International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Discrete Z Transformation based Copyright Protection on Digital Image Using Genetic Algorithm

Prashant C. Harne[1], Rajesh K. Nigam[2]

[1, 2]Department of Computer Sci. & Engineering, Technocrats Institute of Technology & Science,
Anand Nagar, Bhopal, Madhya Pradesh, India

Abstract: ***Today, due to the outburst of exchanging digital images worldwide on the internet and the extensive use of digital media it is necessary to show keen interest in multimedia copyright protection. The aim is to propose a secure algorithm for protecting digital image as copyright using digital watermarking approach. Now day's concept of digital watermarking scheme has attracted research scholars in the emergent areas of digital watermarking security and digital image authentication as a copyright protection. Digital Watermarking is an effectual solution for protecting intellectual property of image, audio and video data. The watermark should be produced in such a way that it is independently and identically distributed. The robustness and fidelity play predominant role during the process of digital watermarking. Robustness is nothing but potency of the watermarking against various image processing attacks and fidelity concern for the original quality of image after embedding the watermark. So in order to gain these features the concept of Discrete Z Transform and Genetic Algorithm is applied.***

Keywords: Copyright Protection**,** Digital Watermarking, Discrete Z Transform, Fidelity, Genetic Algorithm, Robustness.

1. Introduction

A watermark is a recognizable image or pattern in paper that appears as various shades of lightness or darkness when viewed by transmitted light caused by thickness or density variations in the paper. It is the process of embedding information into a digital signal in such a way that is difficult to remove. In this process the modification of the original multimedia data to embed a watermark containing key information such as authentication or copyright codes.

According to the domain in which the watermark is inserted, these techniques are divided into two broad categories: spatial-domain and frequency-domain. Embedding the watermark into the spatial-domain component of the original image is the straightforward method. It has the advantages of low complexity and easy implementation. However, the spatial-domain watermarking algorithms are generally fragile to image processing operations. On the other hand, the representative frequency-domain techniques embed the watermark by modulating the magnitude of coefficients in a transform domain, such as Discrete Cosine transform (DCT), Discrete Fourier Transform (DFT), and Discrete Wavelet Transform (DWT). Although frequency-domain methods can yield high capacity payload and more robustness against many common attacks, the computational cost is higher than spatial-domain watermarking methods.

The embedded data should preserve the quality of the host signal after watermarking. Basic requirements for watermarking generation are Robustness, Imperceptibility, Security and Capacity.

The Discrete Z-Transform (DZT) domain is convenient yet invaluable tool for representing, analyzing, and designing discrete time signals and systems. The locations of Zeroes of the Z transforms are very susceptible to any pixel value change. It has the advantage of easy implementation and pixel wise sensitivity to external tampering. Moreover, it provides better data hiding security protection than the normal LSB check-sum fragile watermarking scheme.

In this paper an innovative image watermarking scheme by integrating DZT and GA is introduced, the proper scaling factors are determined by the GA. Generally the strength of the embedded watermark can be controlled by a scaling factor. The performance of the watermarking process highly depends on choosing a proper scaling factor. It is found that the scaling factor is set to be constant in some SVD-based studies. But some argued that considering a single and constant scaling factor may not be applicable in some cases and suggest users can use multiple scaling factors instead of one.

2. Motivation

We seem to have reached a plateau in technology for many copyright protection problems where break through paradigm changes are necessary for further development and for this purpose we need to ask again and again ourselves the fundamental question try to find gaps in our understanding multimedia security using Genetic Algorithm phenomenon to have access to the unused information available in our data.

The motivation behind proposing such type of work is to pull out the utilization of Discrete Z- Transformations and Genetic Algorithm in the applications of Digital Image Processing and Soft Computing. The concept of GA is not new in the case of multimedia security and may be used to enhance a layer of security level as well as to search the proper values in order to improve the visual quality of the watermarked image and the robustness of the watermark. Also the concept of Discrete Z- Transforms is not new as compared to Discrete Fourier Transforms, Discrete Cosine

Transforms, Discrete Wavelet Transforms and Single Value Decomposition in the case of frequency-domain but we have to enhance the power of it in various application areas.

3. Literature Survey

According to Chih-Chin Lai. et. al. [1]-[3] the hybrid of Discrete Wavelet Transform and Singular Value Decomposition is best for preserving robustness and imperceptibility of digital image. In their work watermark is not embedded on the wavelet coefficients but it is embedded on the elements of singular values of host image's wavelet sub bands. And they are also confident that this type of combination has ability to tackle with most of the image processing attacks. Their proposed logic shows both the significant improvement in imperceptibility and the robustness as compared to previous work.

According to Mohd. Sherfuddin Khan. et. al. [7] Z-transform is resistant to various image processing attacks. Authors supposed that it is not necessary for the original image to be available for detecting the watermark. Performance and robustness of the proposed technique is tested by using basic image processing attacks like filtering, requantization and JPEG compression.

J K Mandal et. al.[8] proposed an Image Authentication Technique in frequency Domain using Genetic Algorithm. a 2×2 sub mask is taken from the host image in recursive manner and Discrete Z-transform is applied on it to transform it into frequency-domain. In each sub mask six bits are embedded in 2^{nd} and 3^{rd} transformed coefficients. In the 2^{nd} coefficient 2^{nd} , 3^{rd} and 4^{th} LSB is chosen for embedding where as in the 3^{rd} coefficient positions are 3^{rd} , 4^{th} and 5^{th}. Embedding position is chosen in such a way that during reverse transform there is no loss of precision. Inverse Z-transform 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 operations 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 frequency domain first time Z-transform and Genetic Algorithm is applied so it enhances the security level and large capacity as compared to existing algorithm that ensures the high payload of the scheme. But this algorithm increases the complexity because redundant coefficient strategy is used.

A new proposal by Chih-Chin Lai.et. al. [4]_suggests us to show keen interest in Digital image watermarking scheme in frequency-domain based on Singular Value Decomposition (SVD) and a Tiny Genetic Algorithm (Tiny-GA). The outputted singular values are very stable and vary very small amount under most of the image processing attacks. In this proposed scheme, the singular values of a cover image are modified by multiple scale factors to embed the watermark image. They used the Tiny-GA to search the proper values in order to improve the visual quality of the watermarked image and the robustness of the watermark.

According to S.M. Ramesh. et. al. [5] performance of the watermarking algorithms is analyzed using different compression standards. Authors discussed several techniques that were presented in the literature for robust watermarking algorithm to defend against the various JPEG compression methods and presented comparison and analysis of recently developed watermarking algorithms. Then an extensive analysis is carried out to estimate and compare robustness of watermarking algorithms by considering the visual quality and fidelity of the original and watermarked images in terms of PSNR. Furthermore, the extracting fidelity (imperceptibility) of the watermarking algorithms is compared by taking the Normalized Correlation value between the original watermark and the extracted watermark. The NC values are computed for different compression ratios of JPEG compression and the values are plotted as a graph for the considered algorithms.

V. Naveen Kumar. et. al.[2] suggested that if patient's information is embedded into a medical image using lossless code for improving the level of security and confidentiality that is essential for distribution of medical information system. This security and confidentiality provides integration of medical images with corresponding documentations along with protection of confidential information. The scheme's imperceptibly embeds in medical images patient's personal information like name and unique identification number. The main objective is to develop a simple model which uses minimum resources for data hiding and hence a strong candidate for this is mobile healthcare applications where the resources of memory, computation and connectivity are extremely limited.

D. Venkatesan. et. al.[6] focused on operator named Center of Mass Selection Operator of genetic algorithm approach to find the optimum pixel locations for embedding digital watermark in host image. Various methods of spatial and frequency domain faced the problem of poor fidelity.

4. Existing System

In the case of digital image watermarking, employing special characteristics is essential for ensuring immunity to geometric transformations. When a watermark is inserted on the entire image, scaling, rotation or cropping will result in the destruction of the watermark because no reference points exist that would lead in finding in the amount of scaling, rotation, or cropping. The use of an image transform, with the exception of the Fourier transforms, will suffer the same problem. The Fourier transform is theoretically rotation, translation, and scale invariant, but the robustness to filtering or compression depends on the range of frequencies that are used for watermarking. Discrete Z-transform based image watermarking technique is proposed and analyzed that Z-transform is resistant to various image processing attacks. Authors persuaded that it is not necessary for the original

image to be available for detecting the watermark. Performance and robustness of the proposed technique is tested by using basic image processing attacks like filtering, requantization and JPEG compression. In frequency domain there has been some work done by the various transforms like DCT, DFT, and DWT. If we are comparing the results of those last systems, they are providing watermarking by using these transforms but there is lack of the obscure images clarity. So we are trying to do the same work by means of DZT which will assure the integrity of image and to sustain most of the Digital Image Processing attacks.

In existing system Discrete Z-transform based image watermarking technique [7] is available where Z-transform is resistant to various image processing attacks. Here it is not essential for the original image to be available for detecting the watermark. However it does not modify the host image therefore it is suitable for the applications which the modification of the image is not allowed.

Again J K Mandal. et. al. [8] introduced a method based on Discrete Z Transforms i.e. a 2×2 sub mask is taken from the host image in recursive manner and DZT is applied on it to transform it into frequency-domain. In each sub mask six bits are embedded in 2^{nd} and 3^{rd} transformed coefficients. In the 2^{nd} coefficient 2^{nd} , 3^{rd} and 4^{th} LSB is chosen for embedding where as in the 3^{rd} coefficient positions are 3^{rd} , 4^{th} and 5^{th}. Embedding position is chosen in such a way that during reverse transform there is no loss of precision. Inverse Z-transform 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.

Also Chih-Chin Lai.et. al. [4]_recommended that Digital image watermarking scheme in frequency-domain based on Singular Value Decomposition (SVD) and a Tiny Genetic Algorithm (Tiny-GA). The resulted singular values are very stable and vary very small amount under most of the image processing attacks.

In this existing scheme, the Tiny-GA is used to search the proper values in order to get better the visual excellence of the watermarked image and the robustness of the watermark. It is nothing but Lightweight Evolutionary Algorithm which requires small efforts as compared to GA. Tiny-GA is used to systematically determine pixel values of transform domain coefficient without making any assumption, However determining the proper values of multiple scaling factors is a difficult problem, especially for different types of cover and watermark images.

5. Proposed System

The proposed system is developed by integrating Discrete Z Transforms with Genetic Algorithm. The reason behind proposing such type of hybrid is to preserve the robustness and fidelity of the image. The robustness and fidelity play predominant role during the process of digital watermarking as copyright protection. Robustness is nothing but strength of the water marking against various image processing attacks and fidelity concern for the original quality of image after embedding the watermark.

The *z*-transform of sequence $x(n)$ is defined by

$$\text{Let } z = e^{-j\omega} \quad X(z) = \sum_{n=-\infty}^{\infty} x(n) z^{-n}$$

$$X(e^{j\omega}) = \sum_{n=-\infty}^{\infty} x(n) e^{-j\omega n}$$

i.e. nothing but Fourier Transform .

In the given sequence, if the set of values of *z* for which the Z Transforms converges, i.e., $|X(z)| < \infty$, is called the Region of Convergence (ROC).

$$|X(z)| = \left| \sum_{n=-\infty}^{\infty} x(n) z^{-n} \right| = \sum_{n=-\infty}^{\infty} |x(n)|\,|z|^{-n} < \infty$$

Now,

$$X(z) = \frac{P(z)}{Q(z)}$$

where , P(z) and Q(z) are polynomials in z.

Zeros: The values of z's such that X(z) = 0

Poles: The values of z's such that X(z) = ∞

5.1 Algorithm

1) Take Host Image (I) as input.
2) Then I, is divided into non overlapping blocks of size n*n. where, n is must be even positive integer. for e.g. 8*8=64 where n = 8 and it is positive integer. Then sub block this image row by row and each block is expressed as sequence of vectors.
3) Now make another image (W), as watermark as secret key using Genetic Algorithm.
4) The development of genetic algorithm is as follows:
   a. Produce an initial population of all individuals
   b. Evaluate the fitness of all individuals
   c. While termination condition is not met
   do
   Select filter individual for reproduction
   Recombine between individuals
   Evaluate the fitness of the modified individuals
   Generate new population
   End while
5) Then perform the Z transform and obtain:
   a. Z transformed image of Real Part
   b. Z transformed image of Imaginary Part
6) Now obtain Embedded Image by adding generated secret key with original Host Image
   i.e. Embedded Image =Generated Key + Host Image.
7) Calculate MSE, PSNR, MAE, RMSE and SR of the Host Image and Embedded Image, and the Embedding process is completed.
8) In Image Authentication process, we need the watermarked Image and the secret Key to identify the watermark.

9) The Image Authentication process also starts by dividing the image into small blocks of size n*n.
10) In every block, by applying the inverse Z transform to every row, we obtain the Zeros (i.e. the values of z's such that X (z) = 0).
11) And finally Calculate MSE, PSNR, MAE, RMSE and SR of the Host Image and Authenticated Image and then Authentication process is completed.

6. Result and Discussion

For results we took test.jpg (Figure 1) as Host Image and calculated MSE, PSNR, MAE, RMSE and SR with various types of Attacks like Gaussian noise, Salt and Pepper Noise and contrast also. Table 1 shows MSE, PSNR, MAE, RMSE and SR of Host Image (test.jpg) with various types of Attacks. Figures from 2 to 13 shows the results obtained in Matlab.

Figure 1: Host Image (test.jpg)

Table 1: MSE, PSNR, MAE, RMSE and SR of Host Image (test.jpg) with various types of Attacks

Host Image (Test.jpg)			MSE	PSNR	MAE	RMSE	SR
			0.443451	51.662348	0.449081	0.665921	0.999979
Type Of Attack	1	Gaussian Noise	0.007752	21.10598	0.070218	0.088045	0.968022
	2	Salt And Pepper	0.000062	42.092685	0.000087	0.007859	0.999742
	3	Contrast	7.398431	39.439407	0.002447	2.720006	0.999627

Figure 2: Host Image (RGB to GRAY)

Figure 3: Watermark to be Embedded

Figure 4: Key Generation Using Genetic Algorithm

Figure 5: Z-transformed Image Real Part

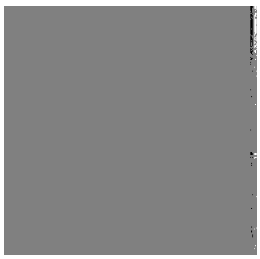

Figure 6: Z-transformed Image Imaginary Part

Figure 7: Watermarked Image

Figure 8: Watermarked Image with Key

Figure 9: Authenticated Image

Figure 10: Original Image and Gaussian Noise Image

Figure 11: Original Image and Salt Pepper Noise Image

Figure 12: Original Image and Contrast Image

Table 2 shows the PSNR values of Proposed and Existing Systems for various Host images.

Here we applied algorithm on 5 Host Images (Lena.jpg, Mandrill.jpg, Peppers, jpg, Boat.jpg, Jet.jpg) and calculated the PSNR (Peak Signal to Noise Ratio) values and we obtained the better results.

Table 2: Comparison of PSNR values among Proposed and Existing Systems [8] for various Host images

Sr. No.	*Host Image*	*PSNR values of Proposed system*	*PSNR values of IAFDGA system*	*PSNR values of Existing system*	*PSN values Existi syste*
		(in db)			
1	Lena	51.171885	38.879440	40.917221	30.3
2	Mandrill	50.419390	39.245163	40.973183	26.4
3	Peppers	51.662348	38.937149	40.942974	30.6
4	Boat	51.593954	38.843693	40.943676	29.7
5	Jet	51.662348	38.373398	40.927849	29.9

Following Figure13 shows Graphical Comparison of PSNR values among proposed and existing systems for various Host images.

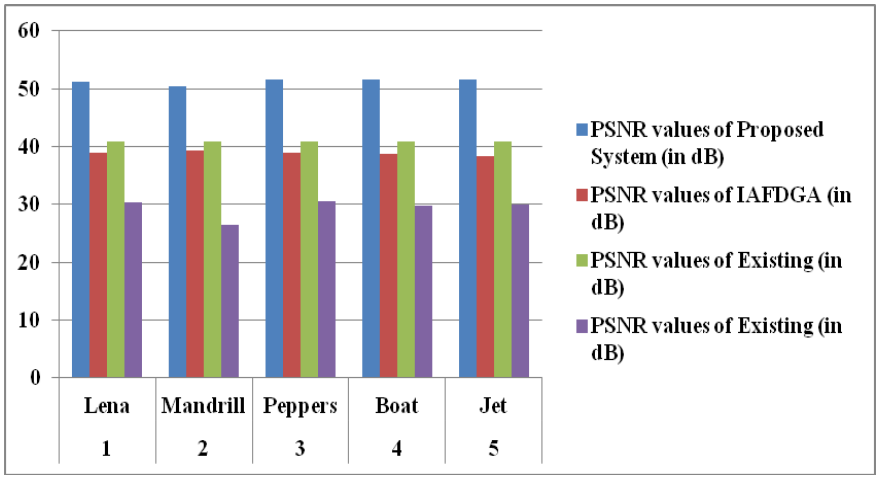

Figure 13: Graphical Comparison of PSNR values among proposed and existing systems [8] for various Host images

Following Table 3 shows MSE, MAE, RMSE and SR for Various Host Images, here we took 5 Host Images (Lena.jpg, Mandrill.jpg, Peppers, jpg, Boat.jpg, Jet.jpg) and calculated the MSE, MAE, RMSE and SR also. And following Figure14 shows Graphical Comparison of PSNR values among proposed and existing systems for various Host images.

Table 3: MSE, MAE, RMSE and SR for Various Host Images

Sr. No.	Host Image	MSE	MAE	RMSE	SR
1	Lena	0.443451	0.449081	0.665921	0.999999
2	Mandrill	0.443451	0.449081	0.665921	0.999999
3	Peppers	0.443451	0.449081	0.665921	0.999963
4	Boat	0.443451	0.449081	0.665921	0.999987
5	Jet	0.443451	0.449081	0.665921	0.999988

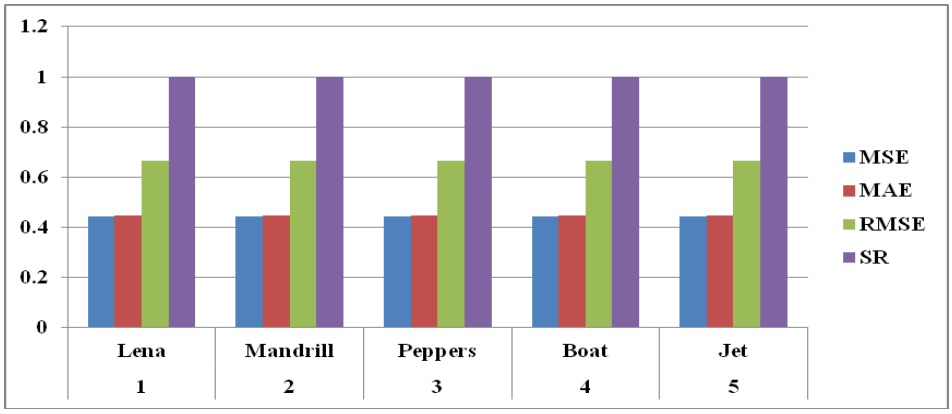

Figure 14: Graphical Representation of MSE, MAE, RMSE, SR for Various Host Images

7. Conclusion

Finally, we have concluded that if we integrate Discrete Z Transformation with Genetic Algorithm for Copyright Protection on Digital Image then it is more effective to sustain most of the Digital Image Processing attacks like Contrast, Gaussian Noise, Salt & Pepper Noise as compared to other Transformations.

References

[1] Chih-Chin Lai and Cheng-Chih Tsai **"**Digital Image Watermarking using Discrete Wavelet Transform and Singular Value Decomposition" IEEE TRANSACTIONS ON INSTRUMENTION & MEASUREMENT Vol. 59, 2010.

[2] V. Naveen Kumar, Mrigank Rochan, Santosh Hariharan, and Kumar Rajamani "Data Hiding Scheme for Medical Images using Lossless code for Mobile HIMS" IEEE**,** 2011.

[3] Chih-Chin Lai "A digital watermarking scheme based on singular value decomposition and tiny genetic algorithm", Elsevier Inc. (Science Direct Digital signal Processing) 2011, PP-522-527.

[4] Chih-Chin Lai, Chung-Hung Ko and Chih-Hsiang Yeh "A digital watermarking scheme based on singular value decomposition and tiny genetic algorithm", IEEE International Conference on Machine Learning and Cybernetics Vol. 4,15-17 July 2012, PP-1546-1551.

[5] S. M. Ramesh and Dr. A. Shanmugam **"**Comparison and Analysis of Discrete Cosine Transform based Joint Photographic Experts Group Image Compression using Robust Watermarking Algorithm" American Journal of Applied Sciences Vol. 8 (1), 2011, PP-63-70.

[6] D. Venkatesan, K. Kannan and S. Raja Bhalchandar "optimization of Fidelity in Digital Image Watermarking using a New Genetic Algorithm",Applied Mathematical Sciences, Vol. 6, 2012, PP-3607-3614.

[7] Mohd. Sherfuddin Khan, Ravi Boda, and Vijay Vamshi Bhukya **"**A copyright protection scheme and tamper detection using Z transform", International Journal of Computers, Electrical and Advanced Communications Engineering, Vol. 1, No.1, January 2012,PP- 119-124.

[8] J. K. Mandal, A. Khamrui, An Image Authentication Technique in frequency Domain using Genetic Algorithm**",** International Journal of Software Engineering & Applications**,** Vol.03, No.5**,** September 2012**,** PP-39-46.