

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320-088X

IJCSMC, Vol. 3, Issue. 7, July 2014, pg.790 – 795

SURVEY ARTICLE



A Survey on Different Watermarking Approaches

Arti ¹, Neeraj Dahiya ²

M.Tech Student CSE Dept., South Point Institute of Technology and Management, Sonipat, Haryana
malikarti66@gmail.com

Assistant Professor CSE Dept., South Point Institute of Technology and Management, Sonipat, Haryana
dhynrj@gmail.com

Abstract— *As the information is transmitted over the public domain, it suffers from different security threats. When the digital information is presented on this public web, it is required to authenticate the information to secure is from theft. Watermarking provides such authentication by embedding the authentication signature in the digital media itself. In this paper, an exploration to the watermarking approach is defined along with different methodologies. The paper has discussed the security concerns and the relative approaches to enhance the information security. The work is here focused on generic approaches that can provide security on different media types.*

Keywords- *Information Security, Data Hiding, Authentication, Digital Media*

I. INTRODUCTION

Today, most of the information is present in the form of digital content available in different media forms such as images, audio, video etc. When the information is subjective to a particular person or the organization, it is required to reserve the information copyrights to that particular individual. Using this digital contents, without the permission of authentication person, is a serious offence. There is the requirement to protect such kind of sensitive digital media from theft. Watermarking provides such an approach to reserve the person to particular individual or the firm. Watermarking actually embed this authenticated information, symbol, logo or signature in the digital media itself. This embedding is performed either in the visible or invisible form.

There are number of watermarking approaches opted by different researchers and organizations. These methodologies depend on the media type as well as the sensitivity of the information content and size of the information content. The media content in which the authentication information object is embedded is called cover object. The cover object can be an image, audio or the video. The basic model of watermarking is shown in figure 1.

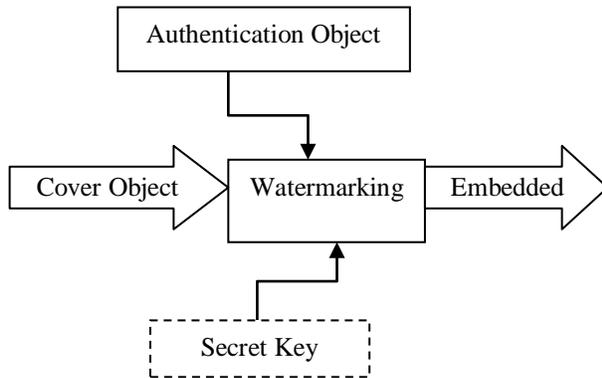


Figure 1 : Watermarking Model

The model is showing cover object in the form of a generic media form that is required to authenticate. The authentication object here is defined as the reserved symbol to the individual or the firm. In this model, a secret key is defined to encode the information object to enhance the security level. The watermarking algorithm is here applied to hide the authentication object in the cover object. Finally the embedded object will be obtained as the final information object.

To perform this security, the third party is involved. The third party is actually responsible for the key sharing and to enhance the security. Here the cryptography can be integrated with watermarking approaches to improve the security level. This cryptographic operation will be handled by using some secrecy key(Sk). This cryptographic process is optional so that defined in dotted rectangular box. As the Watermarking process is performed over these input operations, finally single embedded object will be obtained. In the equational form the Watermarking process is given as

$$EO = \text{Watermarking} (MO, O) \quad (i)$$

Here equation (i) is showing the Watermarking process without incorporating the cryptographic process. To achieve the security along with robustness, the cryptographic process can also be embedded, shown in equation (ii).

$$EO = \text{Watermarking} (MO, O, Sk) \quad (ii)$$

The recovery process from the embedded Object(EO) is reversed to the Watermarking process and the Watermarking recovery model is shown in figure 1.2.

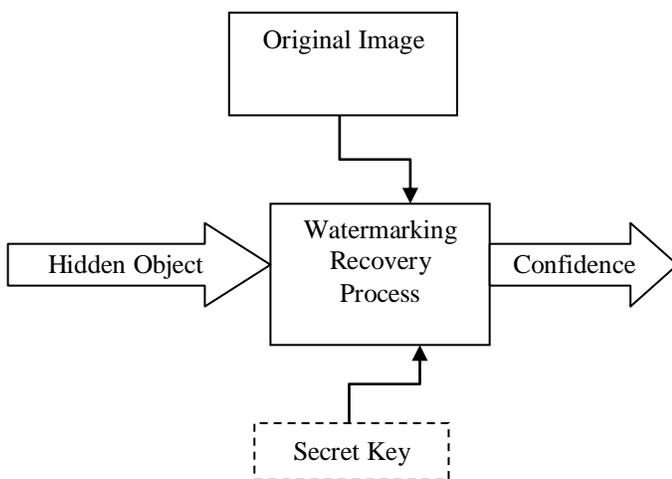


Figure 2 : Watermarking Recovery Process

As we can see, the major input to the process is the Embedded multimedia object (EO). Now to check the authenticity or to verify the existence of a particular hidden object (O) we need the availability of the original Multimedia object (MO) or the Watermarking Object. If the authentication of the Watermarking process is done under cryptographic approach, there is the requirement of relative secret key. As the recovery process is performed, the actual Watermarking will be obtained or the proof of its existence will be obtained [1]. The recovery process is shown by equation (iii)

$$\text{ConfidenceMeasure} = \text{WatermarkingRecovery}(\text{EO}, \text{O}) \quad (\text{iii})$$

In case of cryptographic authentication, the recovery process is given by using equation (iv)

$$\text{ConfidenceMeasure} = \text{WatermarkingRecovery}(\text{WO}, \text{O}, \text{Sk}) \quad (\text{iv})$$

In this section, the introduction to the watermarking process is defined along with standard models. In section II, the work done by the earlier researchers is discussed. In section III, some of the effective watermarking methodologies are discussed. In section IV, the conclusion obtained from the work is presented.

II. LITERATURE REVIEW

In this section, the work done by the earlier researchers is discussed. In spatial domain methods a Stenographer modifies the secret data and the cover medium in the spatial domain, which is the encoding at the level of the LSBs. This method has the largest impact compared to the other two methods even though it is known for its simplicity. Embedding in the 4th LSB generates more visual distortion to the cover image as the hidden information is seen as “non-natural”. This technique in producing fingerprinted secret sharing Watermarking for robustness against image cropping attacks. Their paper addressed the issue of image cropping effects rather than proposing an embedding technique. The logic behind their proposed work is to divide the cover image into sub-images and compress and encrypt the secret data. The resulting data is then sub-divided and embedded into those images portions. To recover the data a Lagrange Interpolating Polynomial was applied along with an encryption algorithm. The computational load was high, but their algorithm parameters, namely the number of sub-images (n) and the threshold value (k) were not set to optimal values leaving the reader to guess the values [Potdar et. al., 2005]. Shirali-Shahreza exploited Arabic and Persian alphabet punctuations to hide messages. While their method is not related to the LSB approach, it falls under the spatial domain. Unlike English which has only two letters with dots in their lower case format, namely “i” and “j”, Persian language is rich in that 18 out of 32 alphabet letters have points [Shirali-Shahreza, 2006]. The secret message is binarized and those 18 letters’ points are modified according to the values in the binary file. Colour palette based Watermarking exploits the smooth ramp transition in colors as indicated in the colour palette. The LSBs here are modified based on their positions in the said palette index. They were in favor of using BMP (24-bit) instead of JPEG images [Johnson & Jajodia, 1998]. Their next-best choice was GIF files (256-color). BMP as well as GIF based Watermarking apply LSB techniques, while their resistance to statistical counter attack and compression are reported to be weak [Kong et. al. 2005, Fridrich et. al. 2002]. BMP files are bigger in size than other formats which render them improper for network transmissions. JPEG images however, were at the beginning avoided because of their compression algorithm which does not support a direct LSB embedding into the spatial domain [Fridrich et al., 2002] claimed that changes as small as flipping the LSB of one pixel in a JPEG image can be reliably detected. The experiments on the Discrete Cosine Transform (DCT) coefficients showed promising results and redirected researchers’ attention towards this type of image. In fact acting at the level of DCT makes Watermarking more robust and not as prone to many statistical attacks. Spatial Watermarking generates unusual patterns such as sorting of colour palettes, relationships between indexed colors, exaggerated “noise”, etc, all of which leave traces to be picked up by Extraction tools. This method is very fragile. There is a serious conclusion drawn in the literature. “LSB encoding is extremely sensitive to any kind of filtering or manipulation of the stego-image. Scaling, rotation, cropping, addition of noise, or lossy compression to the stego-image is very likely to destroy the message. Furthermore an attacker can easily remove the message by removing (zeroing) the entire LSB plane with very little change in the perceptual quality of the modified stego-image”. Almost any filtering process will alter the values of many of the LSBs. By inspecting the inner structure of the LSB, [Fridrich et al., 2002] claimed to be able to extract hidden messages as short as 0.03bpp (bit per pixel). Xiangwei stated that the LSB methods can result in the “pair effect” in the image histograms. This “pair effect” phenomenon is empirically observed in Watermarking based on the modulus operator [Xiangwei et al., 2007]. This operator acts as a means to generate random (i.e., not sequential) locations to embed data. It can be a complicated process or a simple one like testing in a raster scan if a pixel value is even then embed, otherwise do nothing. Avcibas and co-author applied binary similarity measures and multivariate regression to detect what they call “telltale” marks generated by the 7th and 8th bit planes of a stego image [Avcibas et al., 2001].

III. WATERMARKING APPROACHES

Watermarking methods are divided in two main categories called domain specific and the transformation specific. In case of spatial domain based approaches, the information message is directly embedded in the information object. The pixel replacement is here performed to achieve the watermarking. These kind of approaches includes the LSB(Least Significant Bit), Bit plane complexity based approach. LSB is considered as the most basic approach in which the last bit of each pixel is replaced to perform the watermarking. This kind of approach performs the pixel or the bit level substitution over the cover object. In case of bit plane complexity approach, the block level replacement is defined. In such approaches, the cover object is decomposed in smaller objects and the block extraction is performed over it. Once the blocks are obtained, the secret or hidden object blocks replaces this information object. DCT (Discrete cosine Transformation) and DWT (Discrete Wavelet Transformation) are these kind of watermarking approaches. These approaches performs the frequency or intensity level analysis over the cover objects to identify the effective area in which the information hiding will be performed.

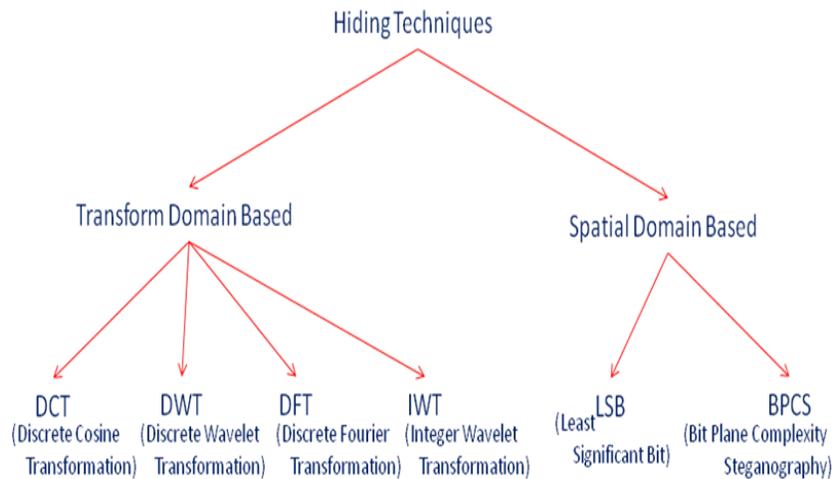


Figure 3 : Watermarking Approaches

A) DCT Approach

Discrete Cosine Transformation is defined as the sequence of data points in terms of cosine functions. These functions are defined as the oscillating information defined at different frequencies. DCT actually transforms the cover object from spatial domain to frequency domain so that the frequency level analysis will be performed over it. This kind of object takes the frequency analysis based decision to identify the effective area in which information hiding will be performed. This information includes the high and low frequency data analysis so that the intensity change over the cover object is performed. In general form, the information is stored in high frequency area. DCT is applied to perform information compression as well to perform watermarking.

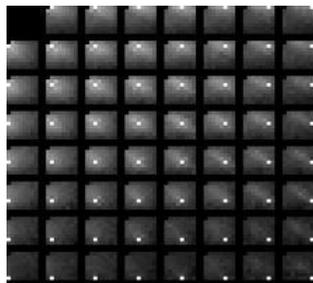


Figure 4 : DCT Transformation

The steps for DCT approach are given here under

- Accept the cover object as input to perform the transition and perform the decomposition to smaller blocks of size nxm
- Perform the frequency or intensity level analysis on each block.

- Obtain the high frequency areas and represent as the mask area where the information will be stored.
- Neglect low frequency areas and perform the effective watermarking over the cover object.

B) Discrete Wavelet Transformation

DWT is defined as another decomposition approach applied on the signal under the function set specification called wavelets. This algorithm is defined as the standard tool to perform frequency and location analysis over the signal. The constant value analysis is applied to identify the effective areas over the images. The approach divided the information object in four different frequency domains called horizontal, vertical, diagonal and approximate analysis. The information can be stored in any one of the frequency domain according to the requirement.

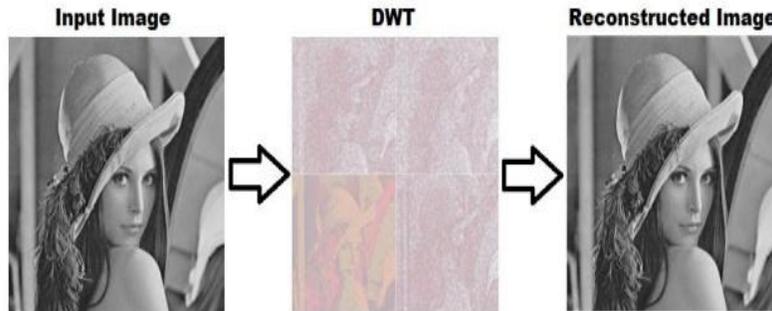


Figure 5 : DWT based Watermarking

C) Discrete Fourier Transformation

DFT is another transformation approach used to decompose the image under the sine and cosine components. This transformation object converts the object in signal form under the frequency domain. The information object is converted to the spatial domain based transformation. The fourier domain based analysis is here defined under the frequency analysis over the spatial domain. The effective image area is identified to perform the information hiding over the cover object.

D) Least Significant Bit

One of the most common techniques used in watermarking today is called least significant bit (LSB) insertion. This method is exactly what it sounds like; the least significant bits of the cover-image are altered so that they form the embedded information. The following example shows how the letter A can be hidden in the first eight bytes of three pixels in a 24-bit image.

```

Pixels: (00100111 11101001 11001000)
        (00100111 11001000 11101001)
        (11001000 00100111 11101001)
        A: 01000001
Result: (00100110 11101001 11001000)
        (00100110 11001000 11101000)
        (11001000 00100111 11101001)
    
```

The three underlined bits are the only three bits that were actually altered. LSB insertion requires on average that only half the bits in an image be changed. Since the 8-bit letter A only requires eight bytes to hide it in, the ninth byte of the three pixels can be used to begin hiding the next character of the hidden message. While LSB insertion is easy to implement, it is also easily attacked.

IV. CONCLUSION

In this present work, the basic watermarking model is been discussed in detail. Along with this, the efforts of the different researchers in the area of watermarking and different watermarking approaches are also discussed in this paper.

References

- [1] **Kong, X., Wang, Z. and You, X. (2005)** “steganalysis of palette images: Attack optimal parity assignment algorithm” in: Proceedings of 5th IEEE International Conference on Information, Communications and Signal Processing, 06-09 Dec 2005, pp. 860-864.
- [2] **Kumar, P.S., Anusha, K., Venkata, R., (2011)** “A Novel Approach to Enhance Robustness in Steganography Using Multiple Watermark Embedding Algorithm”, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307 (Online), vol. 1, Issue-1, 2011.
- [3] **Lee Jiann-Shu., Kuob Yung-Ming, Pau-Choo Chung, E-Liang Chen, (2007)** “ Naked image detection based on adaptive and extensible skin color model”, Pattern Recognition 40 2261 – 2270
- [4] **Licks, V. Jordan, R.(2003)**, “On digital image watermarking robust to geometric Transformations”, Department of electrical and computer engineering the university of new Mexico Eceblgd, albuquerque, new Mexico 87131, USA
- [5] **Manikandan, V. (2011)** “A Novel Method to Analyze Steganographic Content in Internet”, International Journal of Mathematics Trends and Technology, May to June Issue 2011, pp. 1-7.
- [6] **Manikopoulos, C., Yun-Qing, S., Sui, S., Zheng, Z., Zhicheng, N. and Dekun, Z. (2002)**“Detection of Block DCT-based Steganography in Gray-scale Images”, Proceedings of the IEEE Workshop on Multimedia Signal Processing, 9-11 Dec 2002,pp. 355 – 358.
- [7] **Marvel, L.M., Boncelet, C.G., Retter, C.T., (1999)** “Spread spectrum image steganography”, Image Processing, IEEE Transactions on Issue Date: vol. 8, 1999, pp. 1075 – 1083.
- [8] **Matthews, J., (2002)** “An introduction to edge detection: The sobel edge detector,”Available at <http://www.generation5.org/content/2002/im01.asp>, 2002.
- [9] **Neil F. Johnson, and Jajodia, S. (2008)** “Steganalysis of Images Created Using Current Steganography Software” Lecture Notes in Computer Science, vol. 1525, 2008, pp. 273-289.
- [10] **Nikolaidis, N. and Pitas I. (1998)** “Robust image watermarking in the spatial domain”, Signal Processing, vol. 66, 1998, pp. 385-403.
- [11] **Nilchi, A., Taher A. (2008)** “A New Robust Digital Image Watermarking Technique based on the Discrete Cosine Transform and Neural Network”, April 2008, pp: 1 – 7.
- [12] **Paulson, L. D. (2006)** “New System Fights Steganography”, News Briefs, Computer, IEEE Computer Society, vol. 39(8), 2006, pp. 25-27.
- [13] **Petitcolas, F.A.P., (2000)** “Introduction to Information Hiding”. In: Katzenbeisser, S and Petitcolas, F.A.P (ed.) (2000), “Information hiding Techniques for Steganography and Digital Watermarking”, Norwood: Artech House, INC.
- [14] **Popa, R.,(1998)** “An Analysis of Steganographic System”, The "Politehnica" University of Timisoara, Faculty of Automatics and Computers, Department of Computer Science and Software Engineering, May 25, 1998.