International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 04 | Apr 2020 www.irjet.net p-ISSN: 2395-0072

An Overview on Different Watermarking Techniques

Mr. Ankit Kumar Tiwari[1], Mr. Himanshu Mangal[2], Mr. Sudhanshu Vashistha[3], Mr. Santosh Kumar[4]

[1,2]B.Tech Student, Department of Computer Science & Engineering, Arya College of Engineering & Research Centre, Jaipur, India
[3,4]Assistant Professor, Department of Computer Science & Engineering, Arya College of Engineering & Research Centre, Jaipur, India

---

Abstract - *Copyright protection of plain text while traveling over the internet is very crucial. Digital watermarking provides the complete copyright protection solution for this problem. Text being the most dominant medium travelling over the internet needs absolute protection. Text watermarking techniques have been developed in past to protect the text from illegal copying, redistribution and to prevent copyright violations. Digital watermarking is an application associated with the protection of copyright. Any of the digital objects can be used as a carrier to carry information. If the information is related to object, then it is known as a watermark that can be visible or invisible. In the era of digital information, there are multiple danger zones such as violation of copyright and integrity of digital object. In case of any dispute during the violation, the creator of the content may try property recovering the watermark. In this paper a comparative study of the most recently digital water mark techniques such as the DWT, DCT, SVT, NSA and CZT over digital image is presented.*

Key Words: **Cryptography, Image Encryption, Watermarking, Singular Value Decomposition (SVT), Chirp Z-Transform (CZT), NSA, Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT).**

1. INTRODUCTION

The techniques involved in hiding certain information in the digital content is collectively known as information concealment techniques. When used in digital images, they can be classified as steganography or watermark techniques Steganography refers to the science of invisible communication that struggles to hide the very presence of the message itself. The digital watermark is the process to embed information in digital multimedia content so that the information can be extracted or detected later for a variety of purposes including copy prevention and control. 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. That helps determine the authenticity and ownership of an 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 the message in the multimedia data that can be text, audio, images, etc. The changes in Multimedia data are usually not visible. We can classify the watermark techniques according to various criteria such as mastering the data, its visibility to the attackers, robustness and also according to the technique used for recovery in the final receiver. 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, The cover can be accessed and used without any alteration of the data. This technique, It is also called lossless since we get the original image of the cover without loss of Information.

According to the domain in which the watermark is inserted, these techniques are classified in two categories, that is, spatial domain and transformation domain methods [2]. The Spatial domain methods modify the digital data (pixels) directly to hide the watermark bits and they have the advantage of low computational complexity. On the other hand, the transformation domain (frequency) methods do not alter the pixel values directly, but rather modify the transformation coefficients to hide watermark bits such as Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD).

The digital watermark technique [1] is the process for inserting the watermark information (such as symbol, possession name, signature, etc.) into the protection information (such as sound, image, video) and choosing the Brand information of protection information, which is not perceived by the human perceptual system.

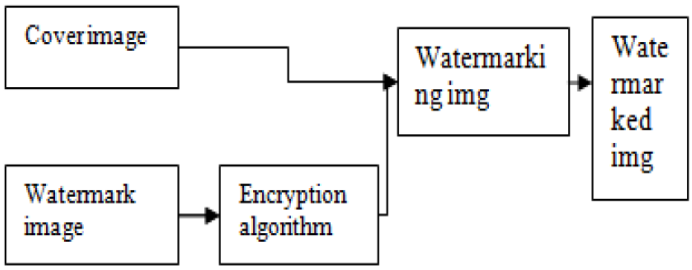

Figure 1 : Fundamental Process of Digital Image Watermarking

The watermark represents the fundamental process of the digital watermark technique. "Referee [1, 2]" provides sufficient detail about watermark requirements and their various types, such as fragile and robust watermarks.

The watermark is usually used to provide proof of ownership of the digital data. Is it is generally achieved by incorporating part 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:

1. **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 conceals a secret message in the LSB of pixel values without introducing many perceptible distortions. Changes in the value of the LSB are imperceptible to human eyes.
2. **Transform the Domain Technique:** This technique is complex and spatial as several Algorithms and transformations are used to hide the summary. Transforming the domain embedding can be termed as a domain of integration techniques for which a number of algorithms have been suggested [3]. The process of embedding data in the frequency domain of a signal is much stronger than the integration principles that operate in the time domain. Most strong steganographic systems nowadays operate within the transformation domain. Transformation domain techniques have an advantage over spatial domain techniques since they hide information in areas of the image that is less exposed to compression, clipping and processing images.

2. Different watermarking technique

A. Singular value decomposition (SVD)

SVD is one of the techniques for image applications treatment. Specifically, SVD has been used for image comparison Pressure, concealment of images and digital watermark. For example, an image is denoted by a matrix A. SVD is defined: A = U * S * VT. The image is broken down into three matrices: two orthogonal matrices U, V and a diagonal matrix S. U, V are called left and right singular vectors. Coefficients the diagonal matrix S is called SV of matrix A. In digital watermark, SVD has some advantages: reduce the size of embedded signal in the image. And the SV of the watermark the image is less influenced by the attacks. Can use as a sturdy feature in digital watermark [6-7].

B. Discrete Wavelet Transform (DWT)

The Wavelet domain is a promising domain for watermark incorporation. DWT is an orthogonal transformation similar to the Discrete Cosine Transform that can be used for audio and video compression, speech recognition, feature extraction, fingerprint, watermark and many other applications in biomedical engineering [8]. This is a frequency domain technique in which the front cover image is first transformed into frequency domain and then its frequency coefficients are modified according to the transformed watermark coefficients and a watermark image is obtained which is very robust. In the decomposition of a single level, DWT decomposes the image hierarchically, providing a spatial and frequency description of the image. It decomposes an image into basically three spatial directions, that is, horizontal, vertical and diagonal in the result that separates the image into four different components, namely LL, LH, HL and HH. Here the first letter refers to applying low pass frequency operations or high pass frequency operations to the rows and the second letter refers to the filter applied to the columns of the cover image. The LL level is the lowest resolution level that consists of the approximation part of the cover image. Rest three levels, that is, LH, HL, HH provide the detailed information of the cover image.

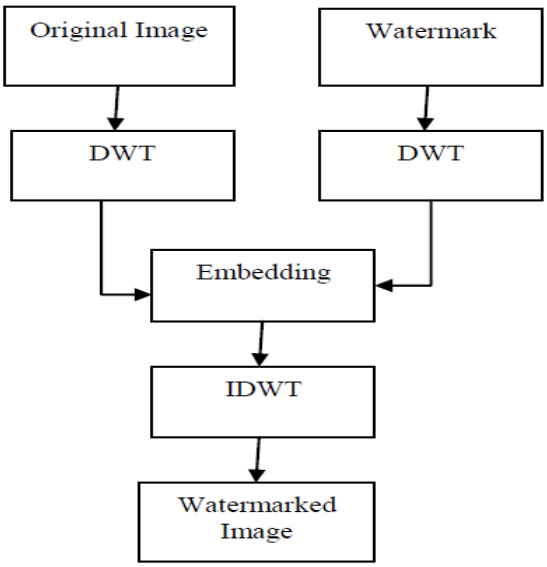

Figure 2 : DWT based Embedding

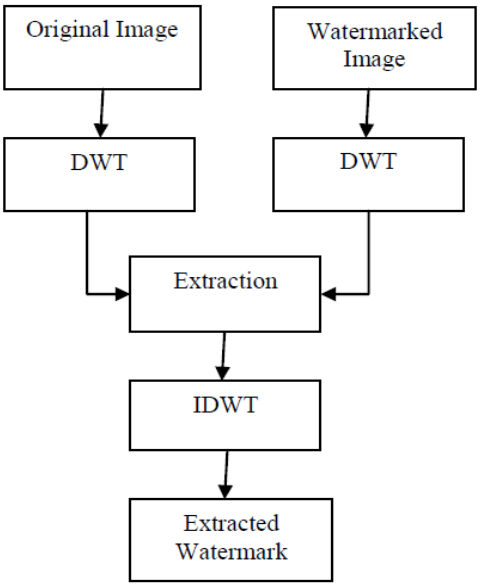

Figure 3 : DWT based Extraction

C. Discrete Cosine Transform (DCT)

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

1. Divide the image into non-overlapping 8x8 blocks.
2. Apply DCT forward to each of these blocks
3. Apply some block selection criteria (for example, HVS)
4. Apply coefficient selection criteria (for example, higher)
5. Embed watermark by modifying the selected coefficients.

D. DFT Domain Watermarking

The DFT domain is the favourite choice of research because it provides robustness against geometric attacks such as translation, rotation, cropping, scaling, etc. There are two types of watermark embedding techniques based on DFT. In the first technique, the watermark is directly embedded and another technique is template-based embedding. In direct inlay,

the watermark is incorporated by changing the phase information within the DFT. A template is a structure used in the DFT domain to judge the transformation factor. First a transformation is made in the image and then the image in which this template is searched is synchronized, and then the detector is used to extract the embedded broad-spectrum watermark.

E. Chirp Z -Transform(CZT)

CZT is actually an algorithm to evaluate the z transform of any signal. The characteristics of the Z domain switch are often directly factored into polynomials along with two poles and zeros from their origins, exactly where two poles type the peak of vitality of the regularity selection, as well as zeros write the valleys with the regularity spectrum . The CZT has got the ability to evaluate the z transformation with problems both inside and outside of your system circle. You will discover that you have the ability to discover the basic consistency, since you could focus on the selection of consistency analyzed that has a high resolution.

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

1. Development with poles.
2. High definition narrow band coherence analysis.
3. Interpolation of the time frame, as well as the change of the test rate.

F. Negative Selection Algorithm (NSA)

Based on the NSA protocol, there is a tendency to initialize self-tracking that involves personal peptides, which provides the standard behavior of your program, and a nonsense sequence involving premature T cells. Then, this appreciation with all the different parts of the random sequence is calculated with respect to many of the parts of the personal chain. In the case that the appreciation of a random aspect is better and identical to the cross reactivity that is offered when generating a tolerance, a random aspect is considered as a personal aspect and is particularly eliminated; in any other case, it is recognized and introduced into this set of sensors.

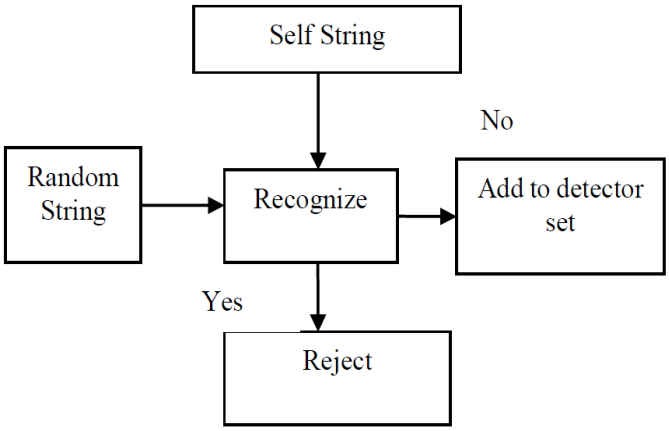

Figure 4 : The Negative Selection Algorithm

3. CONCLUSION

Any of the digital objects can be used as a carrier to carry information. If the information is related to object, then it is known as a watermark that can be visible or invisible. In the era of digital information, there are multiple danger zones such as violation of copyright and integrity of digital object. In case of any dispute during the violation, the creator of the content may try property recovering the watermark. In 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 image based 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 Protecting Rightful 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.