Blind Watermarking Techniques using DCT and Arnold 2D Cat Map for Color Images

Chittaranjan Pradhan, Bidyut Jyoti Saha, Kunal Kumar Kabi, Arun, Ajay Kumar Bisoi

Abstract— The modern era of digital communication facilities bring digital watermarking techniques which is required to copyright and authenticate owner's information which further tracks control of regeneration and redistribution of images over untrusted and public network. In this paper, a blind digital watermarking technique has been proposed using Discrete Cosine Transform (DCT) to embed information in mid-frequency. The Arnold 2D cat map is used to shuffle the original pixel positions of watermark color image. First, the watermark image is divided into its RGB components and Arnold 2D transformation has been applied. The original cover image is decomposed into its respective RGB components. The resulting watermark images are embedded into separate components of cover images using DCT. The intensity values of watermark images are hidden in mid frequency of DCT blocks of cover images. So, it doesn't scatter the original watermark to most visual parts of the image. The experimental results show that the algorithm is effective and robust.

Keywords— discrete cosine transform (DCT); arnold 2D cat map; digital watermarking; shuffling; color image decomposition; embedding; extraction; chaotic map.

I. INTRODUCTION

Within last decades, multimedia communication and distribution is increasing in public and insecure networks. Digital watermarking protects the information from being compromised or redistribution. It preserves the integrity and authenticity of the digital information. Different watermarking schemes are being used for different purposes. Fragile watermarking scheme focuses on image tampering while robust watermarking scheme focuses on robustness against malicious attacks. Spatial domain watermarking scheme includes every bit of watermark information hidden into each byte of original information. This technique is not robust against various attacks. Whereas, in transform domain watermarking information is hidden in such a way that it is difficult for attacker to copy or remove information and is more robust than spatial domain technique. Information can be embedded into high frequency, mid frequency or low frequency via common frequency transformation. The transform coefficients of image are changed to achieve watermarking.

Ruisong Ye [1] proposed a scheme to scramble a digital image which disorders the pixel positions using orbit of the transformation. Due to chaotic properties image can be recovered after several iterations. This technique helped to improve the robustness of watermark image from various hostile attacks.

Lu Ling *et al* [2] proposed a watermarking scheme based on DCT transform by Arnold map and spread spectrum which is proved to be robust and secret in nature. The Arnold transformation has been used to encrypt the watermark image. Resulting encrypted image is embedded into DCT coefficient which is selected by spread spectrum.

Tribhuwan Kumar Tewari *et al* [3] proposed an additive digital watermarking scheme based on DCT to increase the robustness against most common and hostile attacks. The Embedding of watermark information is done into mid-frequency of DCT coefficients only.

Siddharth Singh *et al* [4] proposed data hiding technique in DCT domain using chaotic sequence. The cover image is decomposed to smaller blocks and the Embedding of watermark information is done into mid-frequency of DCT coefficients. Peak signal to noise ratio (PSNR) and Normalized cross-correlation (NC) has been used as performance metrics.

Yang Qianli *et al* [5] had proposed a digital watermarking algorithm based on two dimension Discrete wavelet transform (DWT) and Discrete cosine transform (DCT) with gray images. The images are transformed into three wavelet domain and image is split into sub-blocks. Every block are then transformed into DCT including watermarking components and embedded into cover image.

Chittaranjan Pradhan *et al* [6] proposed a double encryption scheme in DCT domain. Arnold cat map and cross chaos map has been used for encrypting the watermark image twice. The encrypted image is then embedded into DCT domain. The original embedded cover is reconstructed by performing inverse DCT.

In this paper, we have proposed an algorithm for digital watermarking techniques for color images using Arnold 2D cat map and DCT. The original cover is decomposed into its RGB components separately and divided into 8x8 blocks. The watermark color image is also decomposed into its separate RGB components. Arnold's transformation is applied to

Chittaranjan Pradhan is with School of Computer Engineering, KIIT University, Bhubaneswar, India (phone: +91-9861397865; e-mail: chitaprakash@gmail.com).

Bidyut Jyoti Saha is with School of Computer Engineering, KIIT University, Bhubaneswar, India (e-mail: bidyutjyotisaha@gmail.com).

Kunal Kumar Kabi is with School of Computer Engineering, KIIT University, Bhubaneswar, India (e-mail: kunal.kabi90@gmail.com).

Arun is with School of Computer Engineering, KIIT University, Bhubaneswar, India (e-mail: arunchauhan73@gmail.com).

Ajay Kumar Bisoi is with School of Computer Engineering, KIIT University, Bhubaneswar, India (e-mail: akbisoifcs@kiit.ac.in).

978-1-4799-3358-7/14/$31.00 ©2014 IEEE

individual components of watermark image. The resulting encrypted images so formed are embedded in mid frequency of 8x8 2D DCT blocks. Inverse transformation is applied to reconstruct the embedded cover images. Three embedded cover are then concatenated to form final color Embedded cover image.

Our paper organization is as follows: Section 2 gives description of Arnold 2D cat map, Section 3 gives the details of Discrete Cosine Transform (DCT), Section 4 describes the proposed algorithm, and Section 5 gives the detail of results and discussions followed by Section 6 which describes conclusion.

II. ARNOLD 2D CAT MAP

Arnold 2D cat map; proposed by V. Arnold, is a pixel shuffling scheme which iterates several times and shuffles the pixel positions in the image. After certain iterations, the image repeats its pixel coordinates. The 2D Arnold cat map shows chaotic characteristics along with enhanced security than 1D Arnold cat map. Let's take a PxP image whose coordinates are K (i, j). The equation for 2D Arnold cat map is as follows [7]:

$$\begin{cases} i' = (i + aj) \bmod P * P \\ j' = (bi + (ab+1)j) \bmod P * P \end{cases} \quad (1)$$

Where, *a* and *b* are two control parameter. Eq. (1) is applied on the original pixel coordinate (i, j) to form a new pixel coordinate (i', j'). Arnold's period is different than secret encryption key.

III. DISCRETE COSINE TRANSFORM (DCT)

Discrete Cosine Transform (DCT) transforms the space domain or time domain of input into its frequency components. The DCT decomposes an image into several frequency bands. Information can be added into low frequency, mid frequency or high frequency. The mid frequency is used to embed because it is robust against several attacks and doesn't distort the most important parts of an image [3]. In digital signal processing, DCT is the commonly used linear transformation. DCT based watermarking is robust against low pass filtering, blur effects and brightness. 2D DCT algorithm in digital watermarking includes segmentation of image into non overlapping 8x8 blocks and forward DCT is applied to each blocks. Further, a coefficient selection criterion is defined and watermark image is embedded to the selected coefficients. The embedded cover image can be reconstructed using inverse transformation of DCT. The secret information is hidden in mid frequency of the DCT coefficient blocks.2D DCT for embedding in watermarking scheme is defined as follows [4]:

$$E(m,n) = \alpha(m)\alpha(n)\sum_{x=0}^{P-1}\sum_{y=0}^{P-1} f(x,y)\cos\left[\frac{\Pi(2x+1)}{2P}m\right]\cos\left[\frac{\Pi(2y+1)}{2P}n\right] \quad (2)$$

The formula for inverse transformation for reconstruction of embedded cover image is as follows [4]:

$$f(x,y) = \sum_{m=0}^{P-1}\sum_{n=0}^{P-1} \alpha(m) * \alpha(n) * E(m,n)\cos\left[\frac{\Pi(2x+1)}{2P}m\right]\cos\left[\frac{\Pi(2y+1)}{2P}n\right] \quad (3)$$

Where, *m, n* = 0,1,2,…*P*-1 and x, y=0,1,2,…*P*-1. α (*m*) is defined as follows:

$$\alpha(m) = \sqrt{\frac{1}{P}}, \; m = 0; \quad \alpha(m) = \sqrt{\frac{2}{P}}, \; m = 1, 2, \ldots, P-1; \quad (4)$$

IV. PROPOSED ALGORITHM

The proposed algorithm uses Arnold 2D chaotic map to enhance the security of embedding color image data. The watermark color images are decomposed into its respective RGB components. The whole algorithm is applied to these different components of color images. The color cover image is decomposed to its red, green and blue components respectively and divided into 8x8 blocks to embed the individual components of watermark image into mid frequency coefficients of DCT. The embedding and extraction algorithms are described below:

A. EMBEDDING

The steps for embedding the watermark image into coefficients of cover image are as follows:

1. Input the cover image and watermark image.
2. Both the images are decomposed to its RGB components respectively.
3. The components of watermark image are encrypted using Arnold 2D cat map using different secret keys (key1, key2, key3).
4. The individual component of cover image is divided into 8x8 DCT blocks.
5. The encrypted watermark information is embedded into mid frequency of the respective DCT coefficient blocks using the following formulae:

$$I' = I = \beta * W \quad (5)$$

Where, I = cover image, W = watermark,
I'= watermarked image, β = scaling factor.

6. Inverse transform domain is applied to generate individual embedded cover images.
7. The Individual Embedded cover images are concatenated to form final colored embedded cover image (Fig. 1).

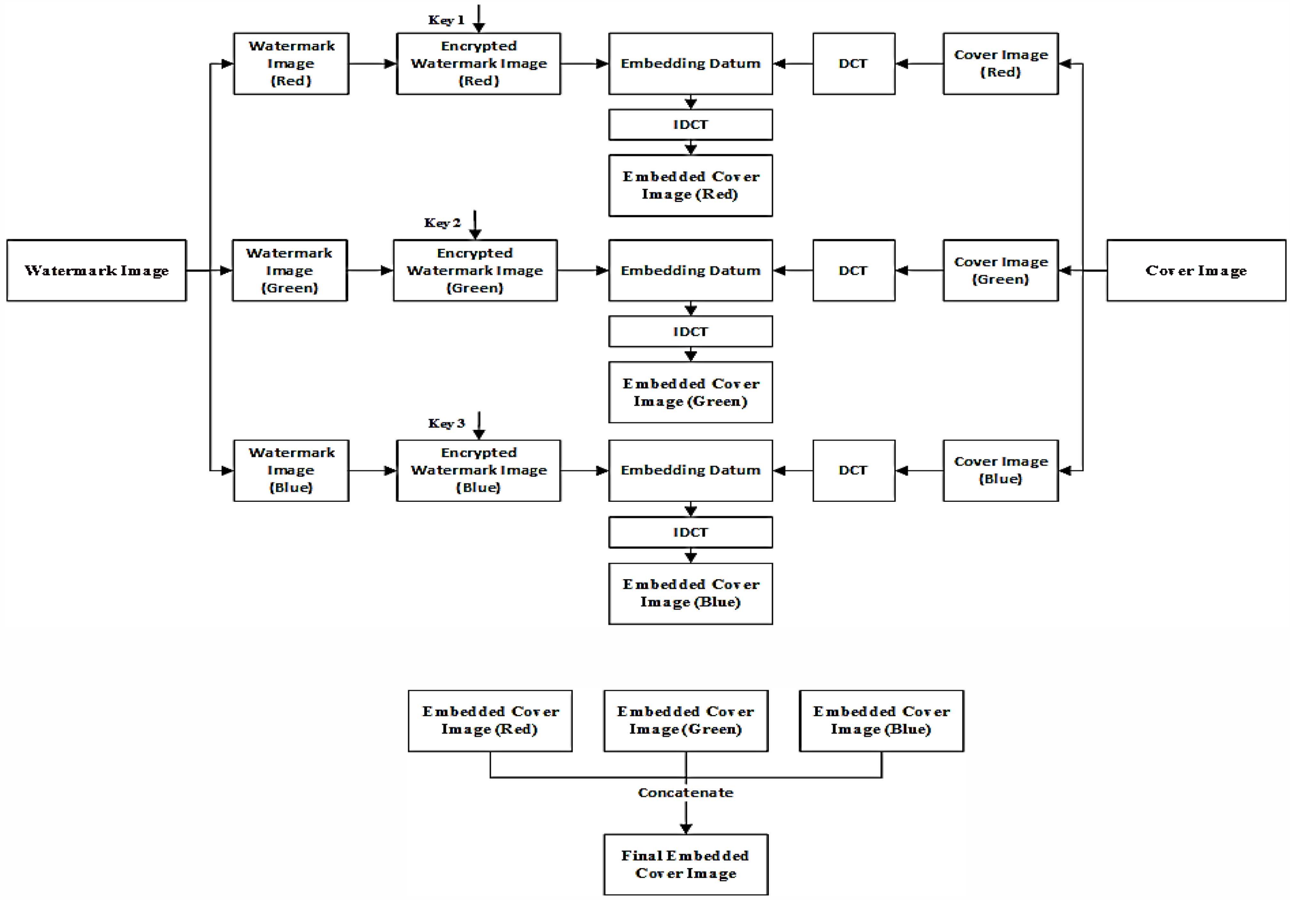

Fig. 1. Block Diagram of Embedding process

B. EXTRACTION

The steps for extraction of watermark image are as follows:

1. The final embedded cover image is decomposed into its respective RGB components.
2. Each individual component is divided into 8x8 DCT blocks.
3. Extract the DCT coefficients from mid frequency of DCT blocks of different components to generate individual encrypted watermark image.

$$W = \frac{I'}{\beta} \tag{6}$$

Where, W = watermark, I' = watermarked image, β = scaling factor.

4. The resulting encrypted watermark images are decrypted by 2D Arnold transformation using secret keys used in encryption process (same key should be used for decryption process).
5. The individual decrypted watermark is combined to form the resultant colored watermark image.

V. RESULTS AND ANALYSIS

For simulation and experiments, MATLAB *2012*a has been used. 'Barbara.png' of size 512x512 has been taken as cover image and shown in Fig. 3(a). 'Lena.png' of size 64x64 has been used as watermark image and shown in Fig. 3(c). Fig. 3(b) shows individual RGB components of cover image. Fig. 3(d) shows the individual RGB components of watermark image. The individual components of watermark images are encrypted using 2D Arnold map with different secret keys (key1=25, key2= 30, key3=45) and Embedded into the mid frequency of 8x8 DCT blocks of their respective components of cover images. Arnold's period is taken as 96. Fig. 3(e) shows the results after encryption of individual watermark images and Fig. 3(f) shows the embedded cover images after applying inverse transform domain. The resulting embedded cover images are further concatenated to produce final embedded colored cover image and shown in Fig. 3(g). Similarly, for extraction process the final embedded cover image is decomposed into its respective RGB components. The final embedded cover image is shown in Fig. 4(a) and its respective RGB components are shown in Fig. 4(b). Fig. 4(c) shows the results of encrypted watermark images after extracting DCT coefficients from mid frequencies. Fig. 4(d) shows the results of different components of watermark image after Arnold decryption process. The combined image of different RGB components is shown in Fig. 4(e) which gives the final color watermark image.

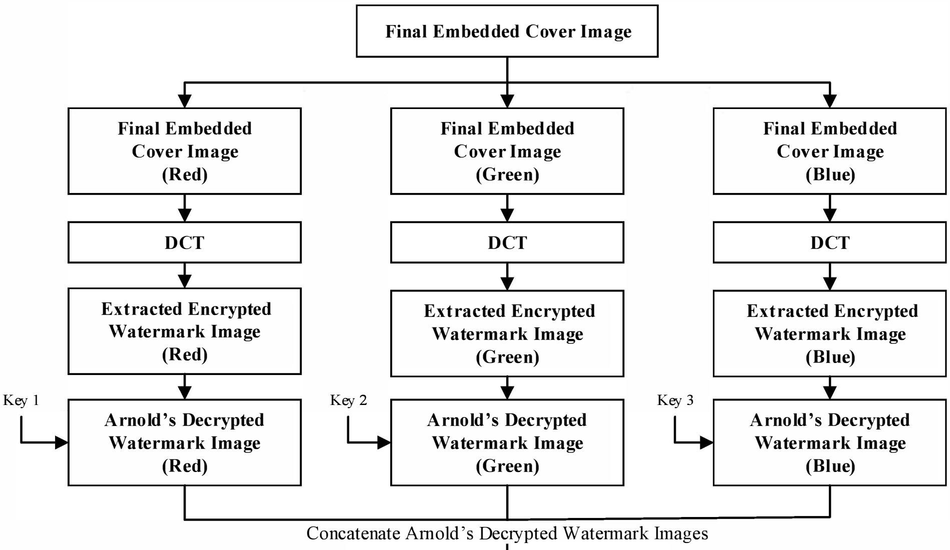

Fig. 2. Block Diagram of Extraction process

Fig. 3. Experimental results of embedding process

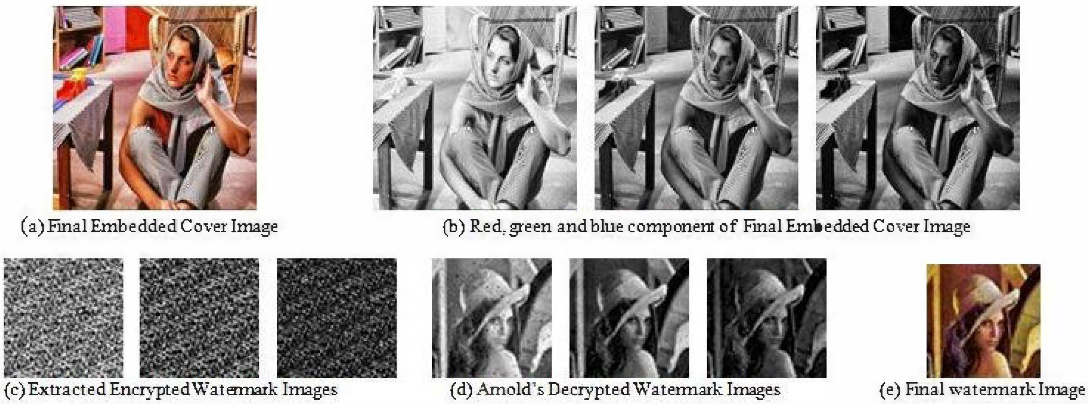

Fig. 4. Experimental results of embedding process

The visibility of the image can be calculated using Peak Signal to Noise Ratio (PSNR). The concealing capability of watermark algorithm is measured in decibels (dB). Greater the value of PSNR, greater the capability of concealing. Generally, PSNR greater than +30dB is assumed to have good concealing properties. PSNR can be calculated using following formula (1.6) [8]:

$$PSNR = 10\log_{10}\frac{A^2}{\frac{1}{M*N}\sum_{i=1}^{M}\sum_{j=1}^{N}\left[f(i,j)-f'(i,j)\right]^2} \quad (7)$$

'Barbara.png' of size 512x512 has been taken as cover image. For the calculation on two different watermark image 'Lena64.png' and 'Baboon64.png' has been taken.

PSNR values calculated for different RGB components with different keys are shown in Table. I.

The robustness of watermarking algorithm can be calculated by comparing original watermark and extracted watermark. Normalized Cross Correlation (NC) can be used to calculate the robustness in our algorithm. NC lies within 0 and 1. Bigger the value of NC, greater the robustness of the algorithm. NC can be defined as follow [8]:

$$NC = \frac{\sum_{a=1}^{N_1}\sum_{b=1}^{N_2} W(a,b)*W'(a,b)}{\sqrt{\sum_{a=1}^{N_1}\sum_{b=1}^{N_2}\left[W(a,b)\right]^2}\sqrt{\sum_{a=1}^{N_1}\sum_{b=1}^{N_2}\left[W'(a,b)\right]^2}} \quad (8)$$

'Lena64.png' and 'Baboon64.png' has been taken as watermark image. The cover image is attacked with different types of attacks and watermark images are extracted. The results of NC after various attacks are tabulated in Table. II. In both the analyses, we have taken keys as Key1=25, Key2=30, Key3=45.

TABLE I. PSNR VALUES

Cover Image	Watermark Image	PSNR(Red)	PSNR(Green)	PSNR(Blue)
Barbara.png	Lena64.png	+43.61 dB	+44.31 dB	+45.15 dB
Barbara.png	Baboon64.png	+41.80 dB	+42.51 dB	+41.09 dB

TABLE II. NC VALUES

Image	Poisson	Salt & Pepper	Speckle	Gaussian
Lena64.png	0.9607	0.5319	0.8567	0.8738
Baboon64.png	0.9698	0.5148	0.8626	0.8863

VI. CONCLUSION

This paper includes a watermarking algorithm using Arnold 2D cat map and DCT. The watermark image has been decomposed to its RGB components and each individual component is encrypted using Arnold's 2D map with different secret keys. The use of different secret keys in encryption of different RGB components makes the algorithm more secure. Cover image is also decomposed and divided into 8x8 blocks. The encrypted watermark components are embedded in 8x8 blocks of DCT coefficients in mid frequency. Hence, embedding in mid frequency results in robustness and avoid various attacks. PSNR is used to determine the concealing capability of algorithm which is in our case is greater than +40dB (Table I) and hence, imperceptible. For robustness of the algorithm, we have calculated NC. Experimental results of Table II show that the watermarking algorithm is robust against hostile attacks. Thus, we can say that the proposed algorithm is a secure and robust. In future, we will enhance the chaotic properties to increase the effectiveness of the algorithm by using higher dimensional chaotic maps. We will also implement the algorithm in DWT domain to increase the concealing capability.

REFERENCES

[1] Ruisong Ye, "A Novel Image Scrambling and Watermarking Scheme Based on Orbits of Arnold Transform", Pacific-Asia Conference on Circuits, Communications and System, IEEE, pp. 485-488, May 2009.

[2] Lu Ling, Sun Xinde and Cai Leiting, "A robust watermarking based on DCT by Arnold transform and spread spectrum", 3rd international conference on advanced computer theory and engineering, IEEE, Vol. 6, pp. 198-201, August 2010.

[3] Tribhuwan Kumar Tewari and Vikas Saxena, "An Improved and Robust DCT based Digital Image Watermarking Scheme", International Journal of Computer Applications, Vol. 3, No. 1, pp. 28-32, June 2010.

[4] Siddharth Singh, Tanveer J Siddiqui, Rajiv Singh and Harsh Vikram Singh, "DCT-domain robust data hiding using chaotic sequence", International Conference on Multimedia, Signal Processing and Communication Technologies, IEEE, pp. 300-303, December 2011.

[5] Yang Qianl and Cai Yanhong, "A Digital Image Watermarking Algorithm Based on Discrete Wavelet Transform and Discrete Cosine Transform", International Symposium on Information Technology in Medicine and Education, IEEE, pp. 1102-1105, August 2012.

[6] Chittaranjan Pradhan, Vilakshan Saxena and Ajay Kumar Bisoi, "Non Blind Digital Watermarking Technique Using DCT and Cross Chaos Map", International Conference on Communication, Devices, and Intelligent Systems, IEEE, pp. 282-285, December 2012.

[7] Musheer Ahmad and M. Shamsher Alam, "A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping", International Journal on Computer Science and Engineering, Vol.2, No. 1, pp. 46-50, 2009.

[8] Mei Jiansheng, Li Sukang and Tan Xiaomei, "A Digital Watermarking Algorithm Based On DCT and DWT", International Symposium on Web Information Systems and Applications, pp. 104-107, May 2009.