International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 3 Issue: 3 962 - 964

Digital Watermarking using Tiny Genetic Algorithm and Discrete Z Transforms

Rinkey A. Aghicha
Department of Info.Tech
SSBT's COET, Bambhori,
Jalgaon, India
e-mail:raaghicha@gmail.com

Gunjan L. Behere
Department of Info.Tech
SSBT's COET, Bambhori
Jalgaon, India
e-mail:mayura101644@gmail.com

Pallavi A. Pati
Department of Info.Tech.
SSBT's COET, Bambhori
Jalgaon, India
email:pallavi744.patil@gmail.com

Mr. Prashant. C . Harne
Department of Info.Tech
SSBT's COET
Jalgaon, India
e-mail:harneprashant2k7@gmail.com

Abstract:-Today, multimedia data security plays most important role in internet era. Media elements like images, audios and videos are used to embed the data. As the digital media is tremendously growing over the internet, it is very inevitable to show interest in multimedia copyright protection. The aim to propose such a system is to provide secure algorithm for protecting digital image by using digital watermarking approach and extraction of that watermark from existing image to prove the authentication. Digital watermarking is solution for protecting intellectual property of image. To achieve features like robustness and imperceptibility of the image, concept of Discrete Z-Transform is used and for generation of key, Tiny Genetic Algorithm is used. Robustness and imperceptibility are important in digital watermarking process. We assure that the result will be better to sustain attacks like cropping, rotation, filtering and compression and embedded watermark will not be affected.

Keywords:-*Digital watermarking, Discrete Z-Transform, Frequency Domain, Imperceptibility, Robustness, Tiny Genetic Algorithm.*

*****

I. INTRODUCTION

A digital watermarking is the act to protect digital image from unauthorized copying and misuse. It is the process of embedding information into a digital signal in such a way that it can't be easy to remove. In this process, a watermark containing key information such as authentication or copyright codes is embedded by performing some modifications in the original multimedia data.

While using watermark, it is inserted according to the domain, these techniques are divided into two categories such as spatial domain and frequency domain. In the spatial domain, it is very straightforward technique to embed the watermark. It results in low complexity and easy implementation, but easy implementation will reduce the signal-to-noise ratio of the result image. The spatial domain watermarking algorithms are fragile to image processing operations. On the other hand, in the representative frequency-domain techniques, the input images are decomposed into multi-scale coefficient initially. In frequency domain, the watermark is embedded by modulating the magnitude of coefficients in a transform domain, such as, Discrete Fourier Transform, and Discrete Wavelet Transform. But we cannot embed too much data in the frequency domain because the quality of the host image will be lowered. That is, the size of watermark should be smaller than the host image. Frequency-domain methods results in high capacity payload and more robustness against many common attacks and the computational cost is much more than spatial-domain watermarking methods. After watermarking, the embedded data should preserve the quality of the host signal. Robustness, Imperceptibility, Security and Capacity are basic requirements for watermark generation.

For representing, analyzing, and designing discrete time signals and systems, the Discrete Z-Transform domain is convenient and invaluable tool. In this domain, 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 compared to normal LSB check-sum fragile watermarking scheme.

II. MOTIVATION

We seem to have reached often high in technology for many copyright protection problems, where break through paradigm changes are necessary for further development. For this purpose we need to ask again and again ourselves the fundamental question and 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 kind of work is to make the utilization of Discrete Z- Transformations and Genetic Algorithm in the applications of Digital Image Processing and Soft Computing. 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, the concept of GA is applied in the case of multimedia security. In the case of frequency domain, the various transforms are used like DFT, DCT, DWT, SVD but the concept of Discrete Z-Transforms can be used in better way to enhance the power of it in various application areas.

III. Literature Survey

Mohd. Sherfuddin Khan et al. [1] proposed a novel fragile watermarking scheme in the Z-transform domain. According to the authors, this is for the first time that this transform has been applied to digital watermarking and they proved that it provides resistance to various image processing attacks. In their work, they also tested the performance and robustness of the proposed technique by some image processing operations such as filtering, re-quantization, and JPEG compression. Authors suggested that there is no need to have the host image while extracting the watermark from watermarked image. The fragility check is done without the host image.

J. K. Mandal et al. [2] proposed an image authentication technique in frequency domain using genetic algorithm. This technique is based on Z-transformation on gray scale images. The first technique defines the process of encoding and second technique depicts the process of decoding such as insertion and extraction algorithm respectively. Insertion algorithm performs insertion of authenticating image bit wise into gray scale image. On the other hand extraction algorithm extracts bits of authenticating image from embedded image. According to the authors, Genetic algorithm is applied to enhance the security level. Dimension of the authenticating image followed by the content are embedded at the time of embedding and reverse process is followed at the time of extraction. High PSNR obtained for various images and large capacity as compared to existing algorithm ensured the high payload of the scheme.

Chih-chin lai et al. [3] proposed a digital watermarking scheme based on singular value decomposition and tiny genetic algorithm. In this algebraic features of the image were extracted by using SVD. Apply SVD on complete host image or on some part of the image, modify the singular values to embed the watermark. Scaling factor will control the strength of the watermark. The produced singular values are very stable and vary very little under various image processing attacks. SVD is employing on the host image to gain the 3 matrices, inserted into diagonal and then apply SVD on new matrix. Tiny GA is used to search the proper values in order to improve the visual quality of watermark image. Tiny GA is lightweight evolutionary algorithm and hence will reduce amount of computational effort to gain most fit solution.

IV. Proposed System

The Z-transform is the most general concept for the transformation of discrete-time series. Z-transform is an essential mathematical tool for the design, analysis and monitoring of system. A working knowledge of the z-transform is required to the study of discrete time filters and systems. It is possible through the use of these transforms that we formulate a closed-form mathematical description of a system in the frequency domain, design the system, and then analyze the stability, the steady state characteristics and the transient response of the system.

In mathematical description and signal processing, the Z-transform converts a sequence of real or complex number which is discrete time domain signal, into a complex frequency-domain representation.

The Z-transform definition is,

$$X(z) = \sum_{n=-\infty}^{\infty} x(n) z^{-n}$$

There are two types of Z-trnsform are as follows
One sided Z-transform:

The one-sided z-transform of a function x (n):

$$X(z) = \sum_{n=0}^{\infty} x(n) z^{-n}$$

Two sided Z-transform:
The two sided z-transform of a function x (n):

$$X(z) = \sum_{n=-\infty}^{\infty} x(n) z^{-n}$$

The z-trasform is the discrete-time counter-part of the Laplace transform. Like Laplace transform the Z-transform allows perception into the transient behavior, the stability of discrete-time systems and the steady state behavior. The Z-

transform is cousin of the Laplace transform. A useful feature of the Laplace and the Z-transforms are the description of a system in terms of the locations of the poles and the zeros of the system transfer function in a complex plane. Figure 1 shows prototype implementation [4].

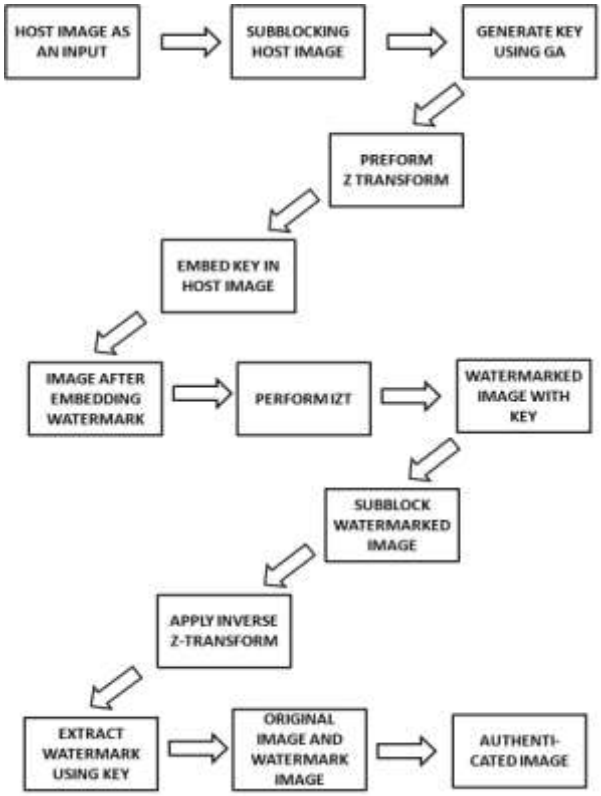

Figure 1. Prototype Implementation

V. APPLICATIONS

- Image watermarking applications in health care in number of medical applications, medical images require special safety and confidentiality, because critical judgment is done on the information provided by medical images.

- Criminal photograph authentication and transmission Most of the crime investigations are based on database submitted to crime branches from remote locations via Internet or mobile phones. When some unwanted crime happens, the criminal(s) photograph is constructed according to preliminary information collected from eyewitnesses where actual incident happens. This sensitive criminal image data needs to be transmitted across network through the Internet or mobile phone. Transmission of such image data demands high and guaranteed security.

- Remote education Distance education is gaining popularity in rural areas of developing countries due to the shortage of teachers. In order to support a variety of curriculum for different states in a diverse country like India along with various languages, there is a need for intelligent technologies to create a deployable remote education solution. The main challenge in the distance education solution is the dissemination of content and teacher-student interaction. The secured transmission of image data is part of distant learning. Image watermarking is solution for providing security in this regard.

VI. CONCLUSION

Though, we concluded that if we permute Discrete Z-Transform with Tiny Genetic Algorithm, it will be more effectual to sustain most of the Digital Image Processing attacks like Contrast, Brightness, Gaussian noise etc. And preserve its Robustness and Imperceptibility as compared to other transforms like DFT, DCT, DWT and SVD.

REFERENCES

[1] 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.

[2] 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.

[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] P. C. Harne, R. K. Nigam, and A. K. Bhavsar, “Permutation of Discrete Z transforms and Genetic Algorithm for Copyright Protection on Digital Image", National Conference on Advances in Computing (NCAC’13), 05-06 March 2013 PP-71-73.