AMSE JOURNALS –2014-Series: Advances B; Vol. 57; N° 1; pp 20-30

Submitted Dec. 2013; Revised March 29, 2014; Accepted April 20, 2014

A Genetic Algorithm Based Approach in Image Authentication using Z Transform (GAIAZT)

* A. Khamrui, **J.K. Mandal

*Department of Computer Engineering, Future Institute of Engineering and Management,
Sonarpur Station Road, Sonarpur, Kolkata-150, West Bengal, India
**Dept of Computer Science, University of Kalyani,
Kalyani, Nadia-741235, West Bengal, India
(khamruiamrita@gmail.com; jkm.cse@gmail.com)

Abstract:

In this proposal a transformed domain based gray scale image authentication/data hiding technique using Z transform (ZT) termed as GAIAZT, has been proposed. Z-Transform is applied on 2×2 masks of the source image in row major order to transform original sub image (cover image) block to its corresponding frequency domain. One bit of the hidden image is embedded in each mask of the source image onto the fourth LSB of transformed coefficient based on median value of the mask. Resulting image mask is taken as initial population. A delicate GA based handling has also been performed as post embedding operation for proper decoding. Genetic algorithm is used to minimize the difference between the source and embedding image. Reverse process is followed during decoding. High PSNR obtained for various images conform the quality of invisible watermark of GAIAZT in Comparison with existing approach Chin-Chen Chang et al.[1].

Key words

Frequency Domain Steganography, Invisible Watermark, peak signal to noise ratio (PSNR), Z Transform (ZT), Median Based Embedding in frequency Domain

1. Introduction

Steganography is an ancient art. It is used for security in open systems. It focuses on hiding secret messages inside a cover medium. The most important property of a cover medium is the amount of data that can be stored inside it without changing its noticeable properties. There are many sophisticated techniques with which to hide, analyze, and recover that hidden information are discussed next. Generally, a steganographic message may be picture, video, sound file [7], [6].

Some steganography algorithm encrypts the secret message and spreads it in highly noisy image regions of a carrier image using spread spectrum and discrete cosine transform methods [12]. Data hiding [5] in the image has become an important tool for image authentication. Ownership verification and authentication are the major task for military people, research institute and scientists. Information security and image authentication has become very important to protect digital image document from unauthorized access [3], [4]. The most notable steganalysis algorithm is the RS attack which detects the stego-message by the statistic analysis of pixel values. To resist to RS analysis, the influence on the correlation of pixels needs to be compensated. The compensation may be achieved by adjusting other bit planes optimization algorithms have been employed in information hiding to find the optimal embedding positions. The genetic algorithm is used to estimate the best adjusting mode. By the adjustment, the artifacts caused by the steganography can be eliminated and the image quality will not be degraded [14]. The motive is to hide a message inside an image keeping the visible properties [13] of source image as close to the original. The most common methods to make these alteration is usage of the least-significant bit (LSB) developed through [9] masking, filtering and transformations on the source image [6]. Some wavelet based transformation technique pre-adjusts the original cover image in order to guarantee that the reconstructed pixels from the embedded coefficients would not exceed its maximum value and hence the message will be correctly recovered [15]. Most of the works [10], [8], [11], [2] used minimum bits of the hidden image for embedding in spatial domain, but the proposed algorithm embeds in transformed domain with a bare minimum distortion of visual property.

Rest of the paper is organized as follows. Section 2 deals with the proposed technique. Results and comparisons are given in section 3. Discussion and Concluding remarks are presented in section 4 and 5, respectively and references are drawn at end.

2. The Technique

In the process of embedding a 2 x 2 mask is chosen in row major order. One bit of the authenticating message/image is embedded in each mask row major order in transformed domain. 2×2 gray scale image mask is transformed from spatial domain to frequency domain using Z-Transform. Along with the hidden image, the dimensional values are also embedded into the real part of the host image mask on fourth LSB bit of the transformed coefficient within 2×2 mask, where the coefficient is chosen based on median value of the coefficient of 2 x 2 mask. Resulting image mask of size 32 bits are taken as initial population. A delicate GA based handling called New Generation has also been performed as post embedding operation for proper decoding. Stego sub intermediate image is obtained through a reverse transform as final step of embedding in a mask. Crossover and Mutation are applied on the New Generated image to obtain stego image. For Crossover operation rightmost 3 bits from each byte of the initial population is taken. A consecutive bitwise XOR is performed on it for the 3 steps. It will form a triangular form and first bit from each step is taken. Mutation is performed between rightmost 2bits of the consecutive two pixels of each mask as a result rightmost two bits of each pixel are swapped. In the process of embedding dimension of the hidden image followed by the content of the message/hidden image are embedded. Reverse process is followed during decoding. Genetic Algorithm is applied onto the embedded image to minimize the difference between source and embedded image.

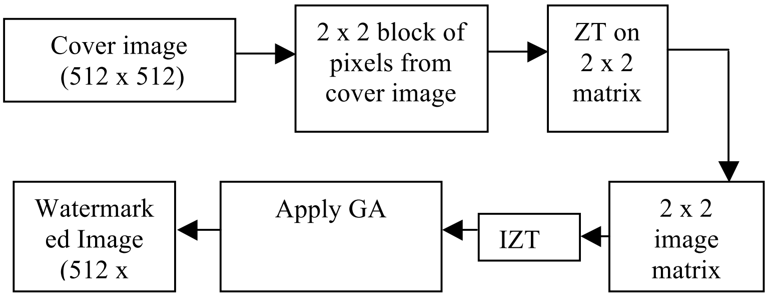


Figure.1.1: The process to embed the Secret data into the source image

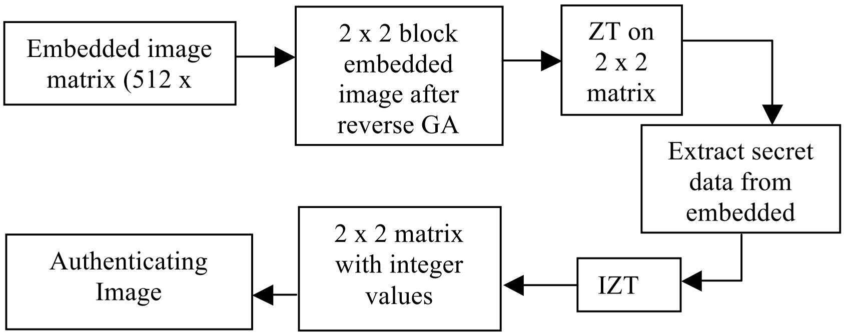

Embedded image matrix (512 x
2 x 2 block embedded image after reverse GA
ZT on 2 x 2 matrix
Extract secret data from embedded
IZT
2 x 2 matrix with integer values
Authenticating Image

Figure. 1.2: The process to extract Secret data from the watermarked image

Figure 1: Schematic diagram of GAIAZT

Z-Transform is a two dimensional function where (n1, n2) is a spatial coordinate can be represented by equation (1).

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

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 (2) becomes the discrete form of two dimensional Z-Transformation equations.

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

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

Where ω_1 and ω_2 are two frequency variables, varies from $-\infty$ to $+\infty$ and n1 and n2 is finite and positive numbers. In case of present implementation ω ranges between 0 to$3\pi/2$ andn1 and n2 varies from 0 to 1.

The discrete form of Two Dimensional Inverse Z-Transform of a function f(n1, n2) is represented by equation (3).

$$f(n1, n2) = \frac{1}{4} \sum_{\omega 1=-1}^{1} \sum_{\omega 2=-1}^{1} f(\omega 1, \omega 2) e^{j\pi(n1\omega 1 + n2\omega 2)} \qquad (3)$$

Schematic diagram of the technique is shown Figure1 of which Figure.1.1 shows process of encoding that of Figure.1.2 depicts the process of decoding. Algorithm of insertion and extraction are given in section 2.1 and 2.2 respectively. A complete example has also been illustrated in section 2.3.

2.1. Insertion Algorithm

The technique uses gray scale image of size p×q as input. Hidden image of size m×n is chosen. One bit of hidden image is embedded in each mask based on median values of transformed coefficients in Z-domain.

Input **:** Host image of size p×q, authenticating image of size m×n.

Output **:** Embedded image of size p×q.

Method **:** Insertion of authenticating image bitwise into the gray scale image.

Step 1: Obtain the size of the hidden image m×n

Step 2: For each hidden message/image, read source image mask of size 2×2 in row major order. Apply Z-Transform onto the selected cover image mask (2×2) to obtain coefficients in transformed domain

Step 3: Obtain Median of the four frequency coefficients obtained in step 2 to choose the byte for embedding

Step 4: Embed 1 secret bit onto the fourth LSB position towards left of the byte

Step 5: 2×2 embedded image mask of size 32 bits are taken as initial population. Apply New Generation as a delicate handle

Step 5: Apply IZ-Transform to back the mask from Z domain to spatial domain

Step 6: Repeat step 2 to 6 for the whole cover image

Step 7: Perform Crossover operation on the New Generated image. For this operation rightmost 3 bits from each byte of the New Generation is taken. A consecutive bitwise XOR is performed on it for the 3 steps. It will form a triangular form and first bit from each step is taken

Step 8: Mutation is performed between rightmost 2 bits of the consecutive two pixels of each mask as a result rightmost two bits of each pixel is swapped

Step 9: Stop

2.2. Extraction Algorithm

The hidden image is received in spatial domain. The embedded image is taken as the input and the hidden message/ image size, content are extracted from It.

Input **:** Embedded image of size p×q.

Output **:** Host image of size p×q, authenticating image of size m×n.

Method **:** Extract bits of authenticating image from embedded image.

Step 1: Reverse Mutation is performed on the rightmost 2 bits of two consecutive pixels of the each mask. For this rightmost two bits of the each pixel are swapped

Step 2: Reverse Crossover is performed by consecutive bitwise XOR operation on the rightmost 3 bits of each byte in three steps. The first bit of each step is taken as the output

Step 3: Read embedded image mask (of size 2×2) in row major order. Apply Z-Transform onto the embedded image mask to transform the embedded sub image from spatial to frequency domain so that four frequency components are regenerated

Step 4: Obtain Median of four frequency components to choose the embedded byte from 2×2 mask

Step 5: Extract the secret bit from the byte embedded in fourth LSB position. Replace hidden message/ image bit position in the block by '1'. For each eight extracted bits construct one image pixel of authenticating image

Step 6: Repeat step 1 to 3 to regenerate hidden image as per size of the hidden image

Step 7: Stop

2.3. Example

The benchmark image Lenna and Jet are taken from the image database [16] for experimental verification. A 2×2 mask from the Lenna image is taken as input as shown in Figure 2b. Figure 2a shows a byte of the Jet image which is taken as authenticating information. The mask is transformed into frequency domain using Z transform by equation 1. Figure 2c shows the coefficients of the transformed mask. Let 85 be the median value of the block. The binary of 85 is

1010101. Secret bit ‘**1**’ is embedded onto the fourth LSB of 85. So the embedded coefficient is now 93(1011**1**101). Figure 2d shows the embedded coefficients. Now the difference between source and embedded coefficients is 93-85=8. As next bit of embedded position is 1, flip all bits right to embedded bit to zero to minimize the difference. Handled Embedded pixel is 1011**000**=88. Now the difference (88-85 = 3) is minimized. Figure 2e shows the GA based handling called New Generation. The New Generated block is back to spatial domain using inverse Z Transform by equation 3 shown in Figure 2f. Crossover followed by Mutation is applied to minimize the difference. For Crossover operation rightmost 3 bits from each byte from the New Generated image is taken. A consecutive bitwise XOR is performed on it for the 3 steps. It will form a triangular form and first bit from each step is taken. For example last three bits of “20” are “100”. After applying Crossover bit stream will be “111”. Figure 2g shows the result of Crossover. Mutation is performed between two consecutive byte of the mask. As a result last two LSBs of two consecutive bytes are swapped. Figure 2h shows the result of Mutation. Final stego image mask is almost closer to the source image mask. So using Genetic Algorithm the quality of the stego image is improved.

10100110 Figure 2a: Bits of Jet Image	10 25 30 20 Figure 2b: Source Image Lenna	85 -20-5J -5 -20+5J Figure 2c: Source image Lenna after ZT	93 -20-5J -5 -20+5J Figure 2d: Embedded Image Block
88 -20-5J -5 -20+5J Figure 2e: Embedded Image Block after New Generation	10 26 30 20 Figure 2f: Stego Image Block after IZT	10 26 29 23 Figure 2g: Stego Image Block after Crossover	10 26 31 21 Figure 2h: Stego Image Block after Mutation

Figure 2: Encoding process of GAIAZT

3. Results and Comparison

Extensive analysis has been made on various images[16] using GAIAZT technique. This section represents the results and comparison in terms of visual interpretation and peak signal to noise ratio. Four benchmark images Lenna, Baboon, Pepper and Jet are taken from image database. Figure 3a shows the source images Lenna, Mandrill, Pepper. Figure 3b shows embedded Lenna, Mandrill, Pepper on embedding Jet image using GAIAZT. Figure 3c is the authenticating image Jet. Jet image is embedded onto the source images in fourth LSB of each median of the mask. From the figure 3 it is clear that image fidelity is intact for embedded images. A set of benchmark images are taken [16] from which some of the result is given following. Three tests are performed to know the efficiency such as Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE) and Image Fidelity (IF). PSNR, MSE and IF values for each embedding against the source image are shown in Table I. Table II compare with existing [1]. The following formulas are used to calculate PSNR, MSE and IF (image fidelity).

$$PSNR = 10 \log\left(max\left(I_{m,n}{}^{2}\right)/MSE\right)$$

$$MSE = \frac{1}{MN} * \sum_{m,n} (I_1\, m,n - I_{\,2}m,n)^2$$

$$IF = 1 - \sum_{m,n}(I_{1_{m,n}} - I_{2_{m,n}})^2 \,/ \sum_{m,n} I_{2_{m,n}}^{2}$$

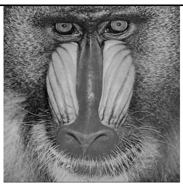
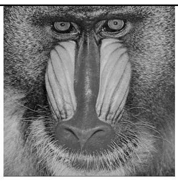
 3.a.i. Host Lenna	 3.a.ii.Host Mandrill	 3.a.iii Host Peppers
 3.b.i.Embedded Lenna	 3.b.ii Embedded Mandrill	 3.b.iii Embedded Peppers
 3.c.i. Hidden Jet	FIGURE 3:VISUAL EFFECT OF EMBEDDING IN GAIAZT	

Table I PSNR, MSE, IF values obtained for various images using GAIAZT

Host Image	**PSNR values**	**MSE Values**	**IF**
Lenna	45.677792	1.759144	0.999891
Baboon	45.717030	1.743320	0.999907
Peppers	45.659969	1.766376	0.999901
Boat	45.020523	2.046577	0.999892
Cameraman	44.113602	2.521854	0.999860
Elaine	45.707283	1.747238	0.999916
Sailboat	45.744381	1.732376	0.999915
Zelda	41.502254	4.601028	0.999057
Average	44.89285	2.239739	0.999792

Table II Comparison of PSNR values between GAIAZT and existing[1]

Host Image	***PSNR values of GAIAZT***	***Capacity of GAIAZT***	***PSNR values of existing[1]***	***Capacity of existing [1]***
Jet	45.656765	25088	31.49	24568
Lenna	45.677792	25088	31.56	24569
Mandrill	45.717030	25088	28.75	24526
Pepper	45.659969	25088	32.14	24575
Zelda	41.502254	25088	33.00	24575
Boat	45.020523	25088	31.17	24435

4. Discussion

Z Transform is a sensitive transformation and it generates two imaginary coefficients in transformed domain. The median imposes another level of security. The position is chosen in such a way that the information is correctly extracted. Three extensive analysis has been made of which PSNR is an approximation to human perception of reconstruction quality, a higher PSNR generally indicates that the reconstruction is of higher quality. Image fidelity refers to the ability of a process to render an image accurately, without any visible distortion or information loss. From the table it is seen that the average value of PSNR is 44.89285 which conform good image quality. Average IF value is 0.999792 which is nearer to 1. From experimental results it is clear that the proposed technique obtained consistent PSNR along with good image fidelity for various images which conform that Z-transformed based image steganography can obtain better visibility/quality.

5. Conclusion

The proposal is a novel embedding approach termed as, GAIAZT based on Z Transformation for gray scale images where concept of median has been used to select the coefficient for embedding in Z-Transformed domain. From experimental results it is clear that the proposed technique obtained consistent PSNR ratio along with good image fidelity for various images which conform that Z-transformed based image steganography can obtain better visibility/quality. Payload may be increased considerably which is the future scope of the paper and hence research in Z-Domain.

Acknowledgement

The authors express deep sense of gratitude to the department of CSE, and DST PURSE Scheme of University of Kalyani, India where the computational works have been carried out.

References

1. Chang C et al “Reversible hiding in DCT- based compressed images”, ScienceDirect Information Science vol :177, July 2007 Pages: 2768-2786.
2. Lifang Yu et al “Improved Adaptive LSB steganography based on Chaos and Genetic Algorithm” , European Association for Signal Processing (EURASIP) Journal on Advances in Signal Processing, volume 2010, Article ID 876946.
3. Ghoshal N., Mandal, J. K. et al., “Image Authentication by Hiding Large Volume of Data and Secure Message Transmission Technique using Mask (IAHLVDSMTTM)”, Proceedings of IEEE International Advanced Computing Conference (IACC 2009), ISBN:978-981-08-2465-5, March 6-7th, Thapar University, Patiala, India.

4. Ghoshal N., Mandal, J. K. et al., “Masking based Data Hiding and Image Authentication Technique (MDHIAT)”, Proceedings of 16th International Conference of IEEE on Advanced Computing and Communications (ADCOM-2008), ISBN: 978-1-4244-2962-2, December 14-17th, Anna University.
5. Ghoshal N., Mandal, J. K. “A Novel Technique for Image Authentication in Frequency Domain using Discrete Fourier Transformation Technique (IAFDZTT)”, Malaysian Journal of Computer Science, ISSN 0127-9094, Vol. 21, No. 1, pp. 24-32, 2008.
6. Ghoshal N., Mandal, J. K. “A Bit Level Image Authentication / Secrete Message Transmission Technique (BLIA/SMTT)”, Association for the Advancement of Modelling and Simulation Technique in Enterprises (AMSE), AMSE journal of Signal Processing and Pattern Recognition, Vol. 51, No. 4, pp. 1-13, France, 2008.
7. Nameer N. EL-Emam, “Hiding a large Amount of data with High Security Using Steganography Algorithm,” Journal of Computer Science ISSN 1549-3636, vol. 3, no. 4, pp. 223-232, 2007.
8. Rechberger C., Rijman V. and Sklavos N., “The NIST cryptographic Workshop on Hash Functions,” IEEE Security and Privacy, vol. 4, pp. 54-56, Austria, Jan-Feb 2006.
9. Pavan S., Sridhar G. and Sridhar V., “Multivariate entropy detector based hybrid image registration algorithm,” IEEE International Conference on Acoustics, Speech and Signal Processing, Philadelphia, Pennsylvania, USA, pp. 18-23, March 2005.
10. Hashad A. I. et al “A Robust Steganography Technique using Discrete Cosine Transform Insertion”, Information and communications Technology, 2005. Enabling Technologies for the New Knowledge Society: ITI 3rd International Conference.ISBN:0-7803-9270-1, 2005.
11. Moulin P. and O’Sullivan J. A., “Information-theoretic analysis of information Hiding,” IEEE Transaction On Information Theory, vol. 49, no. 3, pp. 563-593, March 2003.
12. Ghoniemy S. et al “Robust and Large Hiding Capacity Steganography using Spread Spectrum and Discrete Cosine Transform”, International Journal of Image Processing and Visual Communication ISSN (Online) 2319-1724 : Volume 1 , Issue 4 , February 2013.
13. Chandramouli R. and Memon N., “Analysis of LSB based image steganography techniques,” Proceedings of International Conference, Vol: 3, pp. 1019- 1022, Thessaloniki, Greece, 2001.
14. Wang S. et al. “A Secure Steganography Method based on Genetic Algorithm” , Journal of Information Hiding and Multimedia Signal Processing, ISSN 2073-4212, Ubiquitous International Volume 1, Number 1, January 2010.

15. Ataby A et al. “ A Modified High Capacity Image Steganograpy Technique Based on Wavelet Transform”, The International Arab Journal of Information Technology, vol 7 No 4, October 2010.

16. Weber A. G., The USC-SIPI Image Database: Version 5, Original release: October 1997, Signal and Image Processing Institute, University of Southern California, Department of Electrical Engineering. http://sipi.usc.edu/database/(Last accessed on 20th January, 2011).