Secure Data Hiding In Digital Image Based on Skew Tent Map

Nasreen Mansuri[1], Dr. Amit Srivastava[2]

[1]M.Tech Scholar, [2]Head of Department

Department of Computer Science & Engineering,

Sagar Institute of Research and Technology, Bhopal (M.P.), India

Abstract: Image processing is defined as the process of converting an image into digital format, so that certain operations can be performed on it. With the usage of multimedia is increasing day to day, the visual information which is extracted from high quality digital images plays a very vital role in daily life applications like transferring of images from source to destination etc. Steganography is a science of hiding data into image. We proposed a novel method for embedding of secret data using Skew Tent Map. In this method first of all we convert the data into binary form and then shuffle the message bits using skew tent map and then finaly hide the last two bit of message with the last two LSB of cover image. For recovery of the original image and message data we use Inverse function of skew tent map for inverse of shuffling and extraction of message.A comprehensive set of experiments is carried out to justify proposed method's applicability and evaluate its performance against Peak signal noise ratio (PSNR) and Number of Pixel Change Rate (NPCR) etc. achieve the reason of information hiding with the secret bits of information to replace the random noise, with the lowest plane embedding secret information to avoid noise and attacks, making use of redundancy. The results showed that the proposed algorithm has a good hidden invisibility, good security.

KeyWords: Steganography, Skew Tent Map, PSNR and NPCR etc.

I. INTRODUCTION OF IMAGE PROCESSING

Image processing is defined as the process of converting an image into digital image and performing certain operations on it. There are various operations that are performed, so that enhanced image can be obtained from the original image or we can extract some useful and meaningful information from the original image. The output of the image processing can be an image or characteristics that are associated with the input image. Usually image processing considers images like two dimensional signals, where we apply certain operations on them. With the modern digital technology it is possible to manipulate images (also known as multidimensional signals) with certain systems. These systems range from certain digital circuits to parallel computers [1].

Image stegnography for hide a secret image in the cover image. This approach aims at improving the visual quality of the stego image along with the security of the secret image. This approach still provides high embedded capacity. As it is popular that, Steganography is a technique that allows the one to hide the data within an image while adding some notable changes. In this approach we have explored various steganography methods like image steganography, audio steganography, video steganography and text steganography. All these stenography techniques are used to embed the information in digital carriers. The two most important aspects that should be considered for the image based steganography system are as follows: the quality of stego image and the capacity of the cover image [2].

II. DIFFERENT TYPE OF STEGANOGRAPHY

Different types of cover objects [3] like text, image, audio or video files can be used to hide secret data.

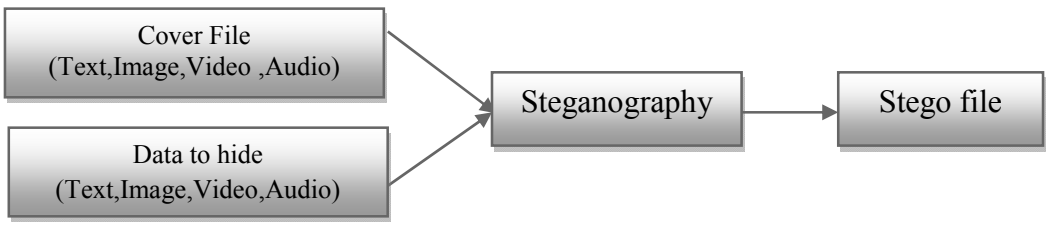

Fig. 1 The Process of Data Hiding

(i) Text Steganography: It is one of the latest and most difficult types of steganography. It is a method of using written natural language to conceal a secret message. Text steganography is most challenging due to the presence of lesser redundancy in text documents as compared to the images and audio files [3].

*(ii) Audio Steganography***:** Audio steganography embeds the message as noise into a cover audio file at a frequency out of human hearing range. Embedding secret messages in digital sound is generally more difficult than embedding messages in other media, compassion to additive random noise is also acute . Commonly used methods for audio Steganography are LSB coding, parity coding, phase coding, spread spectrum, and sound coming back hiding [3].

(iii) Image Steganography: Images are used as the well-liked cover objects for steganography. A message is embed in a digital image through an embed algorithm, using the secret key. The resulting stego image is send to the receiver. On the other face, it is processed by the extraction algorithm using the similar key. During the transmission of stego image unauthenticated persons can only notice the transmission of an image but can't guess the existence of the hidden message [3].

III. LITERATURE REVIEW

In this section we will presents various papers related to stegnography:

"A Review of Methods and Approach for Secure Stenography" [5] has provided a complete review of all the methods and approaches that has been used in making the concept of stenography secure. In this approach, we had survey several different steganographic techniques for encrypting the data.

Steganography is a technique that allows the one to hide the data within an image while adding some notable changes. In this approach we have explored various steganography methods like image steganography, audio steganography, and text steganography. All these stenography techniques are used to embed the information in digital carriers. The two most important aspects that should be considered for the image based steganography system are as follows: the quality of stego image and the capacity of the cover image.

"Art of Hiding: An Introduction to Steganography" [6] has provided the new approach that attempts to identify the requirements that are required for a good stenographic technique. This approach also determines which stenography technique is best suited for which particular applications.

Though there are many different carriers file formats can be used for transferring information from one place to another. But of all these different file formats, digital images are the most popular because of their frequency on the Internet. For hiding secret information in images, there exists a large variety of steganographic techniques some are more complex than others and all of them have respective strong and weak points. For example some techniques have high payload capacity, while on the other hand some techniques do not have high degree of robustness.

"A high quality image hiding scheme based upon Noise Visibility Function and an optimal chaotic based encryption method" [8] has provided a new novel approach for image stenographic for hiding a secret image in the cover image. This approach aims at improving the visual quality of the stego image along with the security of the secret image. This approach still provides high embedded capacity.

The main drawback of this approach is that, though this approach provides high quality of stego image while keeping the high security as well. This approach has capability to adjust the payload of each image pixel. The problem with this approach is that, the overhead computational time taken in this approach is much higher as compared to the previous methods. Because of this higher computational time, the complexity of the way is increased.

"An Efficient Image Encryption and Hiding Method Applied by Double Random Phase Encoding" [9] has provided the new optical ways those posses many advantages like high processing speed, high parallel and high dimension etc. This image encryption and hiding method is being applied by the use of new technique. This technique is known as double random phase encoding technique. The main drawback of this approach is that though this approach provides high processing speed, high parallel and high dimension etc. But still this approach is not widely used because of the fact that this approach does not demonstrate great experiment results. Moreover, this approach is not as effective as earlier approaches.

"An Appearance Based Approach for Gait Identification Using Infrared Imaging" [11] has proposed a new novel approach for gait identification by the using of new imaging system. This imaging system is also known as infrared imaging. This proposed approach is tested over a self created database of thirteen different people with different resolution conditions. The use of infrared cameras at night makes this

approach advantageous over many traditional approaches. Though this approach has many approaches, but still this particular approach has some drawbacks in the fact that this particular approach is being applied on smaller datasets and how this approach will work on large datasets still remains questionable.

"A Secret Sharing Scheme for Secure Transmission of Colour Images" [12] has provided a new approach that is based on secret image sharing and key safeguarding technique. This technique is based on effective and generalized schemes for the hiding of the colour image. This deformation and reformation algorithm reduces the drawbacks of key safe and secret sharing scheme and having its advantages. The proposed scheme is more secure and efficient one because secret image sharing and key safeguarding both are merged so, the security is higher than the single scheme provides either secret sharing or key safeguarding. In this scheme the shares are pre selected and have meaningful information advert to secret sharing scheme shares are distorted one.

IV. PROPOSED METHOD

1. Input 8 bit gray scale Message image P of size of M*N.

$$P = \{p_{ij} \mid 1 \le i \le m \ , 1 \le j \le n \ , p_{ij} \in \{0,1,...,255\}\}$$

Calculate the size of message image and Select the cover image at least 8 times of the size of message image. Let C is the original 8-bit gray-level cover-image of M*N pixels. It is denoted as:

$$C = \{c_{ij} \mid 1 \le i \le M \ , 1 \le j \le N, c_{ij} \in \{0,1,...,255\}\}$$

2. Pixilate both the image and convert to binary form.
3. Generate array T of cover image locations for selected stego key using tent map. Procedure to generate array is given below.

The skew tent map is formulated as

$$F(x) = \begin{cases} x / p, & x \in [0, p] \\ (1-x)/(1-p), & x \in (p, 1] \end{cases}$$

4. Iterate Skew tent map to obtain a pseudo random sequence of size M*N, denoted by $X=\{x_0, x_1, x_2,\ldots,x_{MN-1}\}$.

Sort X in ascendincg order to get $Y=\{y_0,y_1,y_2,\ldots,Y_{MN-1}\}$

According to the relationship of X and Y, a scrambling vector $T=\{t_0,t_1,t_2,\ldots t_{MN-1}\}$ is obtained such that $y_i=x_{ti}$,i=0,1,2,…,MN-1.

5. Replace the LSB's of cover image pixels in the sequence generate in step 4 with message

image bits.

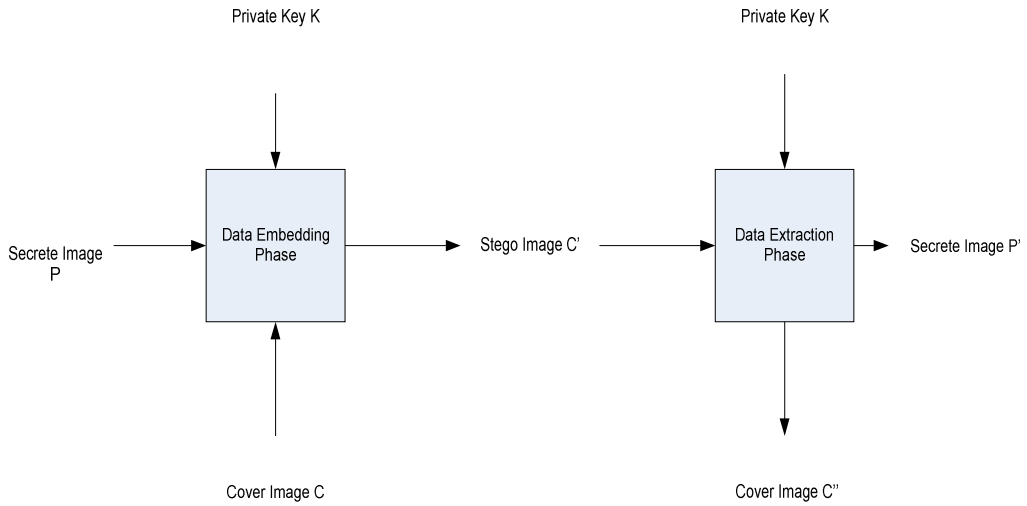

Fig. 2 Block Diagram of Proposed Method

V. CONCLUSION

Skew Tent Map based steganographic method for embedding secret messages into cover images without producing any major changes has been proposed. Purpose enhancement of security and quality is major concern in data hiding and extraction is used for steganograhy which transforms image into binary domain. In our proposed method implementation and the efficient steganography using shuffling and encryption using tent map and random keys. Message hide on encrypted image is embedding in the cover image. So there is a small visual modifying in between cover image and stego image. As a result, the file sizes of the original image and that of the corresponding stego-image will not differ too much. The results showed that the proposed algorithm has a good hidden invisibility, high-class security and robustness for a lot of hidden attacks.

REFERENCES

[1] K.Wawryn, R.Wirski, R.Suszynski, "2D image processing for auto-guiding system", *IEEE 54th International Midwest Symposium on Circuits and Systems (MWSCAS)*, pp. 1 – 4, 2011.

[2] A.A.J Altaay, S.Sahib, M Zamani, "An Introduction to Image Steganography Techniques", International *Conference on Techniques Adavance Computer Science Applications and Technologies (ACSAT)*, pp. 122 – 126, 2012.

[3] Beenish Mehboob, Rashid Aziz Faruqui "A Stegnography Implementation" *International Symposium on Biometrics and Security Technologie ISBAST*, pp. 1 – 5, 2008.

[4] Vladimir Banoci, Gabriel Bugar, Dusan Levicky, "A novel method of image steganography in DWT domain", *IEEE International conference on Radioelektronika*, pp. 1– 4, 2011.

[5] Shaveta Mahajan, Arpinder Singh, "A Review of Methods and Approach for Secure Stegnography", *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol.2, No.10, pp. 67-70, 2012.

[6] Maninder Singh Rana, Bhupender Singh Sangwan, Jitendra Singh Jangir, "Art of Hiding: An Introduction to Steganography", *International Journal Of Engineering And Computer Science,* Vol. 1, No 1, pp. 11-22, 2012.

[7] F.I. Alam, M.M. Islam, "An Investigation into Image Hiding Steganography with Digital Signature Framework", *IEEE International Conference on Informatics, Electronics & Vision (ICIEV),* pp.1 – 6, 2013.

[8] S. Sajasi, A.M. Eftekhari - Moghadam, "A high quality image hiding scheme based upon Noise Visibility Function and an optimal chaotic based encryption method", *IEEE Conference of AI & Robotics and 5th RoboCup Iran Open International Symposium (RIOS),* pp. 1 – 7, 2013.

[9] Xu Hongsheng, Jun lie Xu ,"An Efficient Image Encryption and Hiding Method Applied by Double Random Phase Encoding", *IEEE Fifth International Conference on Computational and Information science (ICCIS)*, pp. 302-305, 2013.

[10] Xu.Xikai Jing Dong , Wei Wang Tieniu Tan, "Video Stegaanalysis Based on the constraints of motion vectors", *IEEE 20th International Conference on Image Processing (ICIP)*, pp. 4422 – 4426, 2013.

[11] A.Kanwar, P.Upadhyay, "An Appearance Based Approach for Gait Identification Using Infrared Imaging", *IEEE International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT),* pp. 719-724, 2014.

[12] H.Kumar, A.Srivastava, "A Secret Sharing Scheme for Secure Transmission of Colour Images", *IEEE International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT)*, pp. 857 – 860,2014.