A Robust Arnold's Cat Map Based Spatial Position in Image Digital Data Hiding

Richa Jain[1], Sumeet Dhillon[2], Dr Y.K Jain[3]

[1,2,3]*Department of Computer science & Engineering,Samrat Ashok Technological Institute, Vidisha, Madhya Pradesh (464001), INDIA*

Abstract – As we know the transfer or modification of digital data in todays era is very easy. This is because of different applications or services which are available on the internet. So with this much of easiness there may be some major issues of proprietorship,which are arrived and with the universal reach of the internet, copying and transferring is very soft practice. Here this paper resolves proprietorship problem by embedding the digital data in the encrypted carrier image. In the working methodology, which is followed in this paper of research, the Arnold's Cat Map algorithm for randomization of pixel values is applied to the carrier image before embedding of data for increasing the confusion. After that robustness is provided by using the AES algorithm. Finally, by using spatial technique, embedding of digital data is done in encrypted image. By embedding in the LSB portion of the pixel, the proposed work is robust against various attacks. The Experiment is done on the real dataset image. Evaluation parameter values obtained in the experiment, determine that the proposed work has maintained high values of SNR, PSNR, and extraction rate as compared to previous work.

Keywords: Color Format, Digital Watermarking, Frequency domain, LSB.

I. INTRODUCTION

As digital world is growing drastically and people are moving towards different services provided by it. Some of these services are social networking, online market. But these technologies give rise to the new problem of piracy or in other words proprietary get easily stolen. In order to overcome this issue, many techniques are suggested and proprietor of the digital data is preserved. So to overcome these problems, different techniques are used for preserving the proprietary to 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 causes of the copyright issue is the easier availability of digital data on the internet and some software that can modify the content as per the user requirement. With few of approaches inclusion of third party was done by most of the researcher where secret message is held by one, while carrier signal is held by other [9]. Here embedding is done in fix part of the image where information can be hidden. If it is fitted then embedding is done over it otherwise it rejects. Now at extraction, image is evaluated under a calculation where it simply accepts or rejects image based on the obtained values. Here the procedure has not specified any measures for attacks.

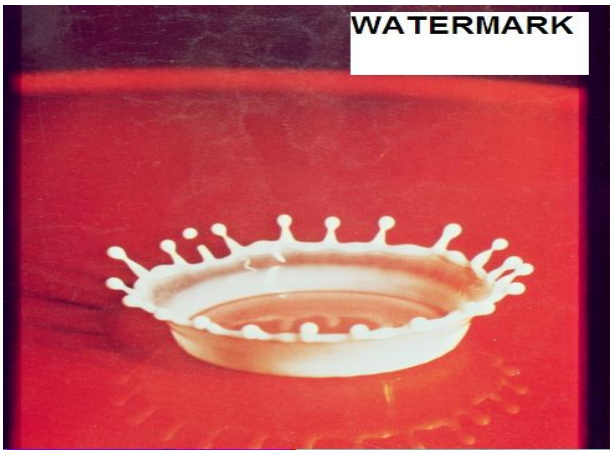


Figure 1: Visible watermark in image data.

Watermark is broadly divided into two categories. First is visible watermarking and other is invisible watermarking. In case of visible, embedding watermark data is open and can be judged by naked eyes. This is shown in fig. 1. On the other hand invisible watermarking is done in such a way that secret information is not seen or judged, so the quality of the carrier signal is affected by this.This is shown in fig. 2, although watermark data are present in the original data. Data may be of any digital information like text file, image, video file, etc.

Figure 2: Visible watermark in image data.

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

II. LITERATURE REVIEW

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 adopts DAM and BCV technique. The Whole work is done for the binary image only as the DAM is based on the binary image. So in [4] image has to be in binary format and watermark information is also in binary format. With this limitation, it is found that the 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 the same technique of DAM and BCV but here edge selecting region is increased by searching surrounding region of the evaluating pixel. It has shown in the result that with this new approach robustness increases and the watermark information can be increase in the original image. In [7] new concept is developed by the paper which is termed as content reconstruction using self embedding, here watermark image is embedded in the original image using a fountain coding algorithm, where multiple packets are designed for the network. So if some of the packets get corrupt by the attack, then the rest of the packets are used for regenerating the original watermark. As this method covers different attacks on the image and recover watermark in original condition up to few levels 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, the 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 in the image which is required during extraction. Robustness of the image are done against compression attack and scaling is also covered. But to cover both intra-coded blocks and inter-code block method utilizes. 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 use for the watermarking, here image is divided into Red, Green and Blue matrix, then whole embedding is done on the blue matrix of the image where some of the LSB's are replaced by the watermark bits while the rest of the MSB's remain same. It has been observed that image quality has not affected by the embedding of watermark. In [8] work is robust against compression attack as it most affects the MSB's while LSB's remain unaffected during the attack.

III. PROPOSED METHODOLOGY

This proposed work focuses on the digital image data hiding techniques. Then two steps are explained first is embedding and other is extracted. In case of extraction watermark should be successfully retrieved 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.

Preprocessing

Here as the image is the collection of pixels where each pixel represents a number. The number which is represented for pixels is actually a value in the range from 0 to 255.Any number in between the range shows the gray scale value of image pixel. So, to read an image, means making a matrix of the same dimension of the image, then fill 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 your signal to chaos to hide it", these activities represent the first steps for using chaos in data hiding. Chaos systems were 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 understood as if the generator produces or start from some different values than it will give 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 repeats itself after a few sets of rounds or rearranges the square matrix back into its original form. This can be understood by an example where if [p, q] are the pixel value in the image which is need to be jumbled while after applying the Arnold's cat map function F([p, q]) a new position is obtained that is [p' q'].

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

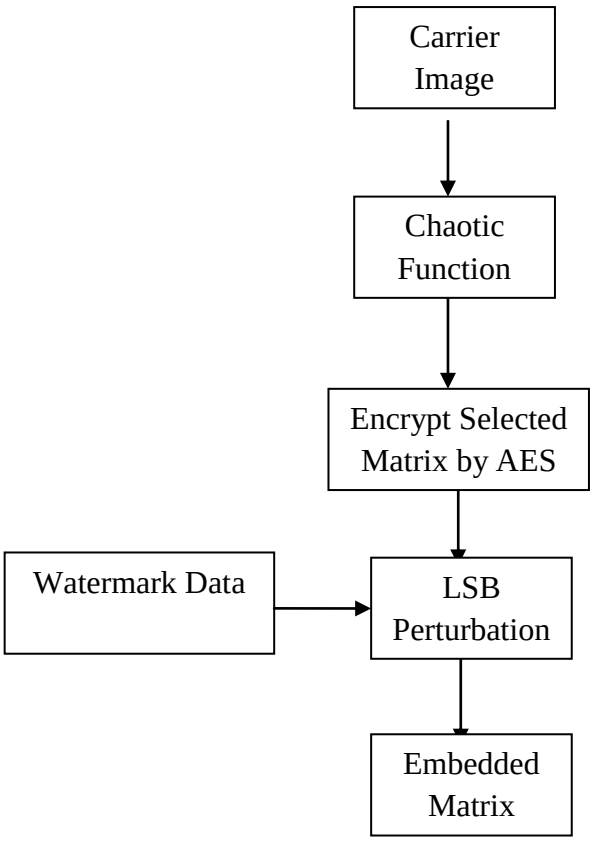


Figure 3. Block diagram of proposed work.

Where N represents the dimension of the image and λ is an integer value range 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, Baker map, Chen map, Standard map, that each of them has their special properties for specific usage. In this work, an Arnold's cat map function is used for the shuffling where the value of λ is chosen such that the determinant of the matrix gets one.

Advanced Encryption Standard (AES):

In this encryption algorithm, four stages are performed in each round. These steps are common in both encryptions as well as in decryption algorithm where decryption algorithm is the inverse of the encryption. Now common step for all types of data is that each data element should be converted into 16 element set of inputs. The input should be in integer data type. The whole methodology consists following four stages.

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

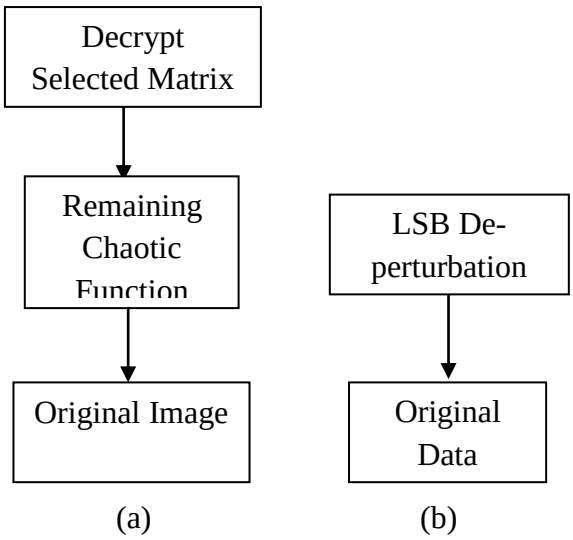


Fig.4 Block diagram of data extraction at receiver end where (a) represent extraction of the original image while (b) represent extraction of original data.

LSB Perturbation

An image is a combination of numeric values. Conversion of these values into equivalent binary values is done at first level, and then replacement of those binary values into last four bits of the selected pixel position specified by LSB is done in one by one manner of whole image. And Number of data hiding characters or number's positions should be less as compare to selected pixel positions.

Extraction steps:

At extraction end receiver can extract data, image or both by using above block diagram's algorithm. In this module encrypted image obtained is decrypted first by applying the reverse AES algorithm. Now chaotic matrix is obtained, which was used at sender end. Now the 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. For data extraction LSB of the selected pixel position is read as the watermark data. As work utilizes last four bits of the pixel value. So collection of all those is done in reverse order as done in embedding module.

IV. Experimental Results

This section presents the experimental evaluation of the proposed embedding and extraction technique for privacy of image. All algorithms and utility measures are implemented using the MATLAB tool. The tests are performed on a 2.27 GHz Intel Core i3 machine, equipped with 4GB of RAM, and running under Windows 7 Professional.

Dataset:

An experiment is performed on the standard images such as Mandrilla, Lena, Tree, etc. These are standard images which are taken from http://sipi.usc.edu/database/?volume=misc. The System is tested on day to day images as well.

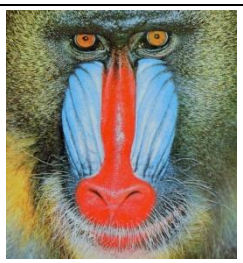
Original Image		
		

Table 1: Dataset Representation.

Evaluation Parameter:

Peak Signal to Noise Ratio:

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

Signal to Noise Ratio:

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

Extraction Rate:

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

Here n_c is the number of pixels which are true.

Here n_a is the total number of pixels present in watermark.

Results:

From table 2 it is observed that under ideal condition proposed work is better than as compared to previous work in [8]. Comparing PSNR evaluation parameters, which shows that compression algorithm has regenerated images in color format only and it gives the parameter value as high as compared to previous values.

From table 3 it is observed that under ideal condition proposed work is better than as compared to previous work in [8]. Comparing SNR evaluation parameters, which shows that compression algorithm has regenerated

Table 2: PSNR based comparison between the proposed and previous work.

PSNR Based Comparison		
Images	**Proposed Work**	**Previous Work**
Mandrilla	9.21456	4.78347
Tree	10.1968	4.94489
Lena	9.21456	4.86716

Table 3: SNR based comparison between the proposed and previous work.

SNR Based Comparison		
Images	**Proposed Work**	**Previous Work**
Mandrilla	33.2255	3.60994
Tree	33.0742	3.45408
Lena	33.2255	3.44045

images in color format only and it gives the parameter value as high as compared to previous values.

Table 4: Extraction rate based comparison between the proposed and previous work.

Extraction Rate Based Comparison		
Images	**Proposed Work**	**Previous Work**
Mandrilla	100	100
Tree	100	100
Lena	100	100

From table 4 it is observed that under ideal condition proposed work is better as compared to previous work in [8]. Comparing extraction rate evaluation parameters, which shows that compression algorithm, has regenerated images in color format only and it gives parameter value as high as compared to previous values.

Table 5: Execution time comparison between the proposed and previous work.

Execution Time Comparison		
Images	**Proposed Work**	**Previous Work**
Mandrilla	21.0847	26.9913
Tree	29.2443	37.7329
Lena	23.7031	26.6131

From table 5 it is observed that under ideal condition proposed work is better than as compared to previous work in [8]. Under execution time evaluation parameters. The proposed work regenerates dictionary from the same

data so the execution time for the same dataset is less, as compared to previous work.

V. CONCLUSION

The use of the Arnold cat map with AES encryption provides a high robustness against various types of intruders. The proposed work has efficiently embedded data in the carrier image, such that the security of the carrier is also maintained. Embedding is done in the LSB position of the pixel values which does not damage the information to the large extent. Proposed work can be used for embedding and extraction of both real and artificial sets of images. Results show that the proposed work maintains the image quality by improving the PSNR evaluation parameters by 99%, while the extraction rate under ideal condition is 100%. Here execution time for embedding and extraction is 19% less as compared to previous approaches. In the future, researchers can apply some other approach to improve robustness against geometrical attacks.

REFERENCES

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

[2] Hartung F., Jonathan K. Su. (2005), "Spread Spectrum Watermarking: Malicious Attacks And Counterattacks" (2005).

[3] "CHAPTER2. WAVELET TRANSFORMS ON IMAGES"Sundoc.Bibliothek.Unillle.De/Dissnline/02/03H033/T4.Pdf, 2008.

[4] Yamato K., Hasegawa M., Tanaka Y. (2012), "Digital Image Watermarking Method Using Between-Class Variance", 978-1-4673-2533.

[5] Piper1 A,. Safavi-Naini R., "Scalable Fragile Watermarking For Image Authentication", Published In IET Information Security, (2012).

[6] Chimanna M., Kho S.R., "Digital Video Watermarking Techniques For Secure Multimedia Creation And Delivery", Vol. 3, (2013) Issue 2, Pp.839-844839.

[7] Korus P., Dziech A. "Efficient Method For Content Reconstruction With Self-Embedding", Ieee Transactions On Image Processing, (2013) Vol. 22, No. 3.

[8] Vargas L.M., Verae., "An Implementation Of Reversible Watermarking For Still Images", IEEE Latin America Transactions, (2013) Vol. 11, No. 1.

[9] Khalilian H., "Watermarking With Empirical PCA-Based Decoding" , Ieee Transactions On Image Processing, Vol. 22, (2013) No. 12.

[10] Alam S., Kumar V., Siddiqui W., "Key Dependent Image Steganography Using Edge Detection", Fourth International Conference On Advanced Computing & Communication Technologies, (2014).

[11] Dragoi I., "Local-Prediction-Based Difference Expansion Reversible Watermarking", Ieee Transactions On Image Processing, Vol. 23, (2014) No. 4.