A Color Image Watermarking Scheme Based On QR Factorization, Logistic and Lorentz Chaotic Maps

Kamred Udham Singh
DST- Centre for Interdisciplinary Mathematical Sciences,
Banaras Hindu University, Varanasi,
U.P-221005, India
kamredudhamsingh@gmail.com

Dr. Achintya Singhal
Department of Computer Science,
Banaras Hindu University, Varanasi,
U.P-221005, India
achintya.singhal@gmail.com

Abstract—Most of the existing color image watermarking schemes use grayscale or binary image as watermark because color image watermark has more data than grayscale or binary watermark. Therefore, it is a challenging issue to design a color image-watermarking scheme. This paper proposes a novel color image watermarking scheme to embed color image watermark into color host image. In watermarking schemes, first divide the host and watermark image into non-overlapping blocks, apply the Discrete Cosine Transformation (DCT) on each blocks of both watermark, and host image. After that QR Factorization, apply on the each blocks of watermark. In this paper, Logistic and Lorentz chaotic maps are usedfor estimating the embedding strength and location. The experimental results reveal that this watermarking scheme is robust against different image processing attacks viz. cropping, contrast adjustment and coloring.

***Keywords**-Chaos Maps; watermarking; DCT; QR Factorization; image.*

*****

I. INTRODUCTION

Last several years, rapid development and popularization of information technology, computer networks and the tremendous usage of the internet humans can easily access the multimedia data from networks that made duplication and unauthorised distribution of multimedia contents viz. video, audio and images much easier. Multimedia security including unauthorized tampering, illegal copying, infringement, modifying digital copyright etc., is the major issues of digital content on a network, to address these issues watermarking technology has been considered as a powerful method and come in existence[1 - 3]. Watermarking is a descendent of a technique known as steganography, which has been in existence for a several centuries. The main objective of digital image watermarking is to embedded the some important information into a host image that can be a grayscale image, binary image, color image, pseudo random sequence etc. which proves the ownership of the object. 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.

Based on domain, Image watermarking schemes are classified into two categories first is spatial domain techniques and second is frequency domain techniques. In Spatial domain watermarking schemes watermark is directly inserted into the host image by modifying the pixel values [4]. Least significant bit is the simplest technique of the spatial domain in which Least significant bit of the host image is substitute with the watermark bit and these schemes are easy to implement with low complexity but not robust against the image processing attacks [3]. Whereas frequency domain watermarking schemes first transform the host image from spatial domain to the frequency domain and then watermark is embedded into the host image by modifying its frequency coefficients. Different type of transformations viz. discrete cosine transforms (DCT), discrete wavelet transforms (DWT), and discrete Fourier transforms (DFT) are used in image watermarking [6-9]. Transformations based watermarking schemes are more robust against image processing attacks in comparison to the spatial domain schemes but transform domain schemes have higher computational complexity. Another classification of watermarking schemes are Blind and Non-Blind schemes Blind image watermarking schemes are those schemes in which watermark extraction is done without using original host image. However, in Non-Blind schemes original host image must be required for watermark extraction. Consequently, blind techniques are comparatively less robust than non-blind schemes.Watermark recovery is usually more robust if the original host image are available.

II. REVIEW OF RELATED RESEARCH

Various types of image watermarking schemes have been previously to provide robust and effective watermarking including authenticity, imperceptibility and integrity.

ISSN: 2321-8169
291 – 296

Zhao et al. [10] proposed a chaotic watermarking scheme based on DWT and logistic. In this scheme, author first divide the image into non-overlapping blocks and select some of them blocks to create a sub image (watermark). The selection of blocks is done with the help of chaotic logistic map and then these blocks are then transformed in the DWT domain and then watermark is embedded it into the host image.

Yeh and Lee [11] proposed a block-based fragile watermarking scheme in spatial domain. An authentication signature, along with a relation signature, intended for recovery purposes. In this scheme author embedded a watermark in host image using LSB (lease significant bit) technique where two least significant bits of each pixel are substituted with the watermark's bits. Consequentially 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.

Wu and Shih [12] proposed a watermarking scheme based on chaotic map and reference register. This scheme 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.

S. Mabtoul et al. [13] proposed a blind digital image-watermarking scheme based on Dual Tree Complex Wavelet Transform and chaotic logistic map. First, a watermark image is pre-processed with a random location matrix. Author apply the Dual Tree Complex Wavelet Transform locally on the host image for creating the 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.

E. Chrysochos et al. [14] 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.

Chou et al. [15] proposed a blind color image-watermarking scheme. Author use the quantization indices of the host image in the uniform color space. This scheme was based on spatial domain, so the robustness of the scheme was not enough good. However, this scheme is robust against some watermarking attacks viz. cropping, scaling, low-pass filtering, and JPEG compression with high compression ratios.

Yin et al. [16], proposed a non-blind color watermarking scheme based on SVD (Singular Value Decomposition) and DWT. In this scheme author, apply DWT on the green component of the image and embedded the scrambled watermark into the green component of the color image. Author tests the robustness against various image-processing attacks viz. cropping, Gaussian noise, median filter, JPEG compression and
Resize.

Zhao et al. [17] proposed a blind watermarking scheme based on DCT and chaotic map. Pixels of watermark was scrambled using chaos map with secret keys. After scrambling process, watermark's bits are embedded into the least signification bits (LSB) of the quantized DCT coefficients. Author test the robustness of the scheme against geometric attacks and signal processing operations and fount the good result.

Shang-Lin Hsieh et al. [18] 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.

QR factorization is the intermediate step in SVD (Singular Value Decomposition), due to this characteristic QR factorization come in existence in watermarking and some watermarking schemes have proposed. Yashar et al. [19] proposed blind watermarking scheme to embed a watermark in a gray-scale image based on QR decomposition and use the R matrix to embedding the watermark in the first row of R matrix after each 8×8 block. Author also mention that first row of R matrix is greater than the other rows so use this property to embed the watermark.

Song et al. [20] proposed a blind watermarking scheme based on QR and logistic chaotic map for grayscale images. Author embedded the binary watermark into the 512×512 host image by modifying the first column coefficients in Q matrix.

Qingtang Su et al. [21] proposed a blind watermarking scheme based on QR for color images. Author first divided the image into non-overlapping 3×3 pixel blocks and then apply the QR decomposition on each blocks, after that color watermark image is embedded into the host image by modifying the second row first column coefficient and the third row first column coefficient of the matrix Q.

III. PRELIMINARY

ChaosInherent 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 verylarge period and great randomicity of chaos signal, but it is certain. Data embedding is the most attractive features of chaos is extreme sensitivity to initial conditions which means thattwo 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 [17].

A. Logistic map

The logistic map is a polynomialmapping(equivalently, recurrence relation)ofdegree 2, chaotic behaviour can arise from very simple non-linear dynamical equations.Logistic map is one of the simplest chaotic mapswas 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[13]. Logistic map is determined by equation 1.

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

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

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].

B. 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.

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

When a=10, $c = \frac{8}{3}$, as long as b is more than 24.74, the solution of Lorenz equation is chaos system. 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[12] [17] [20].

- 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.
- 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.

C. DCT Watermarking Technique

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

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

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

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

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

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.

D. QR Factorization

The QR factorization, which is a type of matrix factorization, was formally introduced in [23], if A € Rm×n has linearly independent columns then it can be factored as

$$\boldsymbol{A = QR}$$

Where Q is m × n with orthonormal columns (its columns are orthogonal unit vector). $Q^T Q = I$, If A is square (m = n), then Q is orthogonal ($Q^T Q = QQ^T = I$) and R is n × n, upper triangular (also called right triangular matrix), with nonzero diagonal elements and R is non-singular. A is a 3x3 matrix; its QR factorization can be presented as:

$$A = QR = [Q_1, Q_2, Q_3] \begin{bmatrix} R_{11} & R_{12} & R_{13} \\ 0 & R_{22} & R_{24} \\ 0 & 0 & R_{34} \end{bmatrix}$$

For example, A is a 3x3 matrix; its QR factorization are:

$$A = \begin{bmatrix} 255 & 255 & 252 \\ 254 & 251 & 244 \\ 254 & 247 & 230 \end{bmatrix}$$

Then $QR(A)$;

$$Q = \begin{bmatrix} -0.5789 & 0.6708 & 0.4636 \\ -0.5766 & 0.0652 & -0.8144 \\ -0.5766 & -0.7387 & 0.3490 \end{bmatrix}$$

$$R = \begin{bmatrix} -440.5190 & -434.7531 & -419.1783 \\ 0 & 4.9753 & 15.0644 \\ 0 & 0 & -1.6234 \end{bmatrix}$$

IV. PROPOSED ALGORITHM

In this paper,an image watermarking algorithm is proposed, 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 watermark image into YCBR color space.
Step 2	Partition each component of the host image and logo images into non-overlapping blocks, and perform the Discrete Cosine Transformation for each blocks of host image and watermark after that apply the QR Factorization 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 + α *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') / α*W

 ISSN: 2321-8169
291 – 296

	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.

V. 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.

 Original Image	 Watermark	 Watermarked Image	 Extracted Watermark
Attack			Extracted Watermark
 Cropped Image			
 Cut Image			

 Brightness +5	
 Brightness -5	
 Contrast +2	
 Contrast -2	

VI. CONCLUSION

In this paper, an image watermarking technique is proposed which is based on two chaotic maps Logistics map and Lorenz map, QR Factorization and a DCT transform. Before embedding the watermark QR factorization 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 robustbecause unauthorized users can not find the actual location where watermark is embedded. Experimental results reveal that the proposed watermarking technique has good robustness against the many attacks

REFERENCE

[1] R. Liu, T. Tan, An SVD-based watermarking scheme for protecting rightful ownership, IEEE Trans. Multimedia 4 (1) (2002) 121–128.

ISSN: 2321-8169
291 – 296

[2] Chen B, Coatrieux G, Chen G, Sun X, Coatrieux JL, Shu H (2014) Full 4-D quaternion discrete Fouriertransform based watermarking for color images. Digital Signal Process 28(5):106–119

[3] Chen W, Quan C, Tay CJ Optical color image encryption based on Arnold transform and interferencemethod. Opt Commun, (2009) 282(18):3680–3685

[4] I.J. Cox, M.L. Miller, J.A. Bloom, Digital Watermarking, Morgan Kaufmann Publishers, San Francisco, CA, 2002

[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] W. Lu, H. Lu, F.-L. Chung, Feature based robust watermarking using image normalization, Comput. Electr. Eng. 36 (2010) 2–18.

[7] M. Ouhsain, A.B. Hamza, Image watermarking scheme using nonnegative matrix factorization and wavelet transform, Expert Syst. Appl. 36 (2) (2009) 2123–2129.

[8] T.-H. Lan, A.H. Tewfik, A novel high-capacity data-embedding system, IEEE Trans. Image Process. 15 (8) (2006) 2431–2440.

[9] 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.

[10] D. Zhao, C. Guanrong and L. Wenbo, “ A chaos-based robust wavelet-domain watermarking algorithm”, Chaos, solitions and fractals,(2004) vol. 22 pp. 47-54.

[11] 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.

[12] Y.T. Wu and F.Y. Shih, “Digital watermarking based on chaotic map and reference register”, Pattern Recognition, ,(Dec 2007).vol.40, no. 12,pp.3753-3763

[13] S. Mabtoul1 , 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, (March 2006).VOL.6 No.3.

[14] 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.

[15] Chou CH, Wu TL Embedding color watermarks in color images. EURASIP J Appl Signal Process, (2003)pp. 32–40.

[16] C. q. Yin, Li Li, A. q. Lv and Li Qu, "Color Image Watermarking Algorithm Based on DWT-SVD," 2007 IEEE International Conference on Automation and Logistics, Jinan, , (2007)pp. 2607-2611.

[17] 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.

[18] 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,(Dec. 2005), vol. 10.

[19] Yashar N, Saied HK Fast and robust watermarking in still images based on QR decomposition.Multimedia Tools Appl (2014), 72:2597–2618,

[20] Song W, Hou JJ, Li ZH, Huang L Chaotic system and QR factorization based robust digital imagewatermarking algorithm. J Cent South Univ Technol , (2011).18(1):116–124.

[21] O. Su, G. Wang, X. Zhang, G. Lv, and B. Chen, “An improved color image watermarking algorithm based on QR decomposition,” Multimedia. Tools Appl., (Nov. 2015). pp.1-23.

[22] S.A. Khayam, The Discrete Cosine Transform (DCT): Theory and Application, Michigan State University, (2003).

[23] De Moor B, Van Dooren P Generalizations of the singular value and QR decompositions. SIAM JMatrix Anal Appl 13(4):993–1014, 1992.