ISSN: 2455 - 1597

ijergs
Open Access

International Journal of Engineering Research and Generic Science (IJERGS)
Available Online at www.ijergs.in

Volume - 4, Issue - 6, November - December - 2018, Page No. 116 - 121

Comparative Analysis of Different Watermarking Techniques in Image or Information Security

[1]Smriti Jain, M.Tech Scholar, Department of Electronic & Communication, Arya Institute of Engineering & Technology, Jaipur, India

[2]Er. Rajkumar Jain, Associate Professor& H.O.D, Department of Electronic & Communication, Arya Institute of Engineering & Technology, Jaipur, India

E-mail: [1]smritijain17593@gmail.com, [2]rkjain1983@gmail.com

Abstract

Digital Water Marking is an application associated with the protection of copyright. Both digital objects can be used as a trainer to convey information. If the information about the object is known as the visible or invisible watermark. During the graduation of digital information, there are many dangerous areas such as copyright and the integrity of the digital object. As a result of a tax burden, the content creator may try to restore the watermark. In this paper, a comparative study of the latest digital water marketing techniques such as DWT, DCT, SVT, NSA and CZT was presented on digital images.

Keywords: Cryptography, Image Encryption, Watermarking, Singular Value Decomposition (SVT), Chirp Z-Transform (CZT), NSA, DWT, DCT.

Introduction

The techniques involved in hiding certain information in the digital content is collectively known as information concealment techniques. When used in digital imagery, they can be classified as stealing or playlists. Information science refers to the science of invisible communication that seeks to conceal the very existence of the message itself. The digital watermark is the process to embed information in digital multimedia content so that the information may be set later for a variety of purposes, including blocking a node of copyright. A digital watermark is used for this purpose that is a digital signal or pattern inserted in a digital image and can also serve as a digital signature. This helps to determine the originality and property of the image.

Steganography is the science of hiding the message in a carrier from the human eye perception. It has many branches that include watermarks. A watermark, in general, it is used for authorization and to prevent counterfeiting or fraud. A digital watermark is different, since it is used for the protection of copyright or license. It is used to hide themes sage in the multimedia data that can be text, audio, images, etc. The changes in Multimedia data are usually not visible. We can classify watermelons according to a variety of criteria such as data management, flawless of the attackers, and sustainability, as in the technique used in the last recipient of the recipient. The digital medium used to carry the summary is known as coverage. When the cover cannot be retrieved at the end of the receiver while the summary is extracted, the technique is called irreversible watermark. In reversible digital watermarks, it can be excessively and simultaneously used without changing data. This technique, It is also called lossless since we get the original image of the cover without loss of Information.

According to the field where the water mark is introduced, these techniques are divided into two categories, namely the spatial domain and the area of conversation [2]. Space Field Methods modify the digital data directly to separate parts of the watermark, and have the advantage of low computational complexity. On the other hand, the conversion field (frequency) does not change directly from the pixel values but changes the convergence parameters to shift the water market such as Transit Cosine Transform (DCT), Separate Wavelet (DWT), and Single Value Analysis (SVD).

The digital watermark technique [1] is the process for inserting the watermark information (Such as code, name of property, signature, etc.) in protection information (eg audio, video and video) and the selection of market information for protection information, which is not determined by the human cognitive system.

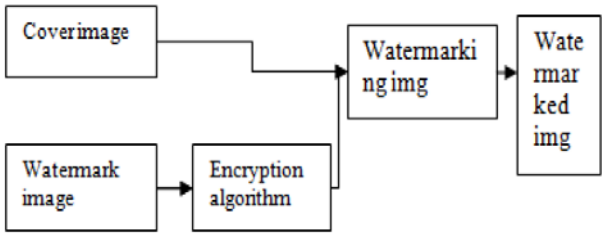

Figure 1 : Fundamental Process of Digital Image Watermarking

Water marking is the primary action of the digital water market. [1, 2] provides sufficient details on the requirements and their different types, such as fragile and strong watermarks. The watermark is more commonly used to indicate ownership of digital data. It is generally realized by combining a portion of the copyright information with digital data. Although, it can be used for the automatic supervision of copy and writing material in the world Broadband. Help in the automatic audit of the radio transmission that can be easily traced during its transmission. The watermark also helps incorporate additional information for the public's advantage - data increase. Essentially, it has appeared as the important technology to solve the problems mentioned above. [1] Your techniques can be divided into the following domains:

A. **Spatial domain methods:** A spatial domain method is used to directly change the pixel values of the bits in the digital image to hide certain information. Less Steganography based on significant bits (LSB) is one of the simplest techniques that hides a confidential message in LSB of pixel values without providing many possible versions. Changes in the amount of LSB are not visible to the human eye.

B. **Transform the Domain Technique:** This technique is complex and spatial as several Algorithms and transformations are used to hide the summary. Transforming the Domain Haven can be named in the scope of integration schemas, where a number of algorithms are selected [3]. The process of including data in the free software range of the signal is much stronger than the principles of integration that are working at that time. Most powerful theft systems today work within the scope of conversion. The techniques of the compost dome have advantages over spatial field techniques because they relate to the image that is less involved in image compression, processing and processing.

Different watermarking technique

Singular value decomposition (SVD)

SVD is an image processing technique. Specifically, SVD is used for image similar to picture, hidden images and digital watermarks. For example, an image called A. SVD is defined as: A = U * S * VT. The image is divided into three matrices: two orthogonal arrays U and V and a diagonal matrix S. U, V called individual and right vectors. The slope coefficients S are called the SV A fan matrix. The SVD digital watermark has some advantages: increasing the signal size contained in the image. The SV of the water market is the image less impact attacks. Can be used as a powerful function in digital watermark [6-7].

Discrete Wavelet Transform (DWT)

The Wavelet domain is a promising domain for watermark the area of wavelets is an important area for melons. DWT is a orthogonal conversion that is similar to the separate cosine conversion used to compress audio, video, speech, transient expression, footprint, Watermarks and many other applications in Biomedical Engineering. This is a common domain area where the current image is first divided into a frequency domain and its frequency changes are changed according to the converted watermark parameter. The watermark image is obtained strongly. In a single level expansion, DWT increases the hierarchical image, spatially and dramatically depict the image. An image based on three spatial, horizontal, vertical and diagonal directions appears in the result of converting the image to four different components: LL, LH, HL and HH. Here, the first letter refers to a request for low passenger traffic or increased passenger traffic, and the second refers to the candidate applied to the contract columns. The LL level is the lowest level of accuracy consisting of the cancellation portion of the partition. Stay three levels, that is, LH, HL, HH detailed information of the decade image.

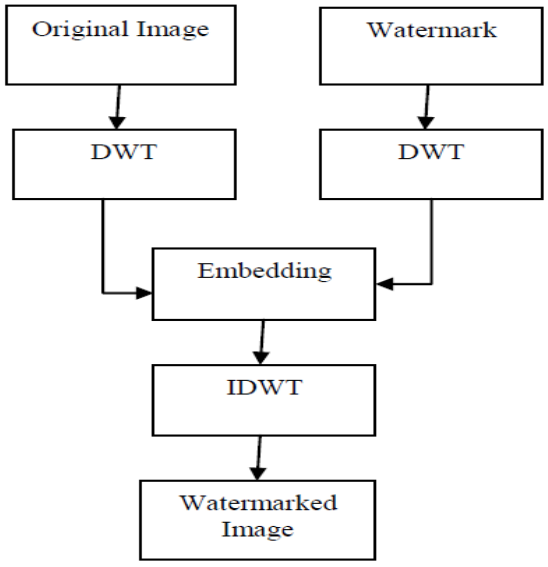

Figure 2 : DWT based Embedding

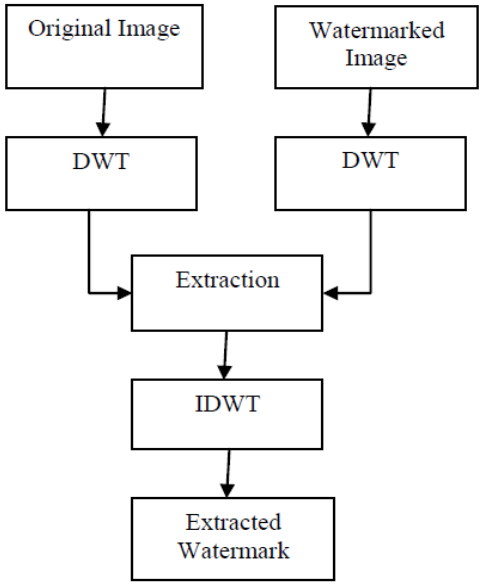

Figure 3 : DWT based Extraction

Discrete Cosine Transform (DCT)

The high frequency components have a watermark in the frequency domain. The main steps are:

1. The image share in blocks other than 8x8 is not overlapped.
2. Apply DCT for each of these blocks
3. By applying block selection criteria (eg, HVS)
4. Apply transaction selection criteria (eg higher)
5. Use the watermark by changing the selected parameters.

DFT Domain Watermarking

The DFT field is the preferred option to search because theft attacks against engineering attacks such as translation, rotation, farming, staging, etc. There are two integration techniques based on DFT. In the first technology market, the water market has been directly integrated, and the other is a template-based integration. In the immediate introduction, the tab is pressed by changing the phase information in the DFT. The template is a structure used in the DFT field to evaluate the conversion factor. First, a transformation is made in the image and the image is then searched for the template, and the detector is used to make the watermark embedded in the watermark.

Chirp Z-Transform (CZT)

CZT is actually an algorithm for evaluating the transformation of each signal. The properties of the Z domain link are often directly in the polynomials with two poles and zeroes of their origin, like the poles, the maximum regulatory amplitude, plus zero wristbands of the electrodes with the regulatory spectrum. CZT has the ability to evaluate the shift of problems inside and outside the decor system. You will discover that you have the opportunity to discover basic consistency, because you can focus on choosing a static analysis that has high resolution.

Some of the main interpretations of chirp z-transform are:

1. Development with poles.

2. A higher definition of narrow cross-analytic analysis.
3. Interpolation of the time frame, as well as the change of the test rate.

Negative Selection Algorithm (NSA)

Different to the NSA protocol, there is a tendency to conjugate eggplant, eggplant, presaged, and important safe with high quality T cells. This interface is easy to use, easy to use and easy to use. If the random side estimate is better and similar to the reciprocal interaction offered when generating tolerance, the random side is a personal aspect and disposed of, in any other case, recognized and presented in this set of sensors.

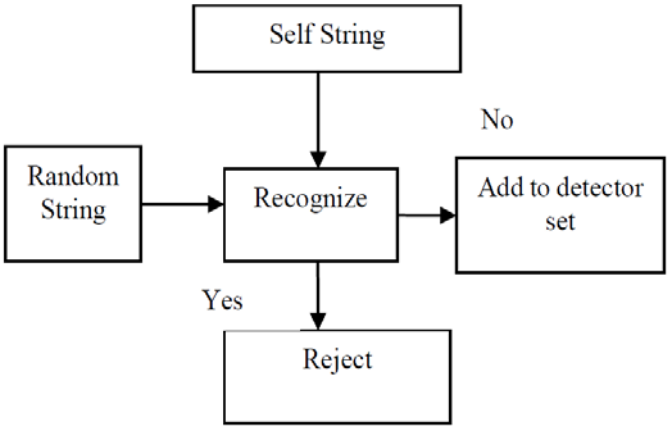

Figure 4 : The Negative Selection Algorithm

Conclusion

This paper has got suggested some sort of different watermarking techniques that are used in image security or information security. In this paper discussed the different types of the watermarking techniques like DWT, DCT, DFT, NSA, CZT, SVT etc to enhance the information security or image security.

References

1. Tri H. Nguyen, Duc M. Duong and Duc A. Duong, “Robust and high capacity watermarking for imagebased on DWT-SVD”, The 2015 IEEE RIVF International Conference on Computing & Communication Technologies Research, Innovation, and Vision for Future (RIVF), pp- 83-88, 2015.
2. Musrrat Ali and Chang Wook Ahn and Millie Pant, “An Optimized watermarking Technique Based on DE in DWT-SVD Domain”, IEEE Symposium on Differential Evolution (SDE), pp – 99-104, 2013.
3. Jasdip Kaur, Narwant Singh and Chahat Jain, “An Improved Image Watermarking Technique Implementing 2-DWT and SVD”, IEEE International Conference On Recent Trends In Electronics Information Communication Technology, pp – 1855-1868, may 20-21 may, 2016.
4. Siraa Ben Ftima, Mourad Talbi and Tahar Ezzedine, “LWT-SVD Secure Image Watermarking Technique”, IEEE International Conference on Electronics, Communication and Aerospace Technology, pp- 510-517, 2017.
5. Baisa L. Gunjal and Suresh N.Mali, “Comparative Performance Analysis of Digital Image Watermarking Scheme in DWT and DWT-FWHTSVD Domains”, 2014 Annual IEEE India Conference (INDICON), 2014.

6. Ruizhen Liu and Tieniu Tan, "An SVD-Based Watermarking Scheme for ProtectingRightful Ownership", IEEE TRANSACTIONS ON MULTIMEDIA, VOL. 4, NO. 1, MARCH 2002.
7. Vladimir I. Gorodetski, Leonard J. Popyack, Vladimir Samoilov and Victor A. Skormin, "SVD-Based Approach to Transparent Embedding Data into Digital Images", Springer Information Assurance in Computer Networks pp 263-274, 2001.
8. Hao-Tian Wu and Yiu-Ming Cheung, "Reversible Watermarking by Modulation and Security Enhancement", IEEE TRANSACTIONS ON INSTRUMENTATION AND MEASUREMENT, VOL. 59, NO. 1, pp- 221-227, JANUARY 2010.