An Image Authentication Technique in Frequency Domain using Genetic Algorithm (IAFDGA)

J. K. Mandal[1], A. Khamrui[2]

[1]Dept. of Computer Science and Engineering, University of Kalyani, Kalyani, Nadia-741235
jkm.cse@gmail.com
[2]Dept. of Computer Science and Engineering, Future Institute of Engineering and Management,
Sonarpur Station Road, Sonarpur, Kolkata-150, West Bengal,
amritakhamrui@rediffmail.com

ABSTRACT

In this paper Genetic Algorithm based image authentication technique in frequency domain using Z transformation (IAFDGA) has been proposed. A 2×2 mask is taken from the source image in row major order. Z transformation is applied to transform it into frequency domain. Six bits are embedded in each sub mask into the second and third transformed coefficients. The sub mask is then transformed into spatial domain using inverse Z transform. Embedded image mask of size 32 bits are taken as initial population. New Generation followed by Crossover and Mutation are applied on it. To obtain New Generation , minimum coefficient of the mask is chosen, if the minimum coefficient is negative then subtract the minimum coefficient from each coefficient of the mask so that extraction of hidden bits are ensured. For the Crossover operation consecutive bit-wise XOR is performed on the rightmost three bits of each byte in three steps. It will form a triangular form and the first bit of each step is taken as the output. Right most two LSBs of two consecutive pixels are swapped with each other as a part of Mutation operation. Genetic algorithm is applied to enhance a layer of security level. At the time of embedding dimension of the authenticating image followed by the content are embedded. Reverse process is followed at the time of extraction. High PSNR obtained for various images compared to existing Chin-Chen Chang et al.[2] conform the quality of invisible watermark IAFDGA. Large capacity as compared to existing algorithm [1] ensured the high payload of the scheme.

KEYWORDS

Frequency Domain, Steganography, peak signal to noise ratio (PSNR), Z Transform (ZT), Genetic Algorithm, Image Fidelity (IF).

1. INTRODUCTION

Data security is the most important thing now days. Data security can be achieved by hiding data into various natural cover data like sound, images, logos etc. Embedded data is referred to as stego-data and it must be embedded in such a way that the fidelity of the cover image is kept intact [4], [8], [13], [14], [15]. Message may be hidden invisible way [5], [6]. Information hiding [4] is a way to authenticate image. Authentication is major task for military people, researchers etc. Image authentication and information security is very important thing to protect digital document from unauthorized access [3]. An example of steganography is the prisoner communicating with the outside world under the supervision of prisoner warden. To ensure another layer of security and make the extraction impossible for the intruder the Genetic

DOI : 10.5121/ijaia.2013.4206

Algorithm is used. The aim is to hide the message/ image by keeping the image fidelity high [9]. The most common method is LSB substitution [9] through masking, filtering and transformation of the source image [7]. In this paper an image authentication and data hiding technique has been proposed. Most of the previous work [12], [11], [1], [2], [10] uses minimum bits for hiding but the present algorithm has high capacity with minimum/undetectable change of the visibility.
Rest of the paper is organized as follows. Section 2 deals with the proposed technique. Results and comparisons are given in section 3. Concluding remarks are presented in section 4 and references are drawn at end.

2. THE TECHNIQUE

A 2×2 sub mask is taken in row major order from the host Gray scale image in recursive manner and Z transformation is applied on it to transform it into frequency domain. In each sub mask six bits are embedded in second and third transformed coefficients. In the second coefficient second, third and fourth LSB is chosen for embedding where as in the third coefficient positions are third, fourth and fifth. Embedding position is chosen in such a way that during reverse transform there is no loss of precision. Identical embedding with same information is done in second and fourth coefficient so that the effect of algebraic addition of complex conjugate during reverse transformation is nullified. Inverse Z transformation is performed to transform the embedded image mask from frequency to spatial domain. Resulting image mask of size 32 bit is taken as initial population. New Generation followed by Crossover and Mutation are applied on it. In New Generation operation find out the minimum coefficient of the mask, if it is less than zero then subtract the minimum coefficient from each of the element of the mask otherwise skip these step. New Generation is applied to keep high image fidelity and to avoid in generating negative pixel during reverse transform. In Crossover operation rightmost three bits of each byte is taken, a consecutive bitwise XOR is performed on three steps, it will form a triangular form and the first bit of each step is taken as the output. Mutation operation is performed on the rightmost two bits of each byte, as a result the rightmost two bits of each byte are swapped with each other. Crossover and Mutation are performed in reversible way. Genetic Algorithm is applied to increase another layer of security without changing the image fidelity.
The formula for Z- Transform is

$$X(z) = \sum_{m=0}^{\alpha} x(m)\, r^{-m} e^{-j\omega n}$$ (limit is taken 0 to α as pixel value cannot be negative for an image)

In the present implementation the value of r is taken as 1 and ω varies between $0 <= \omega <= 2\pi$. For a 2×2 sub image there are four pixel values in the mask and set of frequencies taken are: $\omega = \{ 0, \pi/2, \pi, 3\pi/2\}$.

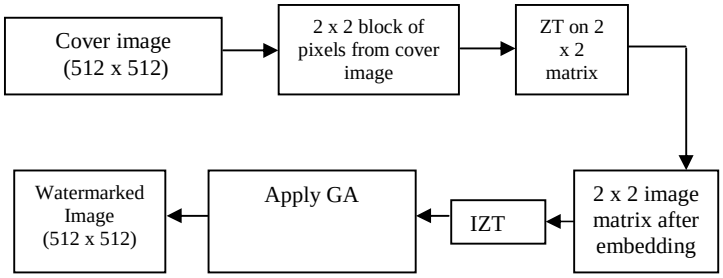


Figure.1.1: The process to embed the Secret data into the source image

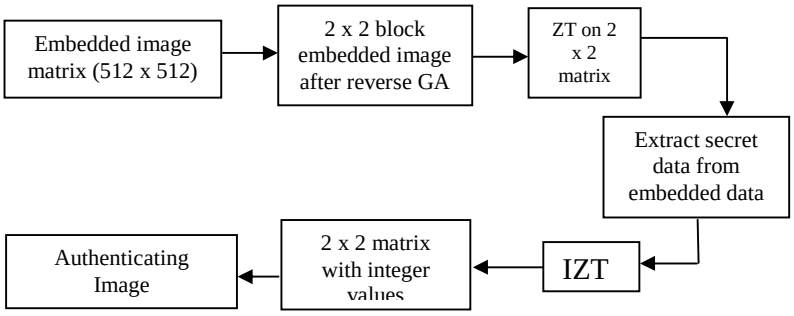


Figure. 1.2: The process to extract Secret data from the watermarked image
Figure 1: Schematic diagram of IAFDGA

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 -∞ to + ∞ and n1 and n2 is finite and positive numbers. In case of present implementation ω ranges between 0 to3π/2 and n1 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. Authenticating image of size m×n is chosen. Six bits of authenticating image are embedded in each mask of transformed coefficients in Z-domain followed by Genetic Algorithm to increase another layer of security without changing visibility.

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 bit-wise into the gray scale image.

1. Obtain the size of the authenticating image m×n
2. Read source image mask of size 2×2 in row major order. Apply Z-Transform onto (2×2) to generate transformed coefficients
3. Embed secret bits onto the second, third and fourth LSB position of the second coefficient of 2 x 2 mask. For embedding secret bits the dimension of the authenticating image followed by the content are embedded
4. Embed secret bits onto the third, fourth and fifth LSB position of the third coefficient of 2 x 2 mask
5. Copy second embedded coefficient onto fourth coefficient of the mask
6. Apply Inverse Z-Transform to transform the mask to spatial domain
7. 2×2 embedded image mask of size 32 bits are taken as initial population. Perform New Generation operation on the initial population. Obtain the minimum coefficient of the embedded image mask. If minimum is negative then subtract magnitude of minimum from each coefficient otherwise do nothing
8. Crossover is applied onto each New Generated mask. A consecutive bit-wise XOR is performed on rightmost three LSBs of each mask in three steps and the first bit of each step is taken as output.
9. For Mutation operation rightmost two LSBs of the consecutive two pixels of each mask are swapped
10. Repeat step 2 to 9 for the whole cover image
11. Stop.

2.2. Extraction Algorithm

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

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.

1. 2×2 mask of the embedded image is taken in row major order. For reverse Mutation operation rightmost two LSBs of two consecutive pixels of each mask are swapped.
2. Reverse Crossover is performed through consecutive bit-wise XOR operation on the rightmost 3 LSBs of each reverse mutated pixel in three steps. The first bit of each step is taken as the output
3. Apply Z-Transform onto the reverse crossover image mask to transform into frequency domain
4. Extract the authenticating bits from the second, third and fourth LSB of the second coefficient of the 2×2 mask. Replace authenticating message/ image bit position in the block by '1'. For each eight extracted bits construct one image pixel of authenticating image

5. Extract the authenticating bits from the third, fourth and fifth LSB of the third coefficient of 2×2 mask. Replace authenticating message/ image bit position in the block by '1'. For each eight extracted bits construct one image pixel of authenticating image
6. Repeat step 1 to 5 to regenerate authenticating image as per size of the authenticating image
7. If the extracted image and embedded authenticating image are same then the document is authentic
8. Stop.

2.3. Example

Consider bits of Jet image (figure 2a) to be inserted into each mask of Lenna image (Figure 2c). Figure 2b shows pixels of Lenna image in spatial domain. Six bits of the Jet image are inserted into the Lenna image in 2×2 mask. Insertion is done in the second coefficient of each mask on second, third and fourth LSB bits and third coefficient on third, fourth and fifth LSB bits of the byte of Lenna. Resultant image after embedding is shown in Figure 2d in frequency domain and Figure 2e in spatial domain. Figure 2f shows New Generation. Figure 2g and 2h shows Crossover and Mutation.

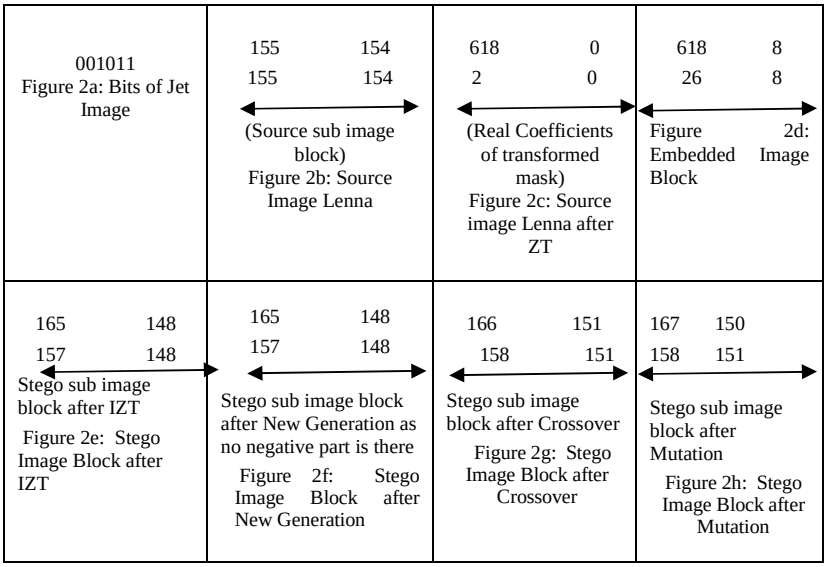


Figure 2: Encoding Process Of Iafdga

3. Results Comparison and Analysis

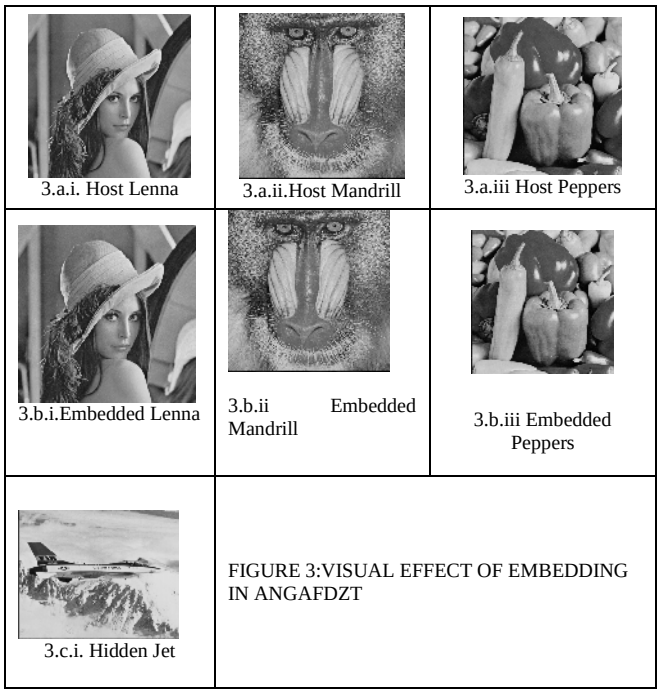
Analysis of result has been made on various images taken from image database [16] using IAFDGA technique in terms of visual interpretation, PSNR, MSE and IF. Figure 3a shows the host images Lenna, Mandrill, Peppers. Figure 3b shows embedded Lenna, Mandrill, Peppers on embedding Jet image using IAFDGA. Figure 3c is the authenticating image Jet. Table I shows the PSNR value for each embedding against the source image.

From the table it is seen that the maximum value of the PSNR is 39.245163 and that of minimum value of the PSNR is 38.373398. Table II shows the comparison of PSNR values and capacity of the proposed technique and the existing Mandal J. K. et al [1] and Chin-Chen Chang et al.[2]. In comparison with existing [1] it is seen that the proposed technique has higher patload compared to the existing [1]. In comparison with existing [2] it is seen that the proposed technique has higher capacity and better PSNR compared to the existing [1]. The maximum capacity of the existing [1] is 216000 and existing [2] 36850 is where as the maximum capacity of the proposed technique is 393210. The average value of PSNR for the proposed technique is 38.85 which is much higher than the existing [2] average value 29.43. The following formula 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 ANGAFDZT

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

Host Image	PSNR values	MSE Values	IF
Lenna	38.879440	8.416592	0.999476
Mandrill	39.245163	7.736851	0.999585
Peppers	38.937149	8.305492	0.999534
Elaine	39.127232	7.949818	0.999616
Sailboat	38.903732	8.369648	0.999590
Boat	38.843693	8.486160	0.999553
Jet	38.373398	9.456718	0.999724

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

Host Image	PSNR values of IAFDGA	Capacity of IAFDGA	PSNR values of EXISTING [1]	capacity EXISTING [1]	PSNR values of EXISTING [2]	Capacity of EXISTING [2]
Lenna	38.879440	393216	40.917221	216000	30.34	36850
Mandrill	39.245163	393216	40.973183	216000	26.46	35402
Peppers	38.937149	393216	40.942974	216000	30.65	36804
Boat	38.843693	393216	40.943676	216000	29.75	36710
Jet	38.373398	393216	40.927849	216000	29.98	36817

4. CONCLUSIONS

The paper proposed an image authentication technique in frequency domain using Genetic Algorithm termed as IAFDGA based on Z Transformation for gray scale images. This paper shows that the proposed technique has higher capacity compared to existing approach Mandal J. K. et al. [1] and better PSNR compared to Chin-Chen Chang et al.[2] without altering the fidelity.

ACKNOWLEDGEMENTS

The authors express deep sense of gratitude to the IIPC Project of AICTE, of the department of CSE, University of Kalyani, India where the computational works have been carried out.

REFERENCES

[1] Mandal J. K. And Khamrui A et al "A Novel Genetic Algorithm based Data Embedding Technique in Frequency Domain using Z Transform", The Second International Conference on Advances in Computing and Information Technology (ACITY) July 13-15,2012 Chennai, India- Volume 2, ISBN 978-3-642-31551-0, Pages: 885-893.

[2] Chin-Chen Chang et al "Reversible hiding in DCT- based compressed images", ScienceDirect Information Science vol :177, July 2007 Pages: 2768-2786.

[3] R. Radhakrishnan, M. Kharrazi, N. Menon, "Data Masking: A new approach for steganography" Journal of VLSI Signal Processing, Springer, Vol. 41, pp. 293-303, 2005.

[4] P. Amin, N. Lue and K. Subbalakshmi, "Statistically secure digital image data hiding" IEEE Multimedia Signal Processing MMSP05, pp. 1-4, Shanghai, China, Oct. 2005.

[5] A. H. Al-Hamami and S. A. Al-Ani "A New Approach for Authentication Technique", Journal of computer Science, ISSN 1549-3636, Vol. 1, No. 1, pp. 103-106, 2005.

[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] C. Rechberger, V. Rijman and N. Sklavos, "The NIST cryptographic Workshop on Hash Functions," IEEE Security and Privacy, vol. 4, pp. 54-56, Austria, Jan-Feb 2006.

[9] S. Pavan, S. Gangadharpalli and V. Sridhar, "Multivariate entropy detector based hybrid image registration algorithm," IEEE Int. Conf. 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 communication Technology, 2005. Enabling Technologies for the New Knowledge Society: ITI 3rd International Conference.ISBN:0-7803-9270-1.
[11] P. Moulin and J. A. O'Sullivan, "Information-theoretic analysis of information Hiding," IEEE Trans. On Info. Theory, vol. 49, no. 3, pp. 563-593, March 2003.
[12] S. Dumitrescu, W. Xiaolin and Z. Wang, "Detection of LSB steganography via sample pair analysis," IEEE Trans. on Signal processing, Vol. 51, no. 7, pp. 1995-2007, 2003
[13] R. Chandramouli and N. Memon, "Analysis of LSB based image steganography techniques," Proc. of ICIP, Thissaloniki, pp. 1019- 1022, Greece, 2001.
[14] Ran-Zan Wang, Chi- Fang Lib, and Ja- Chen Lin, "Image hiding by optimal LSB substitution and Genetic algorithm," 2001 Pattern Recognition Society. Published by Elsevier Science Ltd.
[15] C.Y. Lin and S. F. Chang, "A robust image authentication method surviving JPEG lossy compression," Proc. SPIE, vol. 3312, San Jose, pp. 296-307, Jan. 1998.
[16] Allan G. Weber, 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).

Authors

Amrita Khamrui, (M. Tech in Computer Science & Engg) is an Asst. Prof of Future Institute of Engineering & Management, Kolkata. She is doing her research work in University of Kalyani. She has seven years of teaching and four years of research experience. She has five publications in international conference and two publications in international journal.

Jyotsna Kumar Mandal, M. Tech.(Computer Science, University of Calcutta),Ph.D.(Engg., Jadavpur University) in the field of Data Compression and Error Correction Techniques, Professor in Computer Science and Engineering, University of Kalyani, India. Life Member of Computer Society of India since 1992 and life member of cryptology Research Society of India. Dean Faculty of Engineering, Teachnology & Management, working in the field of Network Security, Steganography, Remote Sensing & GIS Application, Image Processing. 25 years of teaching and research experiences. Eight Scholars awarded Ph.D. one submitted and eight are pursuing. Total number of publications is more than two hundred thirty in addition of publication of five books from LAP Lambert, Germany.