International Journal of Scientific Research & Engineering Trends
Volume 4, Issue 1, Jan-Feb-2018, ISSN (Online): 2395-566X

Chaotic Function Based Data Hiding Approach at Least Significant Bit Positions

Dilip Kumar Mishra, P.G.Scholar
Dept. of Computer Science and Engineering
Millennium Institute of Technology,
Bhopal, India
dilipmishra907@gmail.com

Sriram Yadav, A.P. & Head
Dept. of Computer Science and Engineering
Millennium Institute of Technology,
Bhopal, India
techmillenniumk.yadav@gmail.com

***Abstract* – With the increase in the digital media transfer and modification of image is very easy. So one major issue of proprietorship is raised, as copying and transferring is very soft practice. Here this paper has resolve proprietorship problem by embedding the digital data with encryption. In this work embedding of data is done by applying the Arnold's Cat Map algorithm for randomization of pixel values. Then robustness is provided by using the AES algorithm. Finally using spatial technique embedding of digital data is done in encrypted image. Embedding in LSB portion of the pixel this research work is robust against various attacks. Experiment is done on real data-set image. Evaluation parameter values shows that this research work has maintain the SNR, PSNR values with high robustness of the data.**

***Keywords* – *Encryption, Embedding, Randomization, SNR, PSNR, LSB*.**

I. INTRODUCTION

As digital world is growing drastically people are moving towards different services provide by it. Some of this service are social network, online market. But this technology gives rise to new problem of piracy or in other words proprietary get easily stolen. In order to overcome these issues many techniques were suggested and proprietary of the digital data is preserved. So to overcome this different techniques are used for preserving the proprietary of the owner.

Out of many approaches digital data embedding which is also known as digital watermarking plays an important role. Here digital information is hidden in the carrier signal which resembles the originality of the data like photographs, digital music, or digital video [1, 2, 4]. One of the basic cause of the copyright issue is the easier availability of the internet and some software that can modify the content as per the user requirement.

In few of approaches inclusion of third party was done by most of the researcher where secret message is hold by one while carrier signal is hold by other [9]. Here embedding is done in fix part of the image where information can be hidden. If fit then embedded otherwise rejected. Now at extraction side image is evaluated under a calculation where it simply accepted or rejected image based on the obtained values. Here work has not taken measures for attacks.

Watermark is broadly divided into two category first is visible watermarking and other is invisible watermarking. In case of visible embedding watermark data is open and can be judge by naked eyes. This is shown in fig. 1. On the other hand invisible watermarking is done in such a way

Fig.1Image having visible watermark.

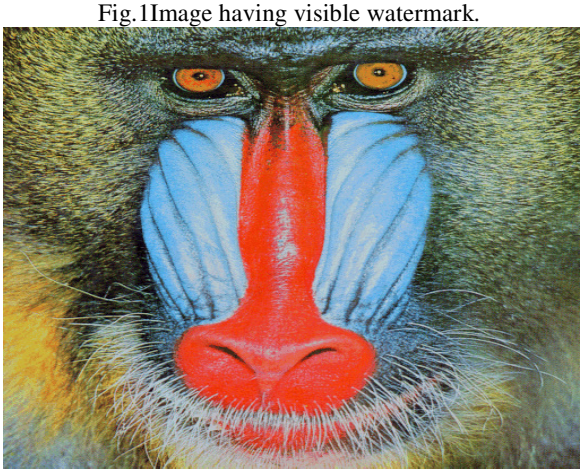
Fig. 2 Image having invisible watermark.

that secret information is not seen or judged, so quality of the carrier signal get affected by this. This is shown in fig. 2, although watermark data is present in the original data. Data may be of any digital information like text file, image, video file, etc.

As privacy of digital data is more in case of invisible data hiding technique so popularity of this technique is quite high. As this reduces the chance of copying the watermark as well from the original signal. Although invisible embedding in carrier image is complex and challenging task but different techniques are working in this field.

II. Related Work

In [4] watermark information is hidden in the edge portion of the image and for finding the exact edge pixels in the image this paper adopt DAM and BCV technique. Whole work is done for the binary image only as the DAM is based on the binary image. So here in this method image has to be in binary form and watermark information is also in binary format. With this limitation it is found that that robustness of the algorithm is quite good against different attacks of noise, filter.

In [5] the extension of the paper [4] is done where hiding is done at the edge region only using same technique of DAM and BCV but here edge selecting region is increased by searching surrounding region of the evaluating pixel. It has been shown in the result that with this new approach robustness increases and the watermark information can be increased in the original image.

In [7] new concept is developed which is termed as content reconstruction using self embedding, here watermark image is embedded in the original image using fountain coding algorithm, where multiple packets are designed for the network. So if some of the packet get corrupted by the attack then rest of the packets are used for regenerating the original watermark. As this method cover different attacks on the image and recover watermark in original condition upto few level of attack. One problem is that after embedding image get transformed in fountain codes packet but embedded image is not available for the user to display and it get reconstruct into original only by decoding the fountain codes. So this algorithm is beneficial for data transferring purpose only.

In [6] instead of embedding the external watermark image, original image is so utilized in the algorithm that it will generate its own watermark bits for the image. This paper focus on the image expansion where spatial domain is used for embedding and supporting information is stored for the image which is required during extraction. Robustness of the image is done against compression attack and scaling is also covered. But to cover both intra-codeblock and inter-codeblock method is utilized.

In [12] during embedding the algorithm uses DWT technique and modulus method for the pixel position selection. At the extraction end embedded image with some supporting information is supplied for generating the original image and watermark bits. This recovery of original watermark is reversible watermarking scheme.

In [8] spatial common technique is used for the watermarking, here image is divided into Red, Green and Blue matrix then whole embedding is done at the blue matrix of the image where some of the LSB's are replaced by the watermark bits while rest of the MSB's remain same. It has been observed that image quality has not affected by the the embedding of watermark. This paper work is robust against compression attack as it most affects the MSB's while LSB's remain unaffected during attack.

III. Proposed Work

This paper focus on the digital image data hiding techniques. Then two steps are explained first is embedding and other is extraction. In case of extraction watermark should be successfully retrieve from the received data without any information loss of the original data as well as watermark [7, 8]. In Fig. 3 whole embedding work block diagram is explained.

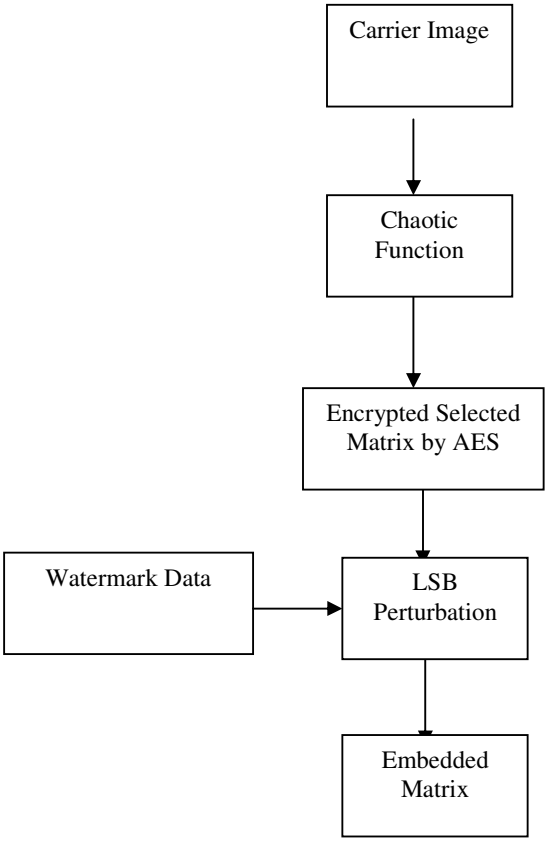

Fig.3 Block diagram of research work.

3.1 Pre-Processing

Here as the image is the collection of pixels where each pixel is representing a number that is reflecting a number over there now for each number depend on the format it has its range such that for the gray scale format it is in the range of 0-255. So reading an image means making a matrix of the same dimension of the image then filling the matrix correspond to the pixel value of the image at the cell in the matrix.

For the first time, "Chaos Concept" was explained by James Yorke and Tien-Yien Li, in 1975. "Secure connections using coordinated chaos would most likely have to be more difficult than simply adding signal to chaos to hide it", these activities represent the first steps for using chaos in data hiding. Chaos systems was designed to make image encryption, aviation, automation etc. [8]. In order to define chaotic signal a deterministic, pseudo periodic conditions are evolved. This can be understand as if the generator produces or start from some different values than it will gives a different signal value. So this makes it different from the other encryption algorithms [7]. Here chaotic map is used in this proposed work for increasing the security of the carrier signal or image from the intruders. Here cyclic chaotic function is used in the work which repeat itself after a few set of rounds or rearrange the square matrix back into its original form. This can be understand by an example where if [p, q] are the pixel value in the image which is needed to be jumbled while after applying the Arnol function F([p, q]) a new position is obtained that is [p' q'].:

$$\begin{bmatrix} p' \\ q' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ \lambda & \lambda+1 \end{bmatrix} * \begin{bmatrix} p' \\ q' \end{bmatrix} \bmod N$$

Where N represents the dimension of the image and λ is an integer value ranges from {1, 2, 3,……..}. This λ affects cycle of the chaotic function [4]. There are many chaotic maps likes: Tent map, Sine map, Logistic map , Cubic map, Arnold's cat map, Barker map, Chen map, Standard map, that each of them has their special properties for specific usage. In this work, an Arnol cat map function is used for the shuffling where λ value is so chosen that determinant of the matrix get one.

3.2 AES

In this encryption algorithm four stages are performed in each round. These steps are common in both encryption as well as decryption algorithm where decryption algorithm is inverse of the encryption one. Now common step for all kind of data is that each data need to be converted into 16 element set of input. Here each input need to be in integer data type. So round consist of following four stages.

- Byte substitution (1 S-box used on every byte)
- Shift rows (permute bytes between groups/columns)
- Mix columns (substitute using matrix multiplication of groups)
- Add round key (XOR state with key material)

3.3 LSB Perturbation

Here as image is combination of numeric value then conversion of that value into its equivalent binary values is done at first level then replacement of those binary value into last four bit of the selected pixel position specified by Gaussian function is done one by one for whole image. Here number of data hiding characters or numbers positions should be less as compared to selected pixel positions.

3.4 Extraction steps

In this extraction steps receiver can extract data and image by using above block diagram. Here Gaussian function will generate same random position at the receiver end when same key is pass. So LSB position of the selected position is read as the original data.

In next module of this step encrypted image obtained is decrypted first by applying reverse AES algorithm. So chaotic matrix is obtained which was developed at sender end. Now remaining cycle of the chaotic function is run to get the original image. It depends on the image dimension and chaotic parameter that how many numbers of iterations are required.

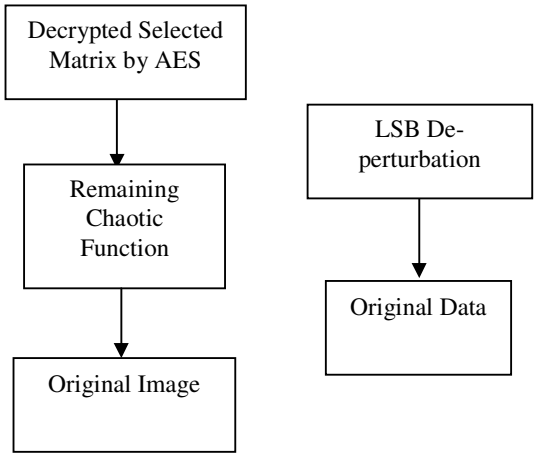

Fig.4 Block diagram of data extraction at receiver end where (a) represent extraction of original image while (b) represent extraction of original data.

IV. Experiment and Results

This section presents the experimental evaluation of the proposed Embedding and Extraction technique for privacy of image. All algorithms and utility measures were

implemented using the MATLAB tool. The tests were performed on an 2.27 GHz Intel Core i3 machine, equipped with 4 GB of RAM, and running under Windows 7 Professional.

4.1 Dataset

Experiment done on the standard images such as mandrilla, lena, tree, etc. These are standard images which are derived from http://sipi.usc.edu/database/?volume=misc. System is tested on day to day images as well.

4.2 Evaluation Parameter

Peak Signal to Noise Ratio

$$\text{PSNR} = 10\log_{10}\left(\frac{Max\_pixel\_value}{Mean\_Square\_error}\right)$$

Signal to Noise Ratio

$$\text{SNR} = 10\log_{10}\left(\frac{Signal}{Noise}\right)$$

Extraction Rate

$$\eta = \frac{n_c}{n_a} \times 100$$

Here n_c is number of pixels which are true.
Here n_a is total number of pixels present in watermark.

4.3 Results

Table 2. PSNR Based Comparison between proposed and previous work.

PSNR Based Comparison		
Images	**Proposed Work**	**Previous Work**
Scene	11.5175	4.8079
Vehicle	8.43389	4.74038
Animal	10.7902	5.19669

From table 2 it is obtained that under ideal condition proposed work is better as compare to previous work in [8]. under PSNR evaluation parameters. As compression algorithm has regenerated images in color format only so this parameter is high as compared to previous value.

Table 3. SNR Based Comparison between proposed and previous work.

SNR Based Comparison		
Images	**Proposed Work**	**Previous Work**
Scene	30.6145	3.50147
Vehicle	32.9504	3.49141
Animal	35.3587	3.58474

From table 3 it is obtained that under ideal condition proposed work is better as compare to previous work in [8]. under SNR evaluation parameters. As compression algorithm has regenerated images in color format only so this parameter is high as compared to previous value.

PSNR based comparison for extraction rate between proposed and previous work has been done and it has been observed that there is no loss of data in the proposed work i.e. hundred percent data obtained in invisible watermarking as in the case of visible watermarking.

So it is obvious that under ideal condition proposed work is better as compared to previous work in [8]. under extraction rate evaluation parameters. As compression algorithm has regenerated images in color format only so this parameter is high as compared to previous value.

Table 4. PSNR Based Comparison between proposed and previous work.

Execution Time Comparison		
Images	**Proposed Work**	**Previous Work**
Scene	24.1494	27.7179
Vehicle	26.3638	28.531
Animal	26.9848	29.6366

From table 4 it is obtained that under ideal condition proposed work is better as compared to previous work in

[8]. under execution time evaluation parameters. As proposed work regenerate dictionary from the same data so execution time for the same is less as compare to previous work.

V. Conclusion & Future Work

Here proposed work has efficiently embedded data in the carrier image while security of the carrier is also maintained by encrypting using AES algorithm. Embedding is done in LSB position of the pixel values. Results shows that the proposed work is producing the results which maintains the image quality as well as robustness. In future, work can be improved for other attacks such as geometry of image.

References

[1]. Tamanna Tabassum, S.M. Mohidul Islam "A Digital Image Watermarking Technique Based On Identical Frame Extraction In 3-Level DWT" Vol. 13, No. 7, Pp. 560 –576, July 2003.

[2]. Frank Hartung, Jonathan K. Su, And Bernd Girod "Spread Spectrum Watermarking: Malicious Attacks And Counterattacks". Of Multimedia Contents" International Journal Of Research In Engineering And Technology Eissn: 2319-1163 | Pissn: 2321-7308, 2005.

[3]. "CHAPTER 2. WAVELET TRANSFORMS ON IMAGES" *Sundoc.Bibliothek.Uni-Halle.De/Diss-Online/02/03H033/T4.Pdf, 2008.*

[4]. Kazuki Yamato, Madoka Hasegawa, Yuichi Tanaka‡ And Shigeo Kato . "Digital Image Watermarking Method Using Between-Class Variance". 978-1-4673-2533-2/12/$26.00 ©2012 IEEE.

[5]. Angela Piper1, Reihaneh Safavi-Naini. "Scalable Fragile Watermarking For Image Authentication". Published In IET Information Security, On 31st December 2012

[6]. Mr Mohan A Chimanna 1,Prof.S.R.Kho "Digital Video Watermarking Techniques For Secure Multimedia Creation And Delivery" Vol. 3, Issue 2, March -April 2015.

[7]. Paweł Korus, Student Member, IEEE, And Andrzej Dziech. "Efficient Method For Content Reconstruction with Self-Embedding". IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 22, NO. 3, MARCH 2013.

[8]. Xiaochun Cao, Ling Du, Xingxing Wei, Dan Meng, And Xiaojie Guo High Capacity Reversible Data Hiding In Encrypted Images By Patch-Level Sparse Representation. IEEE TRANSACTIONS ON CYBERNETICS 2015.

[9]. Hanieh Khalilian, Student Member, IEEE, And Ivan V. Bajic Video "Watermarking With Empirical PCA-Based Decoding" Ieee Transactions On Image Processing, Vol. 22, No. 12, December 2013.

[10]. Shahzad Alam, Vipin Kumar, Waseem A Siddiqui And Musheer Ahmad. 2 "Key Dependent Image Steganography Using Edge Detection". Fourth International Conference On Advanced Computing & Communication Technologies 2014.

[11]. Ioan-Catalin Dragoi, Member, IEEE, And Dinu Coltuc. "Local-Prediction-Based Difference Expansion Reversible Watermarking" . Ieee Transactions On Image Processing, Vol. 23, No. 4, April 2014.