# Digital Watermarking Techniques for Security Applications

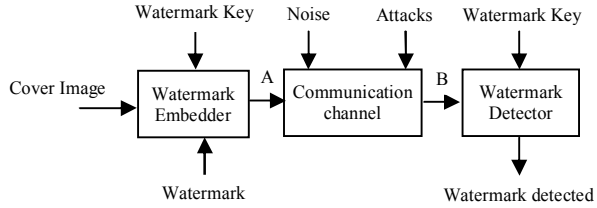
Sonam Tyagi[1], Harsh Vikram Singh[2],
Raghav Agarwal[3] and Sandeep Kumar Gangwar[4]

***Abstract*—Nowadays, the success of internet technology, made our life very much easy and convenient. But the major problem is to secure the data from duplication and unauthorized use. So the digital watermarking is used. With this technology, we embed the secret information into the actual information for protecting it from unauthorized use. By using this technique only authorized user can access the data. It may be classified into two domains that are spatial domain and frequency domain. In this paper, we have briefly discussed about these technologies and their pros and cons.**

***Keywords: Digital Watermarking, Least Significant Bit (LSB), Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Discrete Fourier Transform (DFT)***

## I. WHAT IS DIGITAL WATERMARKING?

Digital watermarking is that technology which is used for protection of digital media such as video, audio and image [1]. In this technique, watermark i.e. secret information is embedded in digital media using some algorithms and the watermarked media is processed. After that, watermark i.e. secret information is extracted using the particular algorithm. This technique, i.e. digital watermarking is used for authentication of data and protection of copyright [2]. Here two phases are used which are embedding of the watermark and detection and extraction of watermark.




A: Watermarked image
B: Noisy Watermarked image

Fig. 1: Digital Watermarking System

### A. Qualities of Digital Watermarking

There are some basic qualities, a digital watermark must possess:

- *Robustness*: It simply means ability to survive. When we transmit a watermarked data, then there are various attacks on that and that information may undergo different types of operations. So in these conditions, watermark must not degrade its quality [4].
- *Imperceptibility*: This simply means that watermark must be such that it cannot be observed by human eyes. It must be such that it can only be accessed by particular operations on watermarked data.
- *Security*: It means that, the watermark must be such that only authorized users can access it. If any user has no embedding information, he must be unable to detect the watermark. This is termed as security of watermark.
- *Capacity*: It simply means that how much amount of information we are able to embed in the original image. Watermark capacity simply refers the secret information amount present in watermarked image.
- *Computational Cost*: It depends on the method which is used for watermarking. If the watermarking method is more complex, then it contains complex algorithm, requirement of more software and hardware, so computational cost increases and vice versa.

## II. DIFFERENT TYPES OF WATERMARKING TECHNIQUES

Digital watermarking is very much popular now a days because it is easily available and it protects our data from illegal use. It has two major areas i.e. spatial domain watermarking and frequency domain watermarking [5]. In the spatial domain techniques, we embed the watermark by modifying the pixel values. On the other hand, in transform domain watermarking, the watermark is embedded into the coefficients of transform domain. Various types of transform domain techniques are DCT, DWT and DFT. From robustness and imperceptibility point of view, transform domain techniques are better than spatial domain techniques.

### A. Spatial Domain Watermarking

We know that the image is made up of pixels. In this method of watermarking, we embed the watermark in some specific pixels of image [6]. In the extraction phase,

[1,2,3,4]*Department of Electronics Engineering,*
*Kamla Nehru Institute of Technology, Sultanpur–228118, India*
*E-mail: [1]sonamtyagi.u@gmail.com, [2]harshvikram@gmail.com,*
*[3]raghavagarwalec051@gmail.com, [4]sandeepw45149@gmail.com*

978-1-5090-2118-5/16/$31.00 ©2016 IEEE

we extract the watermark from these specific pixels. This technique is very much easy to use, less complex and also takes less time. But on the other hand, it is not robust for various types of attacks.

### *B. Transform Domain Watermarking*

The transform domain watermarking is better as compared to the spatial domain watermarking. The image is represented in the form of frequency in the transform domain watermarking. In the transform domain watermarking techniques, firstly conversion of the original image is done by a predefined transformation. Then we embed the watermark in the transform image or in the transformation coefficients. Finally, we take the inverse transform to get the watermarked image [7]. Commonly used transform domain methods are Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and Discrete Fourier Transform (DFT).

#### *1) Discrete cosine transform*

It is generally used for the signal processing. In this we transform the image into the frequency domain. It is applied in many areas like pattern recognition, data compression, and image processing. This technique is more robust than spatial domain watermarking techniques. The main steps used in DCT [5] are:

- Firstly, take the image and divide it into non-overlapping 8*8 blocks.
- Calculate forward DCT of each of the non-overlapping blocks.
- Use HVS blocks selection criteria.
- Now use highest coefficient selection criteria.
- Then embed watermark in the selected coefficient.
- Now take inverse DCT transform of each block.

#### *2) Discrete wavelet transform*

Discrete Wavelet Transform (DWT) gives a multi resolution representation of the image. This representation provides a simple framework for interpreting the image formation. The DWT analyses the signal at multiple resolution. When we apply the DWT to an image, it divides the image into two quadrants, i.e. high frequency quadrant and low frequency quadrant. This process repeats until the signal has been entirely decomposed. If we apply 1-level DWT on two dimensional image, it divides it into four parts, i.e.

*LL*: It consists the low frequency details of the original image. We can say that approximation of the image lies in this part.

*LH*: It consists vertical details of the original image.

*HL*: It consists the horizontal details of the original image.

*HH*: It consists high frequency details of the original image.

Since we know that the detail of original image lies in low frequency coefficients, so we embed the watermark into low frequency coefficients [8]. If we apply IDWT, we can reconstruct the original image from the decomposed image [9].

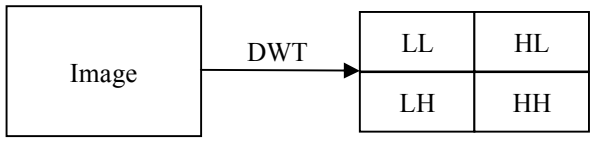



Fig. 2: Level Decomposition

#### *3) Discrete fourier transform*

Discrete Fourier Transform (DFT) offers more robustness against geometric attacks like scaling, cropping, translation, rotation, etc. It decomposes an image in sine and cosine form. In this, embedding may be done in two ways: direct embedding and the template based embedding.

In the direct embedding technique we modifying DFT magnitude and phase coefficients and then the watermark is embedded. The template based embedding technique introduces the concept of templates. In DFT domain, during embedding process, we embed the template, which is used to find the transformation factor. When the image is transformed, firstly this template is searched and it is then used to resynchronize the image. After this, detector is used to extract the embedded spread spectrum watermark [5].

TABLE 1: COMPARISON AMONG DIFFERENT WATERMARKING TECHNIQUES [3], [10], [11]

| Technique | Merits | Demerits |
|---|---|---|
| Least Significant Bit | 1. It is easily understandable and easy to implement.<br>2. It provides low image quality.<br>3. .Perceptual transparency is high. | 1. Here basic robustness is less.<br>2. Sensitive to noise.<br>3. Sensitive to scaling, cropping. |
| Discrete Cosine Transform | 1. Here we embed the watermark into the middle frequency coefficients because in the middle frequency band, the perceptibility of the image doesn't get effected and if there are attacks on watermarked data, the watermark is not removable. | 1. When we proceed to quantization step, higher frequency components present in the image, are suppressed. |
| Discrete Wavelet Transform | 1. DWT provides better localization in both time and frequency domain.<br>2. Here we get higher compression ratio. | 1. The computational cost is higher.<br>2. Compressing time is longer. |
| Discrete Fourier Transform | 1. DFT is used to recover from geometric distortions, because DFT is rotation, scaling translation invariant. | 1. Implementation is complex.<br>2. The computational cost is also higher. |

978-1-5090-2118-5/16/$31.00 ©2016 IEEE

## III. Applications of Digital Watermarking

There are various applications of digital watermarking, some of them are as:

- *Copyright Protection*: Digital watermarking is used to identify and protect copyright ownership. Digital data is embedded with watermarks to identify the copyright owners [13].
- *Medical Application*: For any treatment, medical reports are very much important. If the reports get mixed, it proves very much dangerous for the patients. So by using digital watermarking, we embed the name of the patients on the reports such as an MRI scan and X-Ray reports [12].
- *Annotation and Privacy Control*: To annotate an image multi-bit watermarking can be used. For example, imaging details and patient records related to a medical image can be carefully embedded into the image.

## IV. Watermarking Attacks

When the watermarked media is transmitted, several attacks take place on that watermarked media. These attacks may be given as:

- *Removal Attack*: In this, the unauthorized user tries to remove the watermark i.e. secret information from the watermarked data.
- *Interference Attack*: In these types of attacks, the noise is inserted to the watermarked media. Some examples of this category are averaging, quantization, compression etc.
- *Geometric Attack*: These types of attacks can change the geometry of the image. The examples of this category are cropping, rotation etc.
- *Low Pass Filtering Attack*: This type of attack takes place when we pass the watermarked data from a low pass filter.
- *Active Attack*: It is the most important attack. Here the unauthorized user tries to extract the watermark or simply makes the watermark such that it cannot be detected by any operation.
- *Passive Attacks*: In this type of attack, unauthorized user simply tries to find out that the particular data contain the watermark or not.
- *Image Degradation*: In these types of attacks, the parts of the image are removed, resulting in damage of robust watermarks. Examples of these attacks are partial cropping, row removal and column removal, insertion of Gaussian noise.

## V. Performance Evaluation Metric

If we want to evaluate the performance of the watermarked images, we have to analyze some quality parameters such as MSE, SNR, PSNR, and BER.

*Mean Square Error (MSE)*: It may be defined as the average squared difference between an original image and a distorted image. It is calculated by the formula given as

$$\text{MSE}= \frac{1}{PQ}\left[\sum_{i=1}^{P}\sum_{j=1}^{Q}(m(i,j)-n(i,j))\text{\^{}}2\right]$$

Where P and Q is defined as the height and width of the image respectively. Here m(i,j) represents the pixel value of the original image and n(i,j) represents the pixel value of the embed image [11].

*Signal to Noise Ratio (SNR)*: By this we measure the sensitivity of the image. Here we analyze the effect of the signal strength relative to the noise. It is measured as [14],

$$SNR_{db} = 10\log\left(\frac{P_{signal}}{P_{noise}}\right)$$

*Peak Signal to Noise Ratio (PSNR)*: If we want to find the loss in quality of the watermarked image with respect to the original image, we calculate PSNR. It is given as:

$$\text{PSNR}=10\log_{10}\left(\frac{L*L}{MSE}\right)$$

Where L is the highest value of the image. For example, for 8 bit image, L=255.

*Bit Error Ratio (BER)*: In this, we compare the bit values of watermarked image and the original image. Out of total bits received, the number of bits which contains error is described by the BER. BER may be calculated as:

BER=R/ (P*Q)

Where P and Q represent the height and width of the watermarked image respectively, and R is the count number. Its initial value is zero, if there comes any bit difference between the original image and watermarked image, the value of R increases by one and this process continues [11].

TABLE 2: Related Work

| Year | Work |
|---|---|
| 2000 | Chen *et al.* gave an adaptive watermarking scheme. In this scheme he embeds a binary image as watermark in DCT method. |
| 2005 | Ping Dong *et al.* presented "Digital Watermarking Robust to Geometric distortions." |
| 2008 | Wang H. *et al.* gave a chaotic watermarking scheme which is used for authentication of JPEG images. |
| 2009 | Chen *et al.* gave watermarking procedure for spatial domain. In this he presented a watermarking procedure which is based on information which is block-wise dependent for thwarting VQ attacks. |
| 2010 | A.M. Kothari *et al.* proposed performance of combined DWT-DCT over individual DWT. |
| 2010 | Sridevi *et al.* presented secure watermarking based on SVD and wavelets. |
| 2011 | Yan *et al.* presented a blind watermarking approach. In this there is a protection of vector Geo-spatial data from illegal use. |
| 2012 | Chen *et al.* gave a watermarking scheme which is based on frequency domain. Here a modified algorithm is presented to improve the defect of the JPEG quantification to reduce the bit error rate of the received watermark. |
| 2013 | Kaur *et al.* reviewed paper on image watermarking using LSB. |
| 2014 | Giri *et al.* proposed channel wise watermarking scheme which is based on DWT for colored image. |
| 2014 | Khanduja *et al.* presented robust multiple watermarking technique for relational database. |
| 2014 | Joshi *et al.* proposed paper on secure medical image watermarking. In this he embed dual watermark. |

978-1-5090-2118-5/16/$31.00 ©2016 IEEE

## VI. CONCLUSION

As we can see that digital watermarking is very useful method for digital data authentication. It ensures the protection of copyright and authentication. This paper gives an overall analysis of various types of digital watermarking methods. In this paper we have discussed different methods such as spatial domain methods and transform domain method which consists DCT, DWT and DFT. We have discussed the pros and cons of these methods. From a research point of view, this technology is an interesting field because many techniques are emerging for protection of data and many still have to come.

## REFERENCES

[1] R.G. Schyndel, A. Tirkel, and C.F Osborne,―A Digital Watermark, Proceedings of IEEE International conference on Image Processing, ICIP-1994, pp. 86-90, 1994.

[2] Christine I. Podilchuk, Edward J. Delp,―Digital watermarking: Algorithms and applications, IEEE Signal processing Magazine, July 2001.

[3] Jiang Xuehua,―Digital Watermarking and Its Application in Image Copyright Protection, 2010 International Conference on Intelligent Computation Technology and Automation.

[4] C.-T. Li and F.M. Yang.,―One-dimensional Neighborhood Forming Strategy for Fragile Watermarking. In Journal of Electronic Imaging, vol. 12, no. 2, pp. 284-291, 2003.

[5] V. M. Potdar, S. Han and E. Chang, "A Survey of Digital Image Watermarking Techniques", 2005 3rd IEEE International Conference on Industrial Informatics (INDIN).

[6] N. Chandrakar and J. Baggaa,"Performance Comparison of Digital Image Watermarking Techniques: A Survey", International Journal of computer Application Technology and Research, vol. 2, no. 2, (2013), pp. 126-130.

[7] F. Daraee and S. Mozaffari, "Watermarking in binary document images using fractal codes", Pattern Recognition Letter (2013).

[8] N. Tiwari, M. k. Ramaiya and Monika Sharma, "Digital watermarking using DWT and DES", IEEE (2013).

[9] S. S. Gonge and J. W. Bakal, "Robust Digital Watermarking Techniques by Using DCT and Spread Spectrum", International Journal of Electrical, Electronics and Data Communication, ISSN: 2320-2084, vol. 1, no. 2, (2013).

[10] Chapter 2: Literature Review, Source: Internet

[11] Amit Kumar Singh, Nomit Sharma, Mayank Dave, Anand Mohan, ―A Novel Technique for Digital Image Watermarking in Spatial Domain, 2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing.

[12] G. Coatrieux, L. Lecornu, Members, IEEE, Ch. Roux, Fellow, IEEE, B. Sankur, Member, IEEE 'A Review of digital image watermarking in health care'.

[13] Edin Muharemagic and Borko Furht―A Survey of watermarking techniques and applications 2001.

[14] http://en.wikipedia.org/wiki/Signal_to_noise_ratio_(imaging)

978-1-5090-2118-5/16/$31.00 ©2016 IEEE