**Available Online at www.ijcsmc.com**

**International Journal of Computer Science and Mobile Computing**

**A Monthly Journal of Computer Science and Information Technology**

**ISSN 2320–088X**

***IJCSMC, Vol. 3, Issue. 3, March 2014, pg.676 – 681***

**RESEARCH ARTICLE**

# A Study on Different Audio Watermarking Techniques

**Lovely Malhotra[1], Neha Gupta[2]**

[1]Student, NC College of Engineering, Panipat, Haryana
lovelypanipat@gmail.com

[2]Assistant Professor, NC College of Engineering, Panipat, Haryana
nehagupta3108@gmmail.com

**Abstract— Watermarking is one of the effective approaches that incorporate the information security with network communication and media transformation. Watermarking is about to authenticate some digital content by embedding the secret information or data into the media itself. Watermarking can be applied on different media to enhance the information security. In this paper, the study of different watermarking approaches is defined to improve the information security. The paper includes the study of the efforts of earlier researchers and the approaches in the direction of watermarking as well as the information security. The main concern is given to the audio watermarking as the base media to attain information security.**

**Keywords- Vague Rule, Markov Model, predictive, Web Usage Mining**

## I. INTRODUCTION

Digital media processing enable the easy distribution of different kind of media with easy communication means but it also gives the disadvantage from the content provider or the author point of view. The easy distribution of digital media gives unlimited copying as well as unauthentic copying or theft of digital Medias. To reserve the authentication rights to the content provider is done by embedding the digital objects in these multimedia data. A Watermarking object can be signature or some other digital content that contains the information about the author or the host or the content provider. Enabling the Watermarking appropriately helps to follow up the expected violation of copyrights[1].

In digital media processing there are different methods to hide some secret digital information in some other media. The basic idea of these approaches is same but different respective to the methodology, robustness, capacity and this security level. Two main categorization of such approaches are Watermarking and the Watermarking. Watermarking basically hide the secret information among media files so that secret communication can be drawn between end users.

 

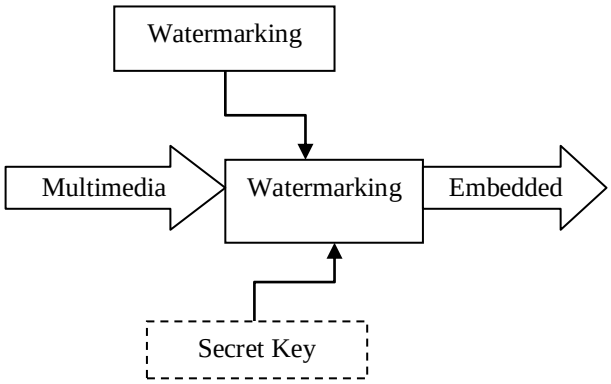


Figure 1: Watermarking Model

The basic requirements of watermarking process is given as under

- The major requirement of Watermarking is the about the specification of data size that can be embedded with robustness. A Watermarking approach must be capable to hide the massive information in multimedia data.
- To achieve the security from third party, Watermarking must be key enabled. For this some cryptography approach is collaborated with Watermarking to achieve the security along with robustness.
- Watermarking can be invisible so that information can be visualize.
- Embedded object must be unremovable in any case.
- Watermarking recovery from the multimedia content will not remove the actual content.
- Watermarking must be performed in real time i.e. practical implementation is required.
- Watermarking must be able to convey the arbitrary information so that effective communication between parties will be done.

Here figure 1 is showing the basic Watermarking process. This Watermarking process requires main multimedia object that can be image, audio or the video. The Multimedia Object(MO) is the actual digital content that provider want to authenticate. The embedding object is the actual digital information or the signature that represent the owner's authenticity and owner want to hide this information in multimedia object. If the owner also want to secure this information some cryptography mechanism can also incorporated with Watermarking process. 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

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

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).

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

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.

 

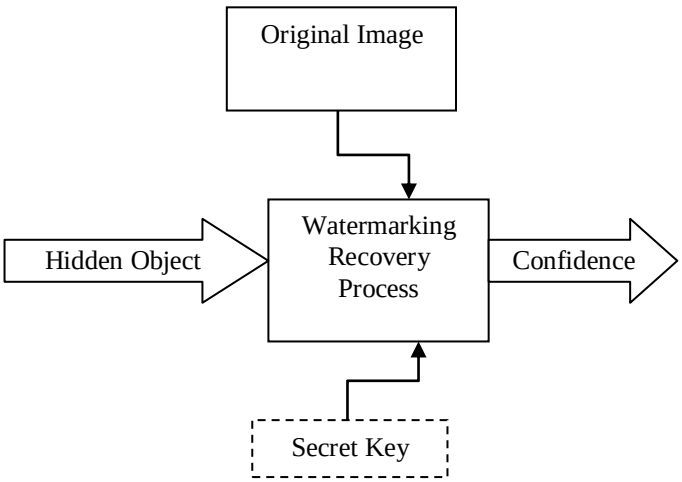


Figure 2 : Watermarking **Recovery Process**

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)

ConfidenceMeasure = WatermarkingRecovery(EO, O) (iii)
In case of cryptographic authentication, the recovery process is given by using equaition (iv)

ConfidenceMeasure = WatermarkingRecovery(WO, O, Sk) (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. EXISTING APPROACHES

Some of the earlier approaches presented by different researchers is discussed in this section.

### A) DCT Approach

DCT is one of the impotent approach that first separate the video frames in smaller parts and assign the weightage to these parts under the quality analysis. The concept of DCT is similar to the Fourier transformation so that the signal is identified under the spatial domain and the frequency analysis on these frames will be done effectively.

The basic process defined by DCT is given as under

- As the video frames is accepted by the DCT, it split the frame in smaller windows of size nxm.
- Extract the intensity from different window forms at position (I,j)
- Define the coefficient for each row and column under the DCT coefficient matrix.
- The extraction of low frequency areas from the frame that will be used as the key area for storing the data over the image
- The compression will be performed effectively by neglecting the non visible areas so that no visible distortion will be done.

### B) Tampar Resistent Hardware

This Watermarking approach combines the Watermarking along with cryptography at intial stage. The cryptography incorporated with the Watermarking can be symmetric as well as asymmetric. The basic requirement of this kind of cryptography are given as under

Sn => A unique serial number

Pri_Key=> Private key

Pub_Key → Public key

Input_Media → Multimedia file

Sym → Symmetric key

 

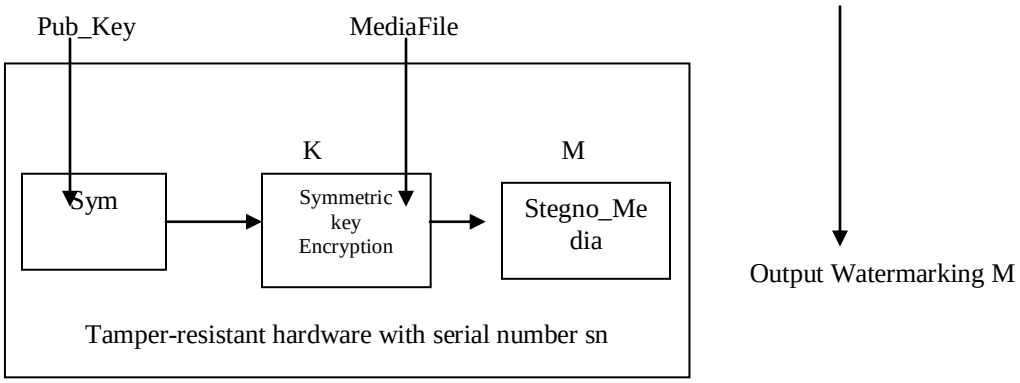


Figure 3 : Symmetric Key Cryptography based Stegnography

As we can see, the public key is defined to perform the cryptography. The media file is pass as the input to the system and the public key is used to perform the symmetric cryptography over the hidden text. As the text is encrypted, it is combined with input media and the Watermarking process is performed. Finally the encrypted text is embedded in the media file and the final secure Watermarking file is obtained as result

C) **Zhao Koch Algorithm**

It is one of the standard algorithm used to embed the copy right contents under the frequency domain. This approach is based on luminance analysis over the image so that the pixel quantization will be performed. The algorithm uses the randomly selection of the coefficient under the DCT composed matrix and based of which the bit formation and bit distribution is performed under the encoded key. The embedding process is defined under different patterns as well as under the manipulation rules. These coefficients are again modified under the bit patterns so that the embedded information can be retrieved from the system[3]

D) **Fridrich Algorithm**

This algorithmic approach is again based on the pattern analysis over the image so that the classification of areas can be done under the frequency analysis. The pattern analysis over the image is done under the randomized coefficient specification along with selection rules. The Watermarking sequence is generated from this random generated number that separate the image in black and white patterns of same size and define the blocks where data will be stored. The approach also uses the smoothing filter so that the lower frequency based filters are defined for the pattern analysis. Once the areas with specific intensity are identified, the small range and patterns are decided that will be included in the image. Approach will use these identified patterns to store the Watermarking information [7].

## 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 Eeceblдg, 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.

 