ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

A LL Chaotic Approach to Non-Blind Image Watermarking

Achintya Singhal, Kamred Udham Singh

Assistant Professor, Dept. of Computer Science, Banaras Hindu University, Varanasi, U.P., India

Research Scholar, DST-CIMS, Banaras Hindu University, Varanasi, U.P., India

ABSTRACT: In this paper a LL Chaos Based Non-Blind Image Watermarking technique is proposed. The scheme is based on watermarking in the transform domain along with Logistic and Lorentz chaotic maps for estimating the embedding strength and location. Test results reveal that the watermarked image generated with the proposed algorithm bears invisible watermark and the watermarking scheme is robust against colouring, cropping etc.

KEYWORDS: LL Chaos, non-blind watermarking, transform domain, image.

I. INTRODUCTION

Digital Watermarking is a descendent of a technique known as steganography, which has been in existence for a few hundred years. In the digital watermark, a pattern of bits are inserted into a multimedia file that signifies the file's copyright data. The objective of digital watermarks is to provide copyright protection for intellectual property that's in digital format by inserting invisible/ visible watermarks in images, audios and videos etc.[4].

Normally two types of watermarking schemes are used Blind scheme and Non-Blind scheme. Blind watermarking scheme is a scheme in which watermark can be detected and extracted without using original object. But in Non-Blind scheme original object (host object) must be required for detecting and extracting watermark. Therefore, blind techniques are comparatively less robust than non-blind techniques and thus for manageable data non-blind techniques are preferred. Watermark recovery is usually more robust if the original, object data are available.

II. REVIEW OF RELATED RESEARCH

A number of earlier works related to copyright protection of digital images that employs digital image watermarking available in the literature inspired us to do this research. Some of such recent researches are briefly described in this section.

Zhao et al [2004] [1] presented a chaotic watermarking algorithm using logistic map. The watermarking was done in wavelet domain. The image is divided in non overlapping blocks and some of them are selected to create a sub image. The blocks selection is done with chaotic logistic map and these blocks are then transformed in the DWT domain where a watermark sequence created using logistic map, is embedded.

Yeh and Lee in [2005] [2], proposed a spatial domain block-based fragile watermarking technique. An authentication signature, along with a relation signature, intended for recovery purposes, is embedded in the two least significant bits of each pixel, for every block. A block relations is created using total. Resulting recovery and authentication data to spread across to other blocks using a spreading function developed using chaotic map.

Wu and Shih[2007] [3] proposed a transformed domain watermarking scheme with high watermarking capacity using a chaotic map and a reference register. The algorithm exploited the characteristics of local spatial similarity and generated more significant coefficients.

S. Mabtoul, E. Ibn-Elhaj, D. Aboutajdine[2006] [6] proposed digital image watermarking in the Complex Wavelet Domain. Initially the watermark, used as copyright sign, is preprocessed with a random location matrix. They applied the DT-CWT transform locally, i.e. on a sub-image, which was extracted from the original image, in the complex wavelet domain. Then, according to the sub-image data, the preprocessed watermark image is adaptively spread and added into the host sub-image DT-CWT coefficients.

E. Chrysochos, V. Fotopoulos, and A. N. Skodras[2008] [7] proposed a frequency domain blind algorithm for digital image based on a chaotic function. The algorithm used a correlation method for detection. The proposed scheme exhibit satisfactory robustness against a wide variety of attacks such as filtering, noise addition, geometric manipulations and JPEG compression with very low quality factors.

Zhao Yantao, Ma Yunfei, Li Zhiquan[2008] [5] proposed a blind chaotic watermarking scheme in DCT domain for digital images. The watermark was scrambled using chaos map with keys. The scrambled watermark is then embedded into the least signification bits (LSB) of the quantized DCT coefficients. Experimental results showed that the scheme has high fidelity and is highly robust against geometric attacks and signal processing operations.

Shang-Lin Hsieh et al. [9] had proposed a secret sharing and wavelet transform based copyright protection scheme for color images. The share image generation phase and the watermark retrieval phase were the two different phases presented. In the generation phase, the image was converted into the YCbCr colour space and then created a special sampling plane using it. Then using discrete wavelet transform the features from the sampling plane were extracted. The scheme then generated a principal share image by employing the features and the watermark.

III. CHAOS AND ITS APPLICATION TO WATERMARKING

Chaos is an inherent random behaviour expressed by defined system and is quasi random movement that seemingly is irregular. Due to very large period and excellent randomicity of chaos signal, chaos system can generate large number of random like high security keys, but it is certain. The most attractive features of chaos in information hiding are its extreme sensitivity to initial conditions. The sensitivity to initial conditions mean that two nearby trajectories starting from very close initial states diverge exponentially when time goes to infinity. As a result of this sensitivity, which manifests itself as an exponential growth of perturbations in the initial conditions, the behavior of chaotic systems appears to be random. Such complex and unpredictable signals can be easily generated by simple dynamic systems like logistic map. A large number of uncorrelated, random-like, yet deterministic chaotic signals can be generated with small perturbation of parameters. Keeping the chaotic parameters and initial condition as the secret key, the chaotic signal can be reproduced easily [5].

A. *Logistic map:*

The logistic map is a polynomial mapping(equivalently, recurrence relation) of degree 2, chaotic behaviour can arise from very simple non-linear dynamical equations. The map was popularized in a seminal 1976 paper by the biologist Robert May, in part as a discrete-time demographic model analogous to the logistic equation first created by Pierre François Verhulst [12].

Logistic map is one of the simplest chaotic maps, which is determined by equation

$$x_{k+1} = \mu x_k (1 - x_k)$$

Where $0 \le \mu \le 4$, $0 < x_{k+1} < 1$ .When $3.5699456 \le \mu \le 4$,the map is in the chaotic states, and the sequence produced by logistic map is random and sensitive to original value. Moreover all the orbits of the logistic map are dense in the range of the map [0, 1].

B. *Lorenz map:*

Lorenz describes atmosphere movement mode using follow equation group, solution of the equation group is not stable and discrete at well, but is attracted around a region and enter a chaos state.

DOI: 10.15680/IJIRCCE.2015. 0309023

$$\begin{cases} \dfrac{dx}{dt} = a(y-x) \\ \dfrac{dy}{dt} = x(b-z) - y \, \dfrac{dy}{dt} = x(b-z) - y \\ \dfrac{dz}{dt} = xy - cz \end{cases}$$

When a=10, c=8/3, as long as b is more than 24.74, the solution of Lorenz equation is chaos system. And initial parameters and initial valves of system variable can be as secret keys. Lorenz equation is three dimension chaos system, this system structure is quite complicated, and it has multi system variables and multi system parameters. The time sequence of this system is more irregular and cannot be forecasted. Using Lorenz equation, chaos system construct sequence cryptogram [11].

(1) It can deal with multi system variables and produce sequence cryptogram. Initial chaos float sequence that can produce sequence cryptogram can be a sequence value of a chaos variable, and it also can be a function value of multi variables. The design of this sequence cryptogram is more flexible, and has larger space. So this design method provides a solution to improve short period effect that is caused by finite precision, and improve security as well.

(2) It can provide a large number of secret key spaces. Lorenz equation has more system variables and system parameters. If adding variable in design process, the secret key space of algorithm is larger than sequence secret cryptogram constructed by low dimension chaos equation.

IV. DCT WATERMARKING TECHNIQUE

Discrete Cosine Transformation has been the most popular transform domain for various image processing. It allows an image to be broken up into different frequency bands viz. high frequency, middle frequency and low frequency, making it much easier to embed watermarking information in the desired frequency band. In general middle frequency bands are preferred over especially for watermarking The middle frequency bands are chosen such that they avoid the most visual important parts of the image (low frequencies) without over-exposing themselves to removal through compression and noise attacks (high frequencies). Embedding in the perceptually significant portion of the image has its own advantages because most compression schemes remove the perceptually insignificant portion of the image. In spatial domain it represents the LSB however in the frequency domain it represents the high frequency components[8].

For DCT with block size (M xN), the connection between the spatial domain image pixels X (i, j) and the transform domain coefficients Y (u, v) is

$$Y(u,v) = \frac{2c(u)c(v)}{\sqrt{MN}} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} X(i,j) cos\left[\frac{(2i+1)u\pi}{2M}\right] cos\left[\frac{(2j+1)v\pi}{2N}\right]$$

where u = 0, 1,……..M -1; v = 0, 1, N - 1, and

$$c(k) = \begin{cases} \frac{1}{\sqrt{2}}, & ifk = 0; \\ 1, & otherwise \end{cases}$$

DCT based watermarking techniques are more robust compared to simple spatial domain watermarking techniques. Such algorithms are robust against simple image processing operations like low pass filtering, brightness and contrast adjustment, blurring etc. However, they are difficult to implement and are computationally more expensive.

V. DCT WATERMARKING TECHNIQUE

We propose a watermarking algorithm, based on Discrete Cosine Transformation along with chaos for estimating embedding and strength factors. This increases the robustness against statistical attacks. This is a non-blind technique and the original image is used to find out the watermark logo.

A. *Insertion algorithm*

Step 1	Decompose the host and logo image into YCBR color space.
Step 2	Partition each component of the host image and logo images into non overlapping blocks, and perform Discrete Cosine Transformation for each blocks of host image and logo.
Step 3	Generate the pseudo image using Logistic map for every components of host image
Step 4	Find the embedding locations chaotically using Lorenz Map
Step 5	Add watermark into different component locations, as is identified in step 4,as per the scheme below. $C' = C + \alpha *W* L$ Where C’ → Watermarked image. C → Host image. α → Strength. W → Pseudo image . L → Logo.
Step 6	Perform inverse Discrete Cosine Transformation of every component of the final watermarked image.
Step 7	Concatenate all the components and converts it from YCBR color space to RGB color values to get the watermarked image.

B. *Extraction algorithm*

Step 1	Decompose the host and watermarked image into YCBR color space.
Step 2	Partition each component of the host image and watermarked images into non overlapping blocks, and perform Discrete Cosine Transformation for each blocks of host image and logo.
Step 3	Generate the pseudo image using Logistic map for every components of host image
Step 4	Find the locations chaotically where embedding was done using Lorenz map.
Step 5	Extract the logo from watermarked image using original image by below equation. $L = (C - C') / \alpha*W$ Where C’ → Watermarked image. C → Host image. α → Strength. W → Pseudo image . L → Logo.
Step 6	Perform inverse Discrete Cosine Transformation to every components of extracted component.
Step 7	Concatenate all the components and convert it from YCBR color space to RGB color value to get logo image.

VI. RESULTS AND DISCUSSION

Based on the above algorithm, the image was subjected to watermarking. Then different attacks were performed on the watermarked image and results were generated. Fig. 1 is the original image, fig. 2 is the watermark used, fig. 3 is the watermarked image and fig. 4 is the extracted watermark.

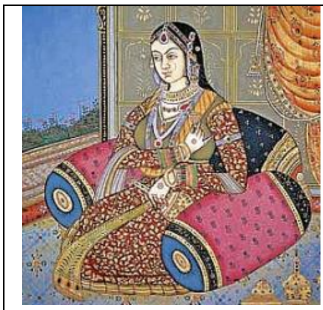
Fig. 1. Original Image

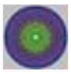
Fig. 2. Watermark Image

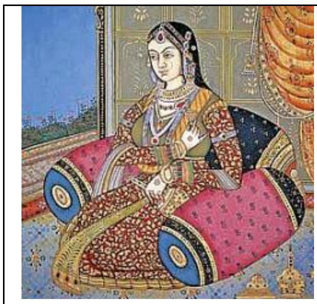
Fig. 3. Watermarked Image

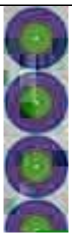
Fig. 4. Extracted Watermark

The watermarked image (fig. 3.) was then subjected to various attacks and then the watermark was recovered. Fig. 5 depicts the watermarked image subjected to auto colouring attack. Auto color adjusts the contrast and color of an image by searching the image to identify shadows, midtones and highlights. By default, Auto Color neutralizes the midtones and clips the shadows and highlight pixels by 0.5%. Fig. 6 depicts the extracted watermark post auto colouring attack. Fig. 7 is a cropped watermarked image and the fig. 8 is the extracted watermark from the cropped image.

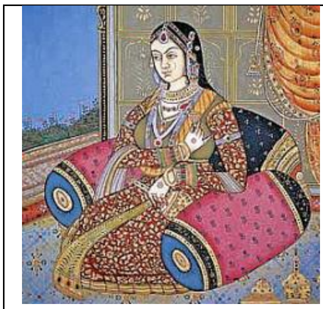
Fig. 5. Auto Colour Attack

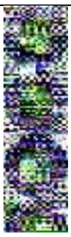
Fig. 6. Extracted watermark

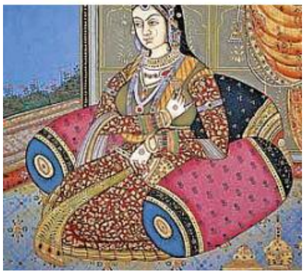
Fig. 7. Cropping Attack

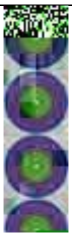
Fig. 8. Extracted watermark

In fig. 9 the watermarked image is subjected to cutting in between, the fig. 10 depicts the extracted watermark from it. In fig. 11 and fig. 13 the watermarked image is subject to increase and decrease of brightness respectively, the fig. 12 and fig. 14 depicts the extracted watermarks from these attacks respectively. In fig. 15 and fig. 17 the watermarked image is subject to increase and decrease of contrast respectively, the fig. 16 and fig. 18 depicts the extracted watermarks from these attacks respectively. The fig. 19 depicts the combined attack of variation of brightness and contrast on the watermarked image, the fig. 20 depicts the extracted watermark from it.

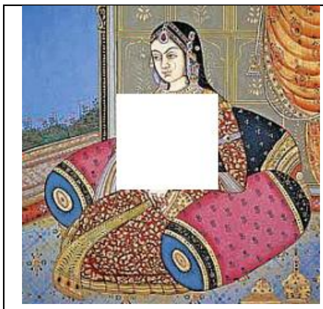
Fig. 9. Image Cutting Attack

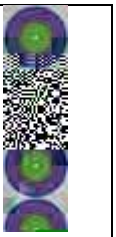
Fig. 10. Extracted watermark

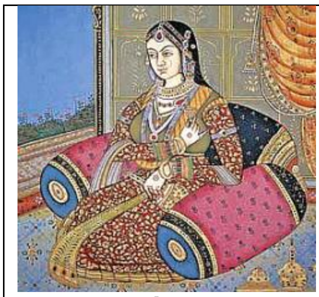
Fig. 11. Brightness Increase Attack

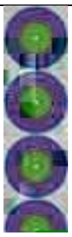
Fig. 12. Extracted watermark

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

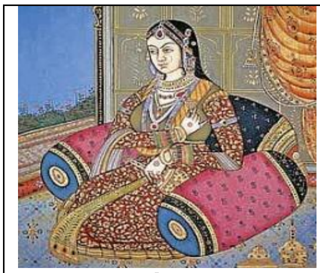

Fig. 13. Brightness Decrease Attack

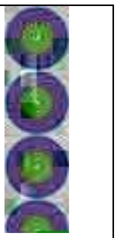

Fig. 14. Extracted watermark

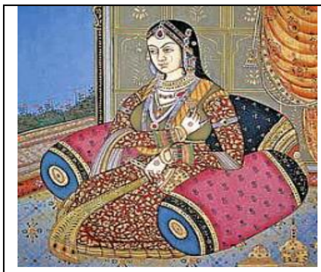

Fig. 15. Contrast Increase Attack

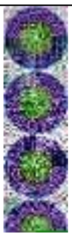

Fig. 16. Extracted watermark

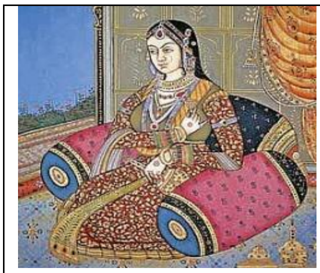

Fig. 17. Contrast Decrease Attack

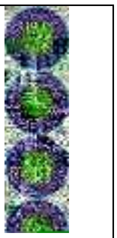

Fig. 18. Extracted watermark

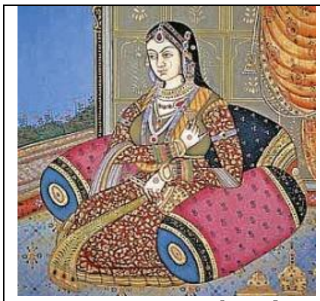

Fig. 19. Combined Varying Contrast and Brightness Attack

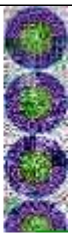

Fig. 20. Extracted watermark

VII. RESULTS AND DISCUSSION

In this project an image watermarking algorithm based on two chaotic maps Logistics map and Lorenz map and a powerful mathematical transform DCT, has been proposed. The watermark values are not embedded directly; it is embedded on chaotic locations and with chaotic strength factor. This algorithm is highly robust as it leaves unauthorized users guessing about the locations where actual embedding has been done. The experimental results show that proposed watermarking algorithm has a good sustainability and has a good robustness against the many attacks.

REFERENCES

1. Zhao, D., Guanrong, C., and Wenbo, L., " A chaos-based robust wavelet-domain watermarking algorithm", Chaos, solitions & fractals, vol. 22, Issue 1, pp. 47-54, 2004.
2. Yeh, G. H., and Lee, G.C., "Toral fragile watermarking for localizing and recovering tampered image", IEEE Symposium on Intelligent Signal Processing and Communication System, Hong Kong, pp.321-324, Dec 2005.
3. Wu, Y. T., and Shih, F.Y., "Digital watermarking based on chaotic map and reference register", Pattern Recognition, vol.40, no. 12, pp.3753-3763, Dec 2007.
4. Berghel, H., and O'Gorman, L., "Protecting ownership rights through digital watermarking", IEEE Computer Mag, pp.101-103, July 1996.
5. Zhao, Y., Yunfei, M., and Zhiquan, L., "A robust chaos-based DCT-domain watermarking algorithm", International Conference on Computer Science and Software Engineering, vol. 3, pp.935-938, 2008.
6. Mabtoul, S., Ibn-Elhaj, E., and Aboutajdine1, D., "A blind chaos-based complex wavelet-domain image watermarking technique", in International Journal of Computer Science and Network Security, vol. 6, no.3, pp. 134-139, March 2006.
7. Chrysochos, E., Fotopoulos, V., and Skodras, A. N., "Robust watermarking of digital images based on chaotic mapping and DCT", 16th European Signal Processing Conference (EUSIPCO 2008), Lausanne, Switzerland, pp. 1-5, August 25-29, 2008.
8. Potdar, V. M., Han, S., and Chang, E., "A survey of digital image watermarking techniques", 3rd International Conference on Industrial Informatics (INDIN 2005) IEEE, pp.709-716, 2005.
9. Hsieh, S. L., Hsu, L. Y., and Tsai, I. J., "A Copyright Protection Scheme for Color Images using Secret Sharing and Wavelet Transform", in proceedings of World Academy of Science, Engineering and Technology, vol. 10, pp. 17-23, December 2005.
10. Fei, Y., Luo, J., and Wu, S., "Color Image Watermark Algorithm Based On Lorenz Chaos Encrypting", International Conference on Signal Processing, vol. 2, 2006.
11. Mooney, A., and Keating, J. G., "Generation and Detection of Watermarks Derived from Chaotic Functions,. Proceedings of Opto-Ireland, SPIE, pages 12, 2005.