A Steganographic Scheme for Color Image Authentication Using Z-Transform (SSCIAZ)

Nabin Ghoshal[1], Soumit Chowdhury[2], and Jyotsna Kumar Mandal[3]

[1] Dept. of Engineering and Technology Studies,
University of Kalyani, Kalyani, Nadia-741235, West Bengal, India
[2] Dept. of Computer Science and Engineering,
Govt. College of Engineering & Ceramic Technology,
73, A. C. Banerjee Lane, Beliaghata, Kolkata-700010
[3] Dept. of Computer Science and Engineering,
University of Kalyani, Kalyani, Nadia-741235, West Bengal, India
{nabin_ghoshal,joy_pinu}@yahoo.co.in,
jkm.cse@gmail.com

Abstract. This paper deals with a novel Steganographic technique which demonstrates the color image authentication in Z-domain based on the Discrete two dimensional Z-Transform. The Transform is applied on mask of sub-image block of size 2 x 2 of spatial components in row major order for the entire image. Single bit from the authenticating secret message/image is fabricated into the real part of the frequency component of each carrier image byte. A delicate re-adjust phase is incorporated in all components of each mask after embedding, to keep the pixel values positive and non-fractional in the spatial domain. Robustness is achieved through embedding bits in variable positions of carrier image determined by a cyclic Fibonacci series. Experimental results show the enhanced performance of the proposed watermarking technique.

1 Introduction

Copyright [4, 5] abuse is the motivating factor in developing new encryption technologies. One such technology is digital watermarking [8, 9]. One of the driving forces behind the increased use of copyright marking is the growth of the Internet which has allowed images, audio, video, etc to become available in digital [2, 3] form. Though this provides an additional way to distribute material to consumers it has also made it far easier for copies of copyrighted material to be made and distributed. Using the Internet a copy stored on a computer can be shared easily with anybody regardless of distance often via a peer-to-peer network which doesn't require the material to be stored on a server and therefore makes it harder for the copyright owner to locate and prosecute offending parties. Copyright marking is seen as a partial solution [7, 9] to these problems. The mark can be embedded in any legal versions and will therefore be present in any copies made. This helps the copyright owner [1, 6, 8] to identify who has an illegal [10, 11] copy.

In general, there is a tradeoff between the watermarks embedding [11] strength (the watermark robustness) and quality (the watermark invisibility). Increased robustness

S.C. Satapathy et al. (Eds.): Proceedings of the InConINDIA 2012, AISC 132, pp. 209–216.
springerlink.com

requires a stronger embedding, which in turn increases the visual degradation of the images. The proposed watermarking scheme adopts a color image as the watermark so human eyes can easily verify the extraction of this visually meaningful watermark. In general, a color image can provide more perceptual information i.e. sufficient evidence against any illegal copyright invasion.

This paper is organized as follows: Two-Dimensional Discrete Z-Transform has been presented with expression evaluated and simplified. The insertion and extraction technique for embedding the authenticating image in the carrier image has been introduced with suitable algorithm and example. The result of the proposed technique SSCIAZ compared with the existing Reversible data hiding based on block median preservation (RDHBBMP [13]) watermarking method in terms of visual interpretation, MSE, PSNR in dB and IF.

The techniques used in this paper includes two dimensional discrete Z-Transform and two dimensional discrete inverse Z-Transform represented as

1.1 Two Dimensional Z Transform

A function $f(n1, n2)$ can be represented in Z-Transform as

$$f(z1, z2) = \sum_{n1=-\infty}^{\infty} \sum_{n2=-\infty}^{\infty} f(n1, n2) z1^{-n1} z2^{-n2} \tag{1}$$

where z1 and z2 are both complex numbers consisting of real and an imaginary parts. Since z1 and z2 are complex numbers, Let $z1=e^{j\omega 1\pi}$ and $z2=e^{j\omega 2\pi}$, Where $e^{j\theta} = \cos\theta + j\sin\theta$. Substituting the values of z1 and z2 in equation (1), the equation becomes the discrete form of Two Dimensional Z Transformation equation.

$$f(e^{j\omega 1\pi}, e^{j\omega 2\pi}) = \sum_{n1=-\infty}^{\infty} \sum_{n2=-\infty}^{\infty} f(n1.n2) e^{j\omega 1\pi^{-n1}} e^{j\omega 2\pi^{-n2}}$$

$$\text{Or } f(\omega 1, \omega 2) = \sum_{n1=-\infty}^{\infty} \sum_{n2=-\infty}^{\infty} f(n1, n2) e^{-j\pi(n1\omega 1 + n2\omega 2)} \tag{2}$$

1.2 Two Dimensional Inverse Z Transform

The Inverse Z-Transform of a function f(n1,n2) is represented as

$$f(n1, n2) = \left(\frac{1}{2\pi j}\right)^2 \oiint f(z1, z2) z1^{n1-1} z2^{n2-1}\, dz1 dz2 \tag{3}$$

Where f(n1,n2) be a function and f(z1,z2) be the Z-Transform of the function f(n1,n2).

1.3 Derivation of Inverse Z Transform from Continuous to Discrete Form

Since z1 and z2 are complex numbers, Let $z1=e^{j\omega 1\pi}$ and $z2=e^{j\omega 2\pi}$, where $e^{j\omega\theta} = \cos\omega\theta + j\sin\omega\theta$. Substituting the values of z1 and z2 in equation (3), we have a discrete form of inverse Z Transform for two dimensions. Now $z1=e^{j\omega 1\pi}$, differentiating this with respect to ω1 we get $\frac{dz1}{d\omega 1} = e^{j\omega 1\pi}j\pi$, therefore $dz1=e^{j\omega 1\pi}j\pi\ d\omega 1$ and $z2=e^{j\omega 2\pi}$, differentiating this with respect to ω2 we get $\frac{dz2}{d\omega 2} = e^{j\omega 2\pi}j\pi$, therefore $dz2=e^{j\omega 2\pi}j\pi\ d\omega 2$. The equation (3) becomes from the above derivation is

$$f(n1,n2) = \left(\frac{1}{2\pi j}\right)^2 \oiint f(e^{j\omega 1\pi}, e^{j\omega 2\pi}) e^{j\omega 1\pi^{n1-1}} e^{j\omega 2\pi^{n2-1}} e^{j\omega 1\pi} j\pi\ d\omega 1\ e^{j\omega 2\pi} j\pi\ d\omega 2$$

The discrete form of this equation is as follows

$$f(n1,n2) = \frac{1}{4}\sum_{\omega 1=-1}^{1}\sum_{\omega 2=-1}^{1} f(\omega 1,\omega 2)e^{j\pi(n1\omega 1+n2\omega 2)} \quad (4)$$

The equation (4) is the discrete form of Two Dimensional Inverse Z Transform.

2 The Technique

The Insertion of the authenticating image is performed in the Z-Domain i.e. the domain obtained after performing the Z-Transform on 2 x 2 sub-image matrix of the original image matrix one by one. Hence, in order to perform the insertion operation of the authenticating image into converted original image byte. Bits from authenticating image are embedded in single bit position under each byte of the source image. The authenticating image pixels are read and are converted into binary values and each binary bit is inserted into one pixel of the original image into which the watermark is supposed to be embedded. Point of insertion of a bit is obtained by computing the Fibonacci series and then taking the LSB two bits as the position of insertion of the bit to be embedded in the image.

Let C_w be the pixel value in Watermarked color image and C be the original pixel value of the digital image to be embedded. Let b[i] be the bit to be embedded in pixel C. The embedding or coding step and the detection scheme or the decoding step is as follows:

2.1 Insertion Algorithm

Input: A carrier image and authenticating message/image.
Output: An authenticated image.
Method: Embedding has been performed on the integer values only while the floating point part has been made intact and has been added after embedding the watermarking bits in the integer part of the pixels values of the source image.

1. Read Image type, dimensions and maximum intensity from source image and write in the output image.
2. Repeat until all pixels have been read from the source image file.
   2.1 Repeatedly Take 2 x 2 blocks of pixels from the matrix at the left and perform Z-Transform of the block of pixels until all pixels in the matrix have been taken.
   2.2 Compute the Fibonacci series and generate the positions using the two LSB bits of the generated number where the watermark bits will be embedded. The Fibonacci series will be repeated after taking a specific number of terms.
   2.3 Read the authenticating image i.e. watermark.
   2.4 Embed the watermark bits in the source image in the position specified by the number generated from the Fibonacci series.
   2.5 Compute the Inverse Z-Transform of the 2 x 2 block of pixels.
   2.6 If any pixel is found to be of negative value, the maximum negative number is stored and added in the watermarked pixel values such that there is no effect on the bit position where the watermark bit is embedded.
   2.7 Compute the Inverse Z-Transform of the block of pixels and the numbers obtained is guaranteed to be of positive values.
   2.8 Repeat the steps from 2.1 to 2.7 until all pixels have been transformed.
3. Stop.

2.2 Extraction Algorithm

The Extraction of the authenticating image is performed in the Z-Domain i.e. the domain obtained after performing the Z-Transform of the embedded image. Hence, in order to perform the extraction operation of the authenticating image from the embedded image, the embedded image is first converted using Z-Transform.

A masking based detection scheme has been proposed to retrieve the embedded watermark from a color carrier image. Bits from authenticating image have been embedded in single bit position under each byte of the source image by choosing a standard 2 x 2 mask in row major order. In case of retrieval of the authenticating image, we will have only one extracted bit from each pixel of the embedded image. Point of extraction of a bit is obtained by computing the Fibonacci series and then taking the LSB two bits as the position of extraction of the bit from the embedded image.

Input: Authenticated image.
Output: The original image, authenticating message/image.
Method: Extraction has been performed on the integer values only while the floating point part has been made intact and has been added after extracting the security bits from the integer part of the pixels values of the source image.

1. Read Image type, dimensions and maximum intensity from embedded image and skip writing in the output image.
2. Repeat until all pixels have been read from the embedded image.
   2.1. Repeatedly Take 2 x 2 blocks of pixels from the matrix at the left and perform Z-Transform of the block of pixels until all pixels in the matrix have been taken.

2.2. Compute the Fibonacci series and generate the positions using the two LSB bits of the generated number where the watermark bits have been embedded. The Fibonacci series will be repeated after taking a specific number of terms so as to avoid core dumb and overflow conditions.
2.3. Calculate the embedded bits from the embedded image from the position specified by the number generated from the Fibonacci series.
2.4. Convert each 8 bits of 0's and 1's into decimal value and write the value in the output image.
2.5. Repeat the steps from 2.1 to 2.6 until all pixels have been transformed and embedded bits have been calculated.

3. Stop.

3 Result Comparison and Analysis

This section represent the results, discussion and a comparative study of the proposed technique SSCIAZ with the DCT-based watermarking method, QFT-based and Spatio Chromatic DFT-based watermarking method in terms of visual interpretation, image fidelity (IF), and peak signal-to-noise ratio (PSNR) analysis and mean square error (MSE). In order to test the robustness of the scheme SSCIAZ, the technique is applied on more than 50 PPM colour images from which it may be revealed that the algorithm may overcome any type of attack like visual attack and statistical attack. Experimental set up for preparing result is any type of PC with 2.00 GHz and above processing speed, 2 GB primary memory and Fedora 6 or above version of OS with gimp application. Distinguishing of carrier and embedded image from human visual system is quite difficult. In this section some statistical and mathematical analysis is given. The original carrier images 'Airplane', 'Baboon', 'Lenna' and 'Oakland' are shown in fig 1a, 1b, 1c and 1d. The dimension of each carrier colour images is 512 x 512 and the dimension of the authenticating colour image (Fig. 1m) is shown in table 1 and 2. Embedded colour images are shown in Fig 1e, 1f, 1g and 1h using SSCIAZ. Single bit of secrete data is embedded in each carrier image byte. The magnified versions of different images have been shown on Fig. 1i, 1j, 1k and 1l.

Peak signal-to-noise ratio (PSNR) is used to evaluate qualities of the stego-images. Table 1 and 2 shows two levels of authenticating data byte embedding which is defined by EL=0 and EL=1 based on PSNR values. Table 2 shows the PSNR values for comparative studies of SSCIAZ and Reversible data hiding based on block median preservation (RDHBBMP) and also the enhancement in terms of hiding capacity of secrete data and PSNR in dB. The average enhancement of secrete data embedding is 34553 bits in SSCIAZ than the existing technique RDHBBMP and also .14 dB of PSNR in EL=0. But in EL=1 the average enhancement of secrete data embedding is 137697.5 bits in SSCIAZ than the existing technique RDHBBMP and also .33 dB of PSNR. In all the existing technique the PSNRs are low, means bit-error rate are high but in the proposed scheme more bytes of authenticating data can be embedded and the PSNR values are significantly high, means bit-error rate is low. The average improvement is shown in Table 2. Table 3 shows the better PSNR values than other exiting techniques like DCT-based [10] watermarking, QFT-based [11] watermarking, and SCDFT-based [12] watermarking in frequency domain. Capacities

of existing techniques are 3840 bytes and the PSNR values are 30.1024 dB, 30.9283 dB, and 30.4046 dB in SCDFT, QFT, and DCT respectively. Whereas the capacity of SSCIAZ is 8112 bytes and PSNR is 49.89 dB and which is fully recoverable. 4272 bytes more secrete data embedding is possible in SSCIAZ technique than existing techniques with average 19 dB more PSNR values.

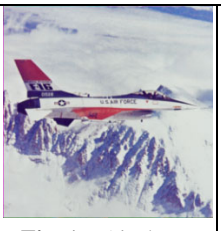

Fig. 1a. Airplane

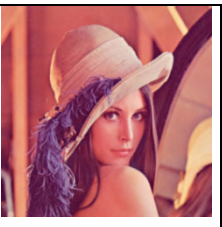

Fig. 1b. Lenna

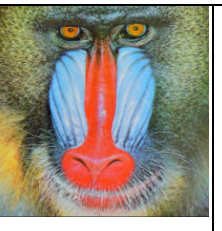

Fig. 1c. Baboon

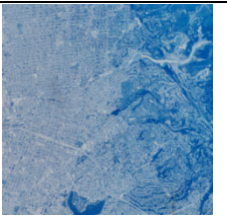

Fig. 1d. Oakland

Fig. 1e. Embedded Airplane

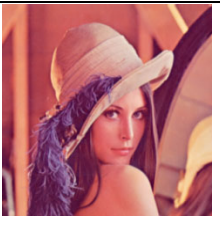

Fig. 1f. Embedded Lenna

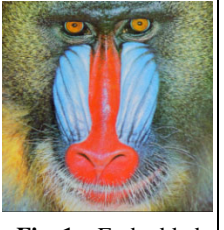

Fig. 1g. Embedded Baboon

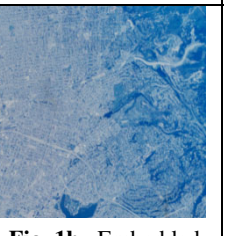

Fig. 1h. Embedded Oakland

Fig. 1i. Magnified Airplane

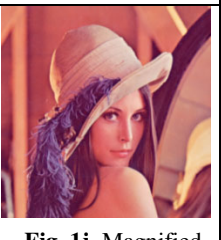

Fig. 1j. Magnified Lenna

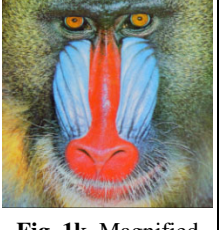

Fig. 1k. Magnified Baboon

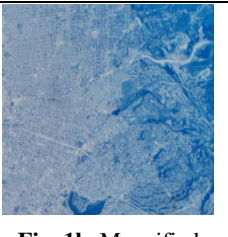

Fig. 1l. Magnified Oakland

Fig. 1m. Earth

Fig. 1. Visual interpretation of embedded image using SSCIZ and corresponding magnified images after embedding

Table 1. Capacities and PSNR values of SSCIAZ

Test images	Indicator	EL=0	EL=1
Baboon	C(bits)	60,000	194400
	PSNR	50.16	45.18
Oakland	C(bits)	60,000	194400
	PSNR	50.17	45.19
Peppers	C(bits)	60,000	194400
	PSNR	50.21	45.22
Average Image	C(bits)	60,000	194400
	PSNR	50.18	45.20

Table 2. Results and comparison in capacities and PSNR of SSCIAZ and RDHBBMP

Test images	Indicator	EL=0		EL=1	
		RDHBBMP	SSCIAZ	RDHBBMP	SSCIAZ
Lena	C(bits)	26,465	64,896	71,769	2,16,600
	PSNR	49.68	49.89	44.35	44.76
Airplane	C(bits)	36,221	64,896	86,036	2,16,600
	PSNR	49.80	49.87	44.64	44.89
Average Image	Δ Ca	34553		137697.5	
	Δ PSNRa	0.14		0.33	

Table 3. Results and comparison in capacities and PSNR of SSCIAZ and DCT, QFT, SCDFT [12]

Technique	Capacity (bytes)	PSNR in dB
SCDFT	3840	30.1024
QFT	3840	30.9283
DCT	3840	30.4046
SSCIAZ	**8112**	**49.8900**

4 Conclusion

SSCIAZ technique is an image authentication process to enhance the security compared to the existing algorithms. Authentication is done by embedding secrete data embedding in each mask of carrier image byte is possible. In compare to Reversible data hiding based on block median preservation, SSCIAZ algorithm is applicable for any types of colour image authentication and strength is high. The PSNR is high and more bytes of authenticating bits can be embedded in the carrier images. The watermark embedded in this method is very hard to detect due to unknown insertion position of the authenticating bits in the carrier image. So, the proposed technique SSCIAZ also provides security from all possible attacks.

Acknowledgement. The author expresses the deep sense of gratitude to the Dept. of Engineering and Technological Studies, University of Kalyani, West Bengal, India, where the work has been carried out.

References

1. Radhakrishnan, R., Kharrazi, M., Menon, N.: Data Masking: A new approach for steganography. Journal of VLSI Signal Processing 41, 293–303 (2005)
2. EL-Emam, N.N.: Hiding a large Amount of data with High Security Using Steganography Algorithm. Journal of Computer Science 3(4), 223–232 (2007) ISSN 1549-3636
3. Amin, P., Lue, N., Subbalakshmi, K.: Statistically secure digital image data hiding. In: IEEE Multimedia Signal Processing MMSP 2005, Shanghai, China, pp. 1–4 (October 2005)
4. Pavan, S., Gangadharpalli, S., Sridhar, V.: Multivariate entropy detector based hybrid image registration algorithm. In: IEEE Int. Conf. on Acoustics, Speech and Signal Processing, Philadelphia, Pennsylvania, USA, pp. 18–23 (March 2005)
5. Al-Hamami, A.H., Al-Ani, S.A.: A New Approach for Authentication Technique. Journal of Computer Science 1(1), 103–106 (2005) ISSN 1549-3636
6. Ker, A.: Steganalysis of Embedding in Two Least-Significant Bits. IEEE Transaction on Information Forensics and Security 2(1), 46–54 (2008) ISSN 1556-6013
7. Yang, C., Liu, F., Luo, X., Liu, B.: Steganalysis Frameworks of Embedding in Multiple Least Significant Bits. IEEE Transaction on Information Forensics and Security 3(4), 662–672 (2008) ISSN 1556-6013
8. Wu, H.C., Wu, N.I., Tsai, C.S., Hwang, M.S.: Image steganographic scheme based on pisel-value differencing and LSB replacement methods. Proc. Inst. Elect. Eng., Vis. Images Signal Processing 152(5), 611–615 (2005)
9. Yang, C.H., Weng, C.Y., Wang, S.J., Sun, H.M.: Adaptive Data Hiding in edge areas of Images With Spatial LSB Domain Systems. IEEE Transaction on Information Forensics and Security 3(3), 488–497 (2008) ISSN 1556-6013
10. Ahmidi, N., Safabkhsh, R.: A novel DCT-based approach for secure color image watermarking. In: Proc. Int. Conf. Information Technology: Coding and Computing, vol. 2, pp. 709–713 (2004)
11. Bas, P., Biham, N.L., Chassery, J.: Color watermarking using quaternion Fourier transformation. In: Proc. ICASSP, Hong Kong, China, pp. 521–524 (June 2003)
12. Tsui, T.T., Zhang, X.–P., Androutsos, D.: Color Image Watermarking Usimg Multidimensional Fourier Transfomation. IEEE Trans. on Info. Forensics and Security 3(1), 16–28 (2008)
13. Luo, H., Yu, F.-X., Chen, H., Huang, Z.-L., Li, H., Wang, P.-H.: Reversible data hiding based on block median preservation. Information Sciences 181, 308–328 (2011)