



Color Image Watermarking Based on LU Factorization, Logistic and Lorentz Chaotic Maps

Kamred Udham Singh
DST-CIMS,

Banaras Hindu University (BHU), Varanasi, UP, India

Achintya Singhal

Department of Computer Science

Banaras Hindu University (BHU), Varanasi, UP, India

Abstract: Color image watermark has more bit information than gray-scale or binary watermark so it is a challenging issue to design a robust color watermarking scheme for content authentication. In watermarking schemes, the Discrete Cosine Transformation (DCT) is broadly used because its frequency component separation is very useful. Furthermore, LU Factorization has little influence on the visual quality of the image watermark. In this paper a LL Chaos and LU Factorization based Non-Blind Image Watermarking technique is proposed. This watermarking scheme is based on Discrete Cosine Transformation along with Logistic and Lorentz chaotic maps with LU Factorization for estimating the embedding strength and location. The experimental results reveal that this watermarking algorithm is robust against different image processing attacks to a certain degree viz. contrast adjustment, cropping and colouring.

Keywords: LL Chaos, non-blind watermarking, DCT, LU Factorization.

1. INTRODUCTION

Last several years, speedy evolution and popularization of information technology, computer networks and the tremendous usage of the internet have made duplication and unauthorised distribution of multimedia contents viz. video, audio and images much easier. Information infringement and unauthorized tampering is the major issues of digital content on a network from a copyright and security view point, protection of the digital data has become an important and challenging task, to address these issues watermarking technology is getting more and more attention and come in existence [1 - 3]. Digital Watermarking is a descendent of a technique known as steganography, which has been in existence for a several centuries. In the digital image watermarking, a pattern of bits are embedded into a multimedia object, which proves the ownership of the object. The main objective of digital watermarking is to provide copyright protection for intellectual property that is in digital format [4]. However, it is the main concern of the image watermarking technique that the embedded watermark must not degrade the quality of the host image and the watermark must be invisible as much possible, property of visibility of watermark is called imperceptibility and efficiency with which we are embedding the watermark into host image is called robustness.

Image watermarking techniques are further classified into two categories on the basis of domain in which the watermark is inserted into the host image, first is spatial domain techniques and second is frequency domain techniques. Spatial domain watermarking techniques watermark is directly inserted into the host image by modifying the pixel values [5]. Least significant bit is the simplest technique of the spatial domain in which Least significant bit of the host image is modify with the watermark bit [3]. Spatial domain technique are easy to implement with low complexity but not robust against the various image processing attacks. Whereas frequency domain techniques first transform the host image representation of spatial domain to the frequency domain

and then embedded the watermark by modifying its frequency coefficients. Various transformations viz. discrete cosine transforms (DCT), discrete wavelet transforms (DWT), and discrete Fourier transforms (DFT) are used in image watermarking [6-10]. Transform domain watermarking techniques are more robust against various image processing attacks in comparison to the spatial domain watermarking techniques but generally it have higher computational complexity. Other classification of watermarking techniques are Blind technique and Non-Blind technique. Blind watermarking techniques are those techniques in which watermark extraction is done without using original host image. However, in Non-Blind technique original host image must be required for watermark extraction. Consequently, blind techniques are comparatively less robust than non-blind techniques and thus for manageable data non-blind techniques are preferred for watermarking. Watermark recovery is usually more robust if the original host image are available.

2. REVIEW OF RELATED RESEARCH

Various types of watermarking techniques have been previously reported for images to provide robust and effective watermarking including authenticity, imperceptibility and integrity. Some of such recent researches are briefly described in this section.

Zhao et al. proposed a chaotic watermarking technique based on DWT and logistic map and done it in wavelet domain. In this technique, author divide the image in non-overlapping blocks and select some of them for create a sub image. The selection of blocks is done with chaotic logistic map and then these blocks are then transformed in the DWT domain where a watermark is created using logistic map and embedded it into the host image [11].

Yeh and Lee proposed a spatial domain block-based fragile watermarking technique. An authentication signature, along with a relation signature, intended for recovery purposes. In this technique author embedded a watermark in host image using least significant technique bit algorithms where two

least significant bits of each pixel are replaced with the watermark's bits. Resulting the watermark's bit is spread across to other blocks using a spreading function that is based on chaotic map. Fragile watermarking techniques are not robust against the image processing attacks [12].

Wu and Shih proposed a watermarking technique based on chaotic map and reference register and this technique exploited the characteristics of local spatial similarity and generated coefficients that are more significant. This watermarking technique is robust and works well under some image-processing attacks, *viz.* JPEG compression, low-pass filter and Gaussian noise [13].

S. Mabtoul et al. proposed a blind digital image watermarking technique based on Dual Tree Complex Wavelet Transform and chaotic logistic map. First, a watermark image as copyright sign is pre-processed with a random location matrix. Author apply the Dual Tree Complex Wavelet Transform locally on the host image for sub image. Then, according to the sub-image data, the preprocessed watermark image is adaptively spread and added into the host sub-image DT-CWT coefficients [14].

E. Chrysochos et al. proposed a blind image watermarking technique based on DCT, correlation method and a chaotic function. The proposed technique used a correlation method for detection. Author tests the robustness against various image processing attacks *viz.* noise addition, geometric manipulations, filtering, and JPEG compression and found the satisfactory results [15].

Zhao et al. proposed a blind watermarking technique based on DCT and chaotic map. Pixels of image watermark was scrambled using chaos map with secret keys. After scrambling process, these bits are embedded into the least significant bits (LSB) of the quantized DCT coefficients. Author test the robustness of the technique against geometric attacks and signal processing operations and found the good result [16].

Shang-Lin Hsieh et al. proposed watermarking technique for color image based on secret sharing and DWT wavelet transform. The technique contains two phases first is share image generation phase and second is watermark retrieval phase. In the generation phase, the image is convert into the YCbCr color space and then created a special sampling plane using it. Now the features from the sampling plane image are extracted using the discrete wavelet transform. The scheme then generated a principal share image by employing the features and the watermark. Proposed watermarking scheme resist several image processing attacks *viz.* blurring, cropping and sharpening, scaling and JPEG compression [17].

Dongyan Wang et al. proposed a non-blind watermarking technique for color image based on LU decomposition, Arnold Transform and DWT wavelet transform. Author first apply the DWT on the host image after that apply the LU

decomposition on HL and LH band because author select these bands for watermark insertion. Now, Arnold transform apply on the color image watermark and watermark bits are embedded by using the quantization method. The algorithm has good features of invisibility and it is robust against various image processing attacks *viz.* contrast adjustment, JPEG compression, Gaussian noise and salt and pepper noise, cropping [23].

3. PRELIMINARY

Chaos Inherent unpredictability or random in the behavior expressed is by defined system is quasi-random movement that seemingly is irregular of a complex natural system *viz.* the atmosphere, the beating heart. Chaos system can generate large number of random like high security keys because of very large period and great randomness of chaos signal, but it is certain. Data embedding is the most attractive features of chaos is extreme sensitivity to initial conditions which means that two nearby trajectories starting from initial states diverge exponentially when the time goes to infinity. Complex and unpredictable signals can be easily generated by 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 [16].

3.1 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. Logistic map is one of the simplest chaotic maps 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 determined by equation 1.

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

Where $0 \leq \mu \leq 4$, $0 < x_{k+1} < 1$

When $3.5699456 \leq \mu \leq 4$, 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].

3.2 Lorenz map

The Lorenz system is a system of ordinary differential equations first studied by Edward Lorenz. 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.

$$\begin{cases} \frac{dx}{dt} = a(y - x) & (2) \\ \frac{dy}{dt} = x(b - z) - y & (3) \\ \frac{dz}{dt} = xy - cz & (4) \end{cases}$$

When $a=10$, $c = \frac{8}{3}$, as long as b is more than 24.74, the solution of Lorenz equation is chaos system. In addition,

initial parameters and initial values 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 [18-21].

(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. Therefore, 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.

3.3 DCT Watermarking Technique

Discrete Cosine Transformation has been the most fascinating transformation methods that transforms the data

$$C(u, v) = \frac{2}{\sqrt{mn}} \alpha(u) \alpha(v) \sum_{x=0}^{m-1} \sum_{y=0}^{n-1} f(x, y) \times \cos \frac{(2x + 1)\mu\pi}{2m} \times \cos \frac{(2y + 1)v\pi}{2n} \tag{5}$$

$$f(x, y) = \frac{2}{\sqrt{mn}} \sum_{u=0}^{m-1} \sum_{v=0}^{n-1} \alpha(u) \alpha(v) f(x, y) \times \cos \frac{(2x + 1)\mu\pi}{2m} \times \cos \frac{(2y + 1)v\pi}{2n} \tag{6}$$

where $f(x, y)$ is the pixel value in the spatial domain, $C(u, v)$ is the DCT coefficient, m and n represent the block size and

$$\alpha(u), \alpha(v) = \begin{cases} \frac{1}{\sqrt{2}} & \text{if } u, v = 0 \\ 1 & \text{else} \end{cases}$$

The DC coefficient, which is the average value of the sample data, is obtained by putting $u = v = 0$ in Eq. (5) and all other coefficients are called the AC coefficients. DCT based image watermarking techniques are more robust in comparison to spatial domain watermarking techniques and robust against various image processing attacks *viz.* low pass filtering, blurring, brightness and contrast adjustment etc. However, frequency domain techniques are difficult to implement and are computationally more complex.

from the spatial domain to frequency domain for various image processing [22]. It have the property of energy compaction so it is widely used in image and signal processing. DCT broken the image into different frequency bands *viz.* high frequency, middle frequency and low frequency. Most of the energy of the image is concentrated in the lower frequencies coefficients and the higher frequency coefficients may be discard from its frequency components without too much data quality degradation. Now it is much easier to embedded the watermark bits in the desired frequency band. Generally middle frequency bands are preferred for watermarking. The middle frequency bands are selected such that they avoid the most visual parts of the image (low frequencies) without over-exposing themselves to removal through compression and noise attacks (high frequencies). Watermarking in the perceptually significant portion of the image has its own strength because most of the image compression technique remove the perceptually insignificant portion of the image. The mathematical equations of 2D discrete cosine transform and its inverse transform are

4. LU FACTORIZATION

As for the theory of matrices, Turing gives LU factorization method in 1948, which is the basic modified way of Gaussian elimination [24]. The LU factorization method decompose the matrix A as the product of lower triangular matrix L and an upper triangular matrix U . For example, A is a 4x4 matrix, its LU decomposition can be presented as:

$$A = [a_1, a_2, a_3] = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{24} \\ a_{31} & a_{32} & a_{34} \end{bmatrix}$$

$$= LU = [l_1, l_2, l_3][u_1, u_2, u_3] = \begin{bmatrix} 1 & 0 & 0 \\ l_{21} & 1 & 0 \\ l_{31} & l_{32} & 1 \end{bmatrix} \begin{bmatrix} u_{11} & u_{12} & u_{13} \\ 0 & u_{22} & u_{24} \\ 0 & 0 & u_{34} \end{bmatrix}$$

5. PROPOSED ALGORITHM

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.

5.1 Insertion algorithm

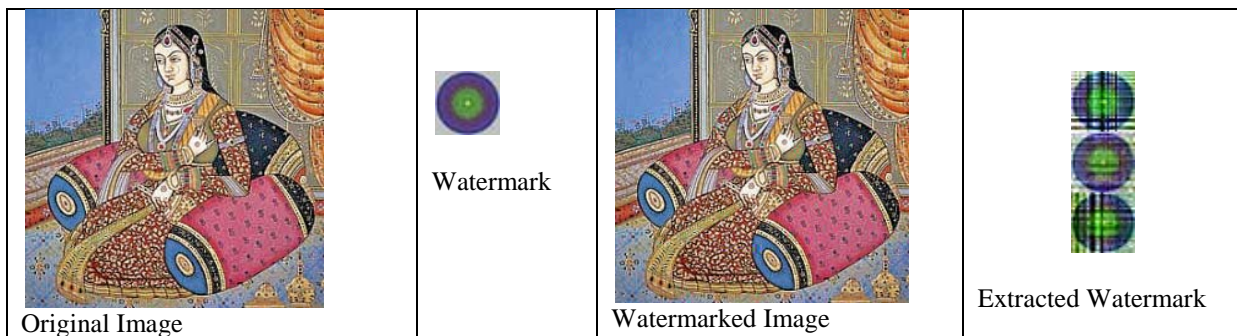
Step 1	Decompose the host and watermark image into YCBR color space.
Step 2	Partition each component of the host image and watermark images into non-overlapping blocks, and perform the Discrete Cosine Transformation for each blocks of host image after that LU Factorization apply on watermark's blocks.
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 $C' \rightarrow$ Watermarked image. $C \rightarrow$ Host image. $\alpha \rightarrow$ Strength. $W \rightarrow$ Pseudo image. $L \rightarrow$ 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.



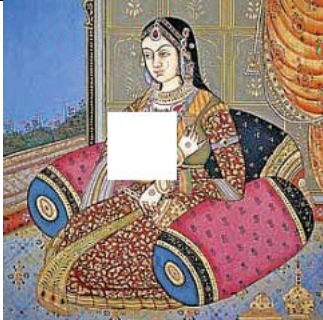







5.2 Extraction algorithm

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 watermark.
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 watermark from watermarked image using original image by below equation. $L = (C - C') / \alpha * W$ Where $C' \rightarrow$ Watermarked image. $C \rightarrow$ Host image. $\alpha \rightarrow$ Strength. $W \rightarrow$ Pseudo image. $L \rightarrow$ 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 watermark image.

6. 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.



Attack	Extracted Watermark
 <p data-bbox="571 477 748 506">Cropped Image</p>	
 <p data-bbox="600 824 719 855">Cut Image</p>	
 <p data-bbox="580 1137 743 1167">Brightness +5</p>	
 <p data-bbox="580 1435 743 1464">Brightness -5</p>	
 <p data-bbox="592 1733 732 1765">Contrast +2</p>	
 <p data-bbox="592 2033 732 2067">Contrast -2</p>	

7. CONCLUSION

In this paper, an image watermarking technique is proposed which is based on two chaotic maps Logistics map and Lorenz map, LU Factorization and a DCT transform. Before embedding the watermark LU decomposition is apply on the watermark and then embedded the watermark on chaotic locations and with chaotic strength factor. Proposed multiple watermark insertion, watermarking technique is highly robust because unauthorized users cannot find the actual location where watermark is embedded. Experimental results reveal that the proposed watermarking technique has good robustness against the many attacks

8. REFERENCE

- [1] I.J. Cox, J. Kilian, F.T. Leighton, T. Shamoan, Secure spread spectrum watermarking for multimedia, *IEEE Trans. Image Process* 6 (12) (1997) 1673–1687.
- [2] R. Liu, T. Tan, An SVD-based watermarking scheme for protecting rightful ownership, *IEEE Trans. Multimedia* 4 (1) (2002) 121–128.
- [3] I.J. Cox, M.L. Miller, J.A. Bloom, *Digital Watermarking*, Morgan Kaufmann Publishers, San Francisco, CA, 2002
- [4] H.Berghel and L. O’Gorman, “Protecting ownership rights through digital watermarking”, *IEEE Computer Mag*, pp.101-103, July 1996.
- [5] J.-C. Liu, S.-Y. Chen, Fast two-layer image watermarking without referring to the original image and watermark, *Image Vis. Comput.* 19 (14) (2001) 1083–1097.
- [6] J.C. Patra, J.E. Phua, C. Bornand, A novel DCT domain CRT-based watermarking scheme for image authentication surviving JPEG compression, *Digit. Signal Process.* 20 (2010) 1597–1611.
- [7] T.-H. Lan, A.H. Tewfik, A novel high-capacity data-embedding system, *IEEE Trans. Image Process.* 15 (8) (2006) 2431–2440.
- [8] A. Phadikar, S.P. Maity, B. Verma, Region based QIM digital watermarking scheme for image database in DCT domain, *Comput. Electr. Eng.* 37 (2011) 339–355.
- [9] W. Lu, H. Lu, F.-L. Chung, Feature based robust watermarking using image normalization, *Comput. Electr. Eng.* 36 (2010) 2–18.
- [10] M. Ouhain, A.B. Hamza, Image watermarking scheme using nonnegative matrix factorization and wavelet transform, *Expert Syst. Appl.* 36 (2) (2009) 2123–2129.
- [11] D. Zhao, C. Guanrong and L. Wenbo, “ A chaos-based robust wavelet-domain watermarking algorithm”, *Chaos, solutions and fractals*, vol. 22 pp. 47-54,2004.
- [12] G.H. Yeh. and G.C. Lee, “Toral fragile watermarking for localizing and recovering tampered image”, in *IEEE Symposium on Intelligent Signal Processing and Communication System*, Hong Kong, Dec 2005, pp.321-324.
- [13] Y.T. Wu and F.Y. Shih, “Digital watermarking based on chaotic map and reference register”, *Pattern Recognition*, vol.40, no. 12,pp.3753-3763,Dec 2007.
- [14] S. Mabtoull , E. Ibn-Elhaj, and D. Aboutajdine1, “A blind chaos-based complex wavelet-domain image watermarking technique”, in *International Journal of Computer Science and Network Security*, VOL.6 No.3, March 2006.
- [15] E. Chrysochos, V. Fotopoulos, and A. N. Skodras, “Robust watermarking of digital images based on chaotic mapping and DCT”, in *16th European Signal Processing Conference (EUSIPCO 2008)*, Lausanne, Switzerland, August 25-29, 2008.
- [16] Y. Zhao, M. Yunfei, and L. Zhiquan, “A robust chaos-based DCT-domain watermarking algorithm”, in *International Conference on Computer Science and Software Engineering*, 2008.
- [17] S. L. Hsieh, Lung-Yao Hsu, and I-Ju Tsai, “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, December 2005.
- [18] Y. Fei, J. Luo, and S. Wu. “Color Image Watermark Algorithm Based On Lorenz Chaos Encrypting” *ICSP2006 Proceedings* 2006.
- [19] LV Jinghu, LU Junan, CHEN Shihua.. *ChaosTime Sequence Analysis and Application[M]*,Wuhan: Wuhan University Press, 2002.
- [20] ZhANGLihong, ZHANG Yifeng. “Research on Lorenz Chaotic Stream Cipher [J]”. *Journal of Electronic Engineering Institute*, 24(1), pp. 31-34, 2005.
- [21] GUAN Xinping, Fan Zhengping, CHEN Cailian, HUA Changchun. *Chaotic Control and its Application in Secret Communication [M]*,Beijing: National Defence Press, 2002.
- [22] S.A. Khayam, *The Discrete Cosine Transform (DCT): Theory and Application*, Michigan State University, 2003.
- [23] Dongyan Wang, Fanfan Yang, and Heng Zhang, "Blind Color Image Watermarking Based on DWT and LU Decomposition ," *Journal of Information Processing Systems*, vol. 12, no. 4, pp. 765~778, 2016.
- [24] A. M. Turing, “Rounding-off errors in matrix processes,” *The Quarterly Journal of Mechanics and Applied Mathematics*, vol. 1, no. 1, pp. 287-308, 1948.