International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463
Vol. 3 Issue 6, June-2014, pp: (122-127), Impact Factor: 1.252, Available online at: www.erpublications.com

# Enhance Security in Reversible Data Hiding Technique Using Arnold Transform

Sarita Nain[1], Sunil Kumar[2]
[1]M. Tech (ECE), PDMCE, Bhadurgarh, Haryana, India
[2]Asst. Prof., PDMCE, Bhadurgarh, Haryana, India

**Abstract: In rapid development era of communication, internet has made it easy to receive and send information but security is still one of the prime concerns. Various techniques have been implemented in this field of encryption and steganography. In this paper reverse steganography with arnold transform is proposed to hide the secret message in images with encryption and found more secure. Comparison with other technique is also given.**

## 1. INTRODUCTION

Origin of steganographic word is from Greek word which means “Covered Writing”. Five hundred years ago, the Italian mathematician Jerome Cardan reinvented a chinese ancient method of secret writing. The scenario goes as follows: a paper mask with holes among two parties, this mask is placed over a blank paper and the sender writes his secret message through the holes then takes the mask off and fills the blanks so that the message appears as a innocuous text.

Due to the rapid development of multimedia and internet, presently it has become easier for the hackers to edit, modify and duplicate the data. Now a day it necessitates finding appropriate protection because of the sensitivity of information. Steganography deals with the techniques used for protection of information. Steganography in our days performs vital importance since it is a support tool to the copyright protection, which the authentication processes allow the distribution and legal use of different material

It is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message [10]. It is kind of security through obscurity. The steganography is used in applications, which includes confidential communication secret data storing, for providing protection against data alteration. The secret information can be stored in cover files like text, image, audio and video.
For steganographic systems, the major requirement is that the stego object should be perceptually and statistically indistinguishable to the degree that it does not raise suspicion. In other words, the hidden information should impose slight or undetectable modification to the cover objects.

Most of the steganographic techniques hide secret data in images as it is relatively easy to implement [10]. The most important property of the cover source is the amount of data that can be stored in it without changing its properties. Many researches are working in this area and have proposed different techniques with varying capacities and with varying degree of success for hiding the data. Recently the neighboring pixel difference techniques have gained interest among researches. It is a technique [1] in which difference of neighboring pixel is taken of an image and the corresponding histogram is obtained. From the histogram peak points and zero points are calculated for embedding data, as discussed ahead. However, there remain several issues which need to be resolved before an efficient steganography system is developed. Some are:

i) Locating the best position in an image which might result in lower PSNR degradation
ii) How to increase the data hiding capacity?
iii) How to increase the imperceptibility?
iv) How to increase the robustness?
v) Should not be destroyed by image compression
vi) Should be secure
vii) Should ne invariant to image transform like cropping, rotation and scaling
viii) Should be universal i.e., should be under consideration
ix) Should be resilient to common signal processing and geometric distortions and watermarked copies of a document.

In this paper, we have investigated the issues of locating the appropriate location in a given image and have taken up the Adjacent Pixel difference (APD) technique [1] as the baseline algorithm. Three different benchmark images are taken and fixed message size is stored in all of them. The picture quality is measured by means of PSNR using MATLAB platform and compared.

## 2. Proposed work

Many effective reversible data hiding techniques have been proposed. Basically now a day mostly techniques are using APD or by using pixel-difference transformation. Many existing data hiding approaches are not lossless, such as secure spread spectrum [7]. The early reversible data hiding method embeds data in a spatial domain [10].

The NSAS method utilizes the peak point and zero point-pairs of an image histogram and slightly modifies the pixel values to embed data [18]. NSAS hides more data than many reversible data hiding methods. The quality of the stego-image is apparent in that the stego-image has a peak signal-to-noise ratio (PSNR) of at least 48 dB. The Barbara image with a size 512 × 512 and 256 gray-level is used as an example to illustrate the NSAS method. The method includes two processes, i.e., data embedding and data extraction.

This study proposes a novel data hiding technique, Adjacent Pixel Difference (APD), which improves the hiding capacity and the stego-image quality. The method concerns the pixel difference and shifting pixel values. Since APD does not include complicated calculations, the method is easy to implement. But still there is less security in hiding the message for more secret and secure data. For example: data of military usages, matter related to banking or any other important data related to country’s security need z-security. Also capacity of hidden data is to be improved. And to make fulfillment of the requirement now used technique involved Arnold Transform, which greatly enhance the security as well as robustness of the system.

### Arnold Transform Enhance Security

Technology is continuously expanding and as it is there are more and more techniques discovered that attempt to improve already existing works. An interesting field to expand upon is that of encryption. This paper is concerned with an applied mathematical example of using chaos to encrypt grey scale images. There are two major parts of the encryption, namely the Arnold Cat Map and Chen’s chaotic system. The Arnold Cat Map takes concepts from linear algebra and uses them to change the positions of the pixel values of the original image. The result after applying the Arnold Cat Map will be a shuffled image that contains all of the same pixel values of the original image. Chen’s chaotic system will then take the image produced from the Arnold Cat Map and change the actual grey scale values of the pixels, the result will be the final encrypted image.

Mathematically the Arnold Cat Map, (ACM), is represented as the following:
The Arnold Cat Map is a discrete system that stretches and foldsits trajectories in phase space.
Let $X = \begin{smallmatrix} x \\ y \end{smallmatrix}$, where X is a vector, then the ACM transformation is,

$$\Gamma: \begin{matrix} x \\ y \end{matrix} \quad \begin{matrix} 1 & p \\ q & pq+1 \end{matrix} \quad \begin{matrix} x \\ y \end{matrix} \quad \bmod n$$

Some conditions for the map is that p and q are positive integers and

$$\det \begin{matrix} 1 & p \\ q & p+q \end{matrix} = 1 \,,$$

which make the map area preserving.

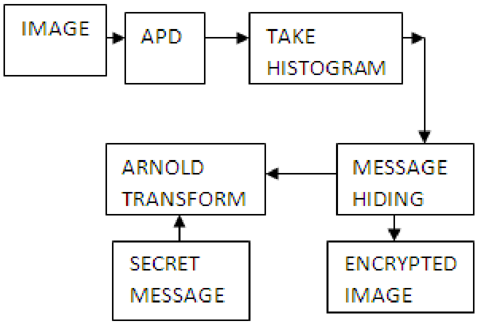


**Fig 1: Block Diagram ON ENCRYPTED SIDE**

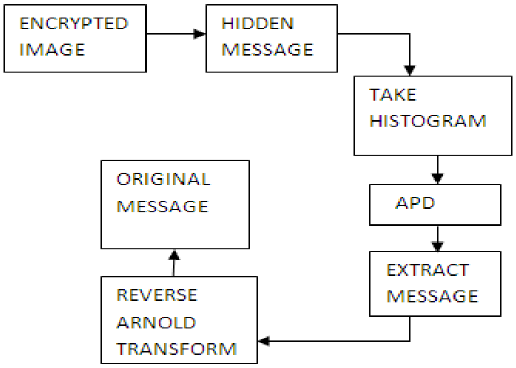


**Fig 2: Block Diagram ON DECRYPTED SID**

**Proposed Algo for Creating Transformation Table:**

1. Select Image to be encryption from data store

2. Insert key of 256 bits

3. Calculate Image Pixels Value Horizontal Value of Pixel = Pixel Width/10 Vertical Value of Pixel = Pixel Height/10

4. Select a Random Function to Calculate Final value for Horizontal and Vertical Pixels Horizontal Pixel□ Select Random Value between Horizontal Value of Pixel and Pixel Width Vertical Pixel□ Select Random Value between Vertical Value of Pixel and Pixel Height.

5. Select a Variable No-Of-Pixel to store Multiple Value of Horizontal Pixel and Vertical Pixel No-Of-Pixel = Horizontal Pixel X Vertical Pixel.

6. Using Hash Function (Here I am using SHA-1) I am generating a Seed Value. This SHA-1 will apply on 256 bits Selected Key Seed = SHA-1(Above Selected KEY)

7. Divide Seed into two Part equally Seed-1 and Seed-2 Seed-1 □ First Half of Seed called “Image Crypto System Seed-2□ Second Half of Seed

8: If Seed-1 is Greater Then Seed-2 Then We Will Select another Variable Seed Value and assign any numeric value between 0 to 4 (Randomly Choose) Otherwise Value of Seed Value Variable vary between 5 to 9 (Randomly choose ).

9: If Variable Seed Value is Equal Between 0 to 4 then calculate new seed value (Here we are working on ASCII value of seed). Seed = Seed + (Seed-1 Mod 2) + 1 Otherwise Seed = Seed + (Seed-2 Mod 2) + 1

10: Repeat Process 8 to 9 till No-Of-Pixel/2

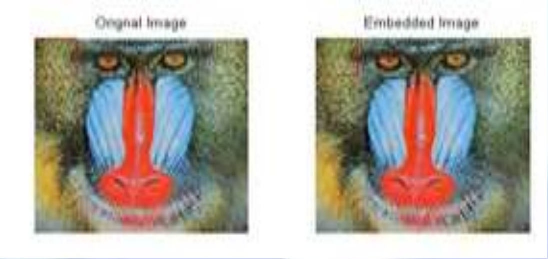
11: Final Output of Step 10 will represent Create transformation Table

## 3. RESULT and CONCLUSION

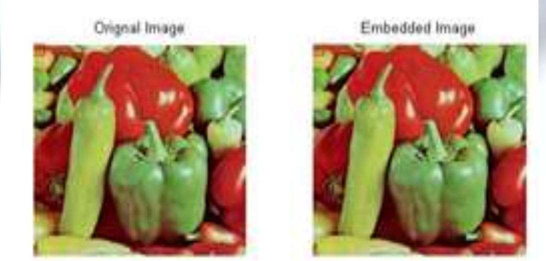
Proposed work is implemented successfully. In this present work, data hiding approach is presented by using Arnold Transform (AT). Present work is about to hide data by using AT. Here AT is performed to enhance security and capacity. Here a Histogram shifting is performed to hide data and after that a key is used to make data more secure. Finally data is hidden with more security and perfection.

The red block shown in the image is just an indication to show that data is hidden at that place. And block is intentionally made visible, but in real it's not present in the image**.**

LENA



LION



VEGETABLE

CAMERA

| Message Image | Capacity | Strength | Block size | PSNR | Message hide | No. of BITS req. to store msg |
|---|---|---|---|---|---|---|
| LENA | 1447 | 2 | 50 | 63.7066 | sarita | 48 |
| LION | 5646 | 3 | 100 | 35.7627 | I like you | 80 |
| VEGETABLE | 290 | 2 | 25 | 57.8837 | delicious | 72 |
| CAMERA | 10741 | 2 | 125 | 57.2309 | beautiful | 72 |

Many different blocks are there in the above table. Here message image indicate the image in which data is to be hidden. Next block is of Capacity which control the level of data hiding capacity without making any distortion in the image. Block size defines no. up to which data is needed to be hide. PSNR stands for peak signal to noise ratio, it define the quality of image. Now here comes message hide block which refers to the message that has been hidden in the image. Last block is for no. of bits that are used to hide the data. As be the no. of alphabet, multiply it with 8 to calculate the no of bits required. As shown in the above table first of all in Lena image, here data hidden is SARITA and number of bits required to store the data are 48(as number of alphabets in sarita are 8, so no. of bits req. = 6*8=48) . As block size in this case is 50 which shows how many pixels are used to hide the data which is given here by capacity of that block that is 1447 bits and strength is 2bits.PSNR is 63.7066.

## 4. FUTURE WORK

In the present work security of system is increased while maintaining the PSNR and image quality of the image in comparisons to base work. Further area of improvisation can be made in capacity and robustness transformation into the frequency domain.

## REFRENCES

[1]. Yu-Chiang Li, Chia-Ming Yeh, Chin-Chen Chang " Data Hiding Based On The Similarity Between Neighboring Pixels With Reversibility" October 24, 2009.
[2]. Yuan-Yu Tsai, Du-Shiau Tsai, Chao-Liang Liu "Revesible Data Hiding Scheme Based On Neighboring Pixel Differences" September 12, 2012.
[3]. Szymon Grabski, Krzysztof Szczypiorski "Steganography in OFDM Symbols of Fast IEEE 802.11 n Networks" 2013.
[4]. Ching-Te Wang, Ching-Lin Wang, Lin-Chun Li and Sheng-You Guo " The Image High Capacity And Reversible Data Hiding Technique Based On Pixel Frequency Of Block" 2011.
[5]. Graeme Bell and Yeuan-KuenLi "A Method For Automatic Identification Of Signatures Of Steganography Software" June 2, 2010.
[6]. Anjali A. Shejul and Prof. U. L Kulkarni " A DWT Based Approach For Steganography Using Biometric" 2012.
[7]. Chin-Fang Li and Huei-Ju Tsai "A Reversible Data Hiding Scheme For Digital Images Using LAU-Side Match Prediction" 2010
[8]. Shiuh-Jeng Wang, Chi-Yao Wang and Dushyant Goyal" Multilevel Data Hiding For Embedding Reversibility Upon Improving Histogram Shifting." 2010.
[9]. Xiao Yi YU, Aiming Wang " Reversible Data Hiding Based On Histogram Shifting" 2009.
[10]. Cancelli, G.; Doerr, G.; Cox, I. J. & Barni, M. (2008). Detection of ±1 LSB steganography based on amplitude of histogram local extrema, Proceeding of International Conference on Image Processing. 2008.
[11]. Peterson, Gabriel, "Arnold's Cat Map". Retrieved October 22, from 2008http://online.redwoods. cc.ca.us/instruct/ darnold/maw / catmap. htm .
[12]. Tzu-Chuen Lu and Chang-Chun Huang "Lossless Information Scheme Based On Pixel Complexity Analysis" 2007.
[13]. Avcibas, I. and Memon, N. and Sankur, B. (2002). Image steganalysis with binary similarity measures, Image Processing. 2002. Proceedings.
[14]. Ross J. Anderson and Fabien A.P. Petitcolas "On The Limits Of Steganography" 1998.

## About Author

The Author have completed her B.TECH. (ECE) from MDU, Rohtak, Haryana and currently pursuing M.TECH. (ECE) from PDMCE, Bhadurgarh, Haryana. Her area of interest is “hiding the secret data in images” that is Steganography.

E-mail: nainsarita2@gmail.com