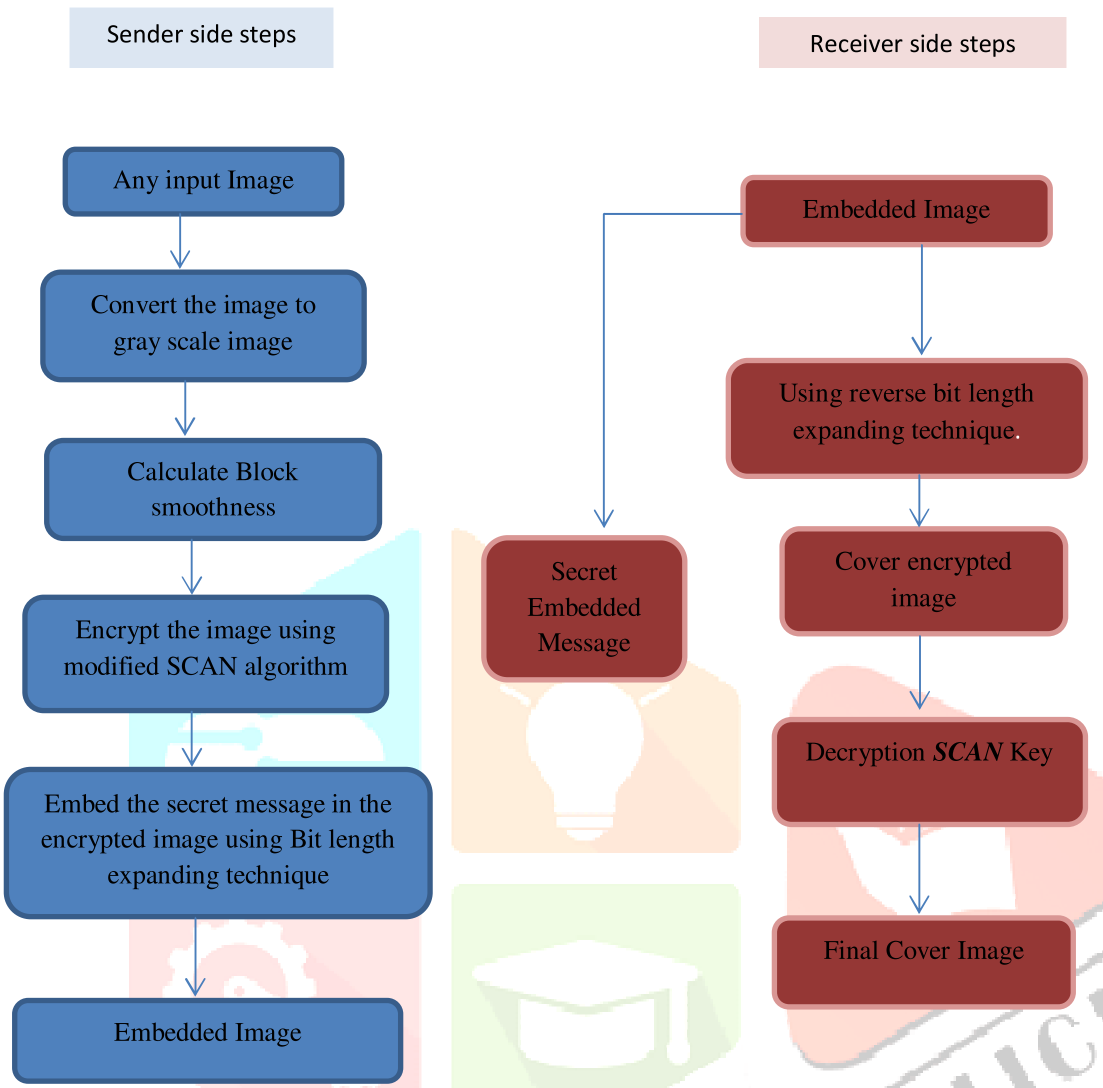
Sender side steps
Receiver side steps
Any input Image
Convert the image to gray scale image
Calculate Block smoothness
Encrypt the image using modified SCAN algorithm
Embed the secret message in the encrypted image using Bit length expanding technique
Embedded Image
Embedded Image
Using reverse bit length expanding technique.
Secret Embedded Message
Cover encrypted image
Decryption SCAN Key
Final Cover Image

Fig 4. Steps for implementation

IV. EXPERIMENTAL RESULTS

For trial result we dealt with the Lena picture and apply the base code and altered code after we saw that there is contrast between blunder rate in base code and changed code. In the altered code mistake rate was not as much as base code.

V.CONCLUSION

In the experimental results we took the lena.jpg image after that we see in the base code the error percentage was 46.18 and peak to signal ratio was 104.46 DB.

While in the modified code the error percent was 17.69 and the peak to signal ratio was 112.79 DB. So after the conclusion we improved the error rate and peak to signal noise ratio

REFERENCES

[1] Wien Hong, Tung-Shou Chen and Han-Yan Wu, "An improved reversible data hiding in encrypted images using side match," IEEE Signal processing letter,vol. 19 no.4,April 2012

[2] Princy Raj and Sreekumar K, "A survey on reversible data hiding in encrypted image," IJCSIT, vol. 5(6), 2014

[3] Dhananjay Yadav, Vipul Singhal, Devesh Kumar Bandil, "Reversible data hiding techniques," IJECSE, ISSN: 2277-1956

[4] T. Margaret 1, PG Student [Embedded System], Dept. of ECE, Sathyabama University, Chennai, Tamil Nadu, India1, "Reversible Data Hiding In Encrypted Images by XOR Ciphering Technique," IJAREEIE vol. 3, Issue2, February 2014

[5] Reza Moradi Rad, Abdolrahman Attar, and Reza Ebrahimi Atani, "A New Fast and Simple Image Encryption Algorithm Using Scan Patterns and XOR," International Journal of Signal Processing, Image Processing and Pattern Recognition, Vol.6, No.5 (2013), pp.275-290

[6] I. Ozturk and I. Sogukpınar, "Analysis and Comparison of Image Encryption Algorithms", Journal of transactions on engineering, computing and technology, vol. 3, (2004), pp. 38.

[7] X. Zhang, "Reversible data hiding in encrypted images," IEEE SignalProcess.Lett., vol. 18, no. 4, pp. 255–258, 2011.

[8] Sabeena O.M, Rosna P.Haroon, "Reversible Data Hiding in Encrypted color images by Reserving Room before Encryption with LSB Method",IJCER, ISSN Vol, 04, Issue, 10, October– 2014

[9]D.Rajshekar Reddy, Dr.V.Santosh Kumar, "Reversible Data Hiding in Encrypted Images by XOR Ciphering Technique", IJATIR,ISSN 2348–2370 Vol.06, Issue.08, October-2014, Pages: 726-729

[10] http://www.heroturko.net/software/soft-win/1517047-mathworks-matlab-r2016a-x64-cygiso.html