Scope International Journal of Science, Humanities, Management and Technology. ISSN : 2455-068X
Vol.3 Issue 1 (2017) 49 - 57. Submitted 4/03/2017. Published 28/03/2017

WATERMARKING TECHNIQUES USING MATLAB

R.Kuttimani, K.Sangeetha

Department of Electronics and Communcation Engineering

Dhanalakshmi Srinivasan Institute of Technology, Samayapuram, T.N, India

Abstract - Digital Watermarking is a technique by which we can easily hide a message or important task, such as an image, song, video, data bits etc. behind another signal to increase its security and confidentiality. The main aim of the paper is to focus upon various techniques to increase and study the application of the Digital Watermarking, to discuss various properties that are required in a Digital Watermarking system and to carry out various Digital Watermarking models for encryption and decryption principles. This paper has also enlightened upon the designing of various codes using MATLAB Programming to describe Digital Watermarking.

Keywords: Decryption, Digital Watermarking, Encryption, MATLAB Programming.

I. INTRODUCTION

With the growing advancement in the field of Communication, I.T. Sector etc. there is a linking between the computation and communication which offers various substantial new opportunities for processing and distribution of valuable digital creations like Email, Audio Tracks, Still Images, and Movies. At the same time, if somebody wants to access the data, the new technology makes them easier and flexible for copying and use of pirated materials across the Internet. Thus, to overcome piracy, we use encryption techniques as well as copyright principles so that only authorized users can use the data. Therefore, Digital Watermarking is basically a phenomenon by which we can easily encrypt and decrypt a data in digital format so that it can be used by authorized users and unauthorized users will not be able to decrypt the data.[1] There are various applications Digital Watermarking such as

Broadcast Monitoring.

- Owner Identification & Copyright Infringement can easily identify the owner.
- Online and Offline money transaction.
- Copy Control- to prevent illegal copying of videos, data etc.

In the present paper, we have described three basic models along with their programming codes using MATLAB Programming. These models have designed in such a way to enhance the properties and characteristics of Watermarking. There are basically two techniques or models that we have developed for the encryption and decryption of digital Watermark. These are:

- Watermarking without side-information.

- Watermarking with side-information.

II. WATERMARKING WITHOUT SIDEINFORMATION

The term side information can be defined as an auxiliary signal apart from the input signal which can be used as a key for better encryption and decryption process. The basic model for this watermarking technique is shown in fig. 1.

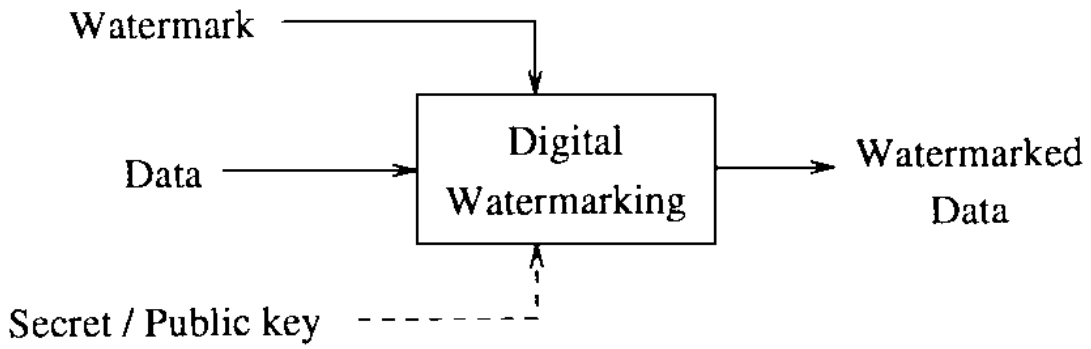

Fig.1: Representation of basic model of Watermarking

Encryption

1. Select a random reference pattern whose dimension must be the same as the original image and elements are lying in the interval [-1,1].
2. The watermarking key acts as a pseudo-random number generator and calculate the random message pattern such that whether we are embedding 1 or 0. If it is 1 leave the random reference pattern as it is and if it is 0 take the negative random reference pattern.
3. Now, scale the message pattern obtained by a constant α which is used to control the embedded strength. Initially put α=1
4. Add this scaled image with the original image to get the watermarked image.

Detector

1. Now, calculate the linear correlation between the watermarked image and the reference pattern which can be generated by using the watermarked key.
2. Now, if the result came is above the threshold value we say the message bit was 1.
3. If the result came is below the negative of the threshold value we say the message bit was 0.
4. And, if the result came is between the positive and negative value of threshold we say no message bit was embedded.

With the help of this algorithm we developed the code using MATLAB Programming for the watermarking without side information technique and develop the output graph as shown in fig.2.

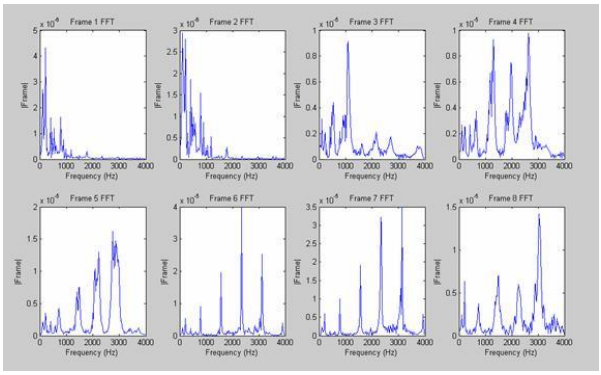

Fig.2: Representation of output waveform

Ideally, we want these three graphs to be no overlapping so that we can easily determine the threshold value to calculate the message bits being embedded. Also, this graph shows the alteration in embedding strength and the less effectiveness of the watermarked properties.

The general representation of the watermarked image is shown in fig.3.

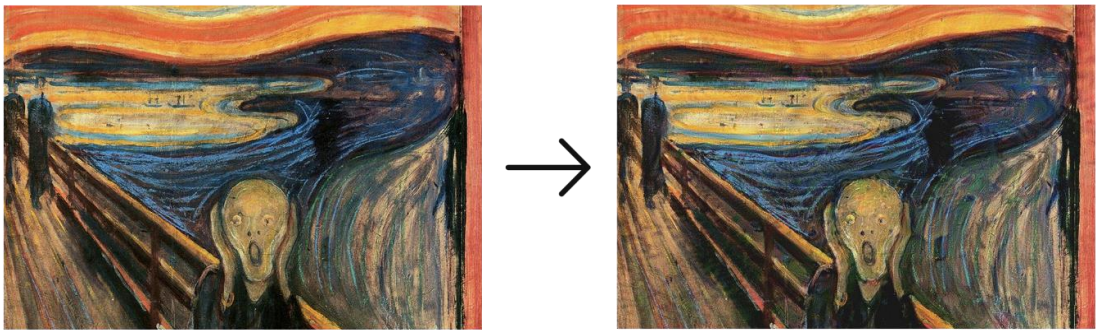

Fig.3: Representation of basic model of Watermarking without side information.

III. WATERMARKING WITH SIDEINFORMATION

The general block diagram for this technique is shown in fig.4

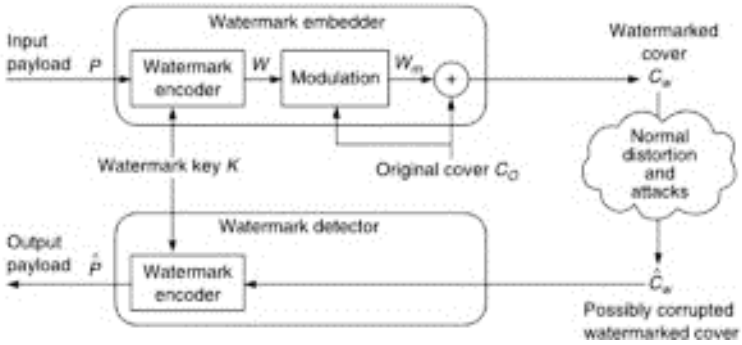

Fig.4: Representation of basic model of Watermarking with side information.

This model is similar to the above model with the only difference that the watermark encoder this time encrypts the message bits with the watermark key as well as with the individual information of the original photograph. The basic encryption and decryption techniques are discussed below.

Encryption

1. Select a random reference pattern whose dimension must be same as the original image and elements are lying in the interval [-1,1].
2. The watermarking key acts as pseudo random number generator and calculate the random message pattern such that whether we are embedding 1 or 0. If it is 1 leave the random reference pattern as it is and if it is 0 take the negative random reference pattern.
3. Here unlike above process we will going to calculate the value of α by linear correlation between watermarked image and message pattern.
4. Now scale the message pattern obtained by a constant α which is used to control the embedded strength.
5. Add this scaled image with the original image to get the watermarked image.

Detector

1. Now, calculate the linear correlation between the watermarked image and the reference pattern which can be generated by using the watermarked key.
2. Now, if the result came is above the threshold value we say the message bit was 1.
3. If the result came is below the negative of the threshold value we say the message bit was 0. 4. And if the result came is between the positive and negative value of threshold we say no message bit was embedded. With the help of this algorithm we developed the code using MATLAB Programming for the watermarking with side information technique and develop the output graph as shown in fig.5.

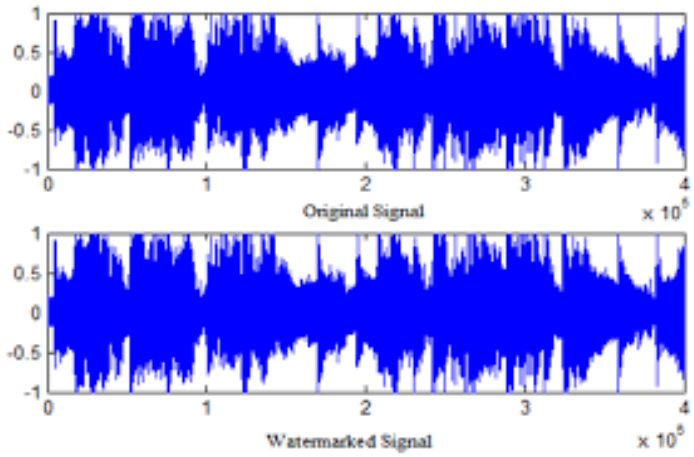

Fig.5:Representation of output waveform (Original and watermarked)

IV. RELATED WORKS

Digital Watermarking and Self-Authentication using Chirp Coding

This paper basically discusses Digital Watermarking encryption and decryption techniques using chirp coding. Chirp code is nothing but the same as linear frequency modulation. The basic technique involved in this paper is the use of a matched filter that is for the reconstruction of the chirp code which in turn used to signify the pattern of message pattern. Encryption

1. In the first step a random binary sequence is taken and after which chirp coding is carried out. The purpose of chirp coding is to 'diffuse' each bit over a range of compact support.

2. In the second step, we will develop the reference pattern of the chirp codes. for 1 we apply the chirp sin(αt2), and for 0 we apply the chirp - sin(αt2) where t is the chirp period.

3. Now the length of the chirp codes and the watermark must be the same which can be achieved by calculating a chirp constant α.

4. Now scale the message pattern obtained by a constant α which is used to control the embedded strength.

5. The basic model for the watermarked signal (which is real) is s(t) = chirp(t)xf(t) + n(t) where chirp(t) = sin(αt2) n(t)=signal on which watermark has to be added. F(t)=watermark function.

Decryption

1. For decoding or reconstruction of the message bits, a correlation is required between the chirp codes and the watermarked.
2. Now, if the result applied is +chirp then the message bit was 1.
3. And if the result applied is -chirp then the message bit was 0.

Nested Digital Image Watermarking Technique Using Blowfish Encryption Algorithm

This paper enlightens upon the Nested Digital Watermarking principle. The method involved in this watermarking technique is that the watermarked image is encrypted to a new watermarked image and this phenomenon is known as nesting of watermarking. Thus, this paper defines a model i.e. blowfish algorithm for the nesting of watermark and defines its encryption and decryption methods.

Blowfish algorithm is a Feistel network or symmetric type cryptography.

It includes two parts:

1. Key-expansion part: in this method, conversion of at most 448 bits keys to 4168 bytes several subkeys arrays is carried out.
2. Data- encryption part: In this method, 16-round Feistel network is used and in each round consists of a key-dependent permutation, data-dependent substitution and a key. All operations are XORs and additions on 32-bit words.

The paper has discussed two models for encryption and decryption of nested watermarking.

Encryption

The general block diagram for the encryption process is shown in fig.6.

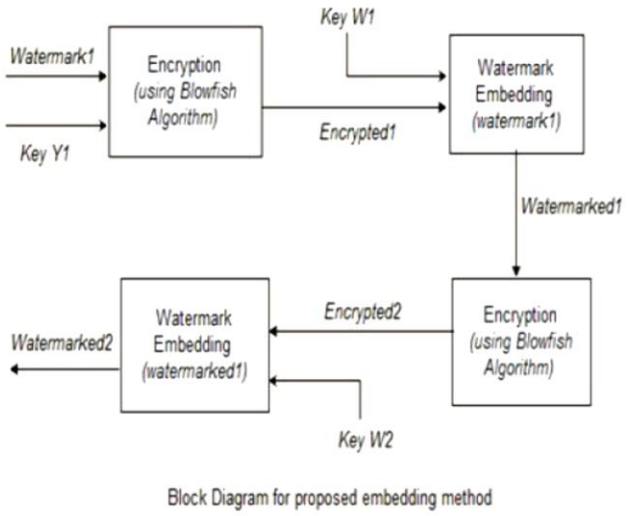

fig.6: Representation of block diagram of nested watermark encryption

As shown in figure watermark 1 is embedded into watermark 2 with the help of the blowfish algorithm. Now, this watermark 2 is again embedded into the original image by using the blowfish algorithm in order to produce the final watermarked image.

Decryption The general block diagram for the encryption process is shown in fig.7.

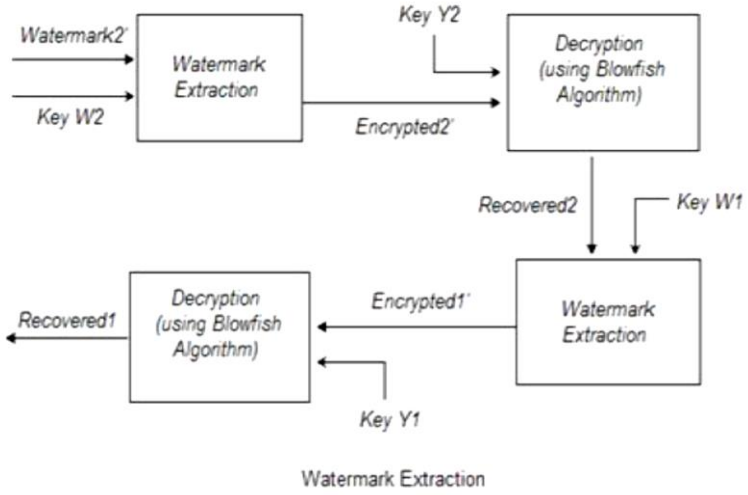

Fig.7: Representation of block diagram of nested watermark extraction

As shown in the figure the same process as discussed above for the encryption process is repeated here again. The only difference here is we repeated the process in reverse order i.e. final watermarked image will be decrypted with key k2 and the process repeated unless we receive the original signal.

V. LIMITATIONS OF THE RELATED WORKS

1. The use of the algorithm for encryption & decryption principle was complex and difficult to understand.
2. The papers were mainly focused on theoretical approach rather than the practical approach.
3. The papers were failed to discuss the features and characteristic behaviour of digital watermarking.
4. The papers discussed have broadly dependent on digital image watermarking i.e. an Image is used to hide the original signal.

VI. SYSTEM PROPOSED

The main aim of our paper is to describe a technique through which it is easy to show digital watermarking in such a way that a voice signal is used to hide a particular original signal. For this we have used Discrete Wavelet Transform principle.

Encryption

The general block diagram of the encryption technique is shown in fig.8.

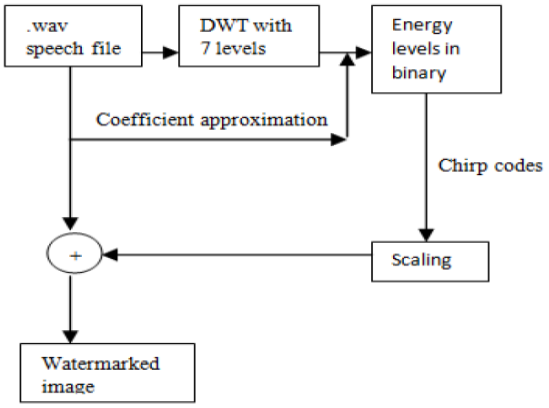

Fig.8: Representation of block diagram of DWT encryption technique

The basic steps involved are as follows:
1. Read a .wav file and extract a section of a single vector of the data.
2. Now, take the wavelet decomposition with 7 levels and also calculate the approximation coefficients for the input signal.
3. Calculate the total energy level (percentage) and present the value in binary format.
4. Now, calculate the chirp codes and pass it or scaling which is then added with the original signal to produce a watermarked image.

5. Thus, it can be seen that we have hide a signal below a voice signal. Based on above algorithm we have also developed programming codes using MATLAB.

Decryption

The general block diagram of the encryption technique is shown in fig.9.

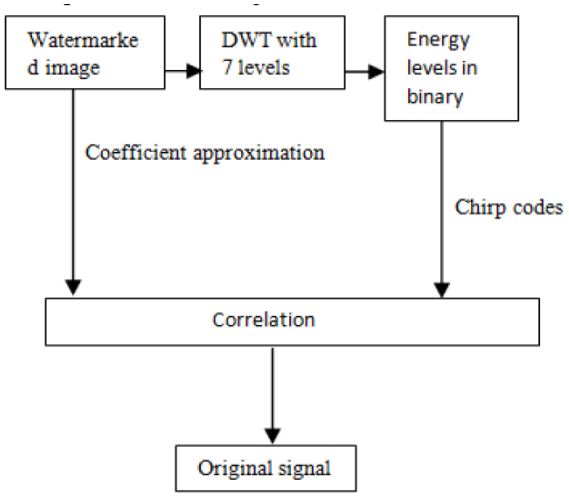

fig.9: Representation of block diagram of DWT encryption technique

1. Read a watermarked signal and extract a section of a single vector of the data.
2. Now take the wavelet decomposition with 7 levels and also calculate the approximation coefficients for the input signal.
3. Calculate the total energy level (percentage) and present the value in binary format.
4. Now, calculate the chirp codes and then correlate with the original signal to produce original signal.
5. Thus, it can be seen that we have recover the original signal.

CONCLUSION

This paper has successfully discussed various techniques for the enhancement of various watermarking properties such as effectiveness, fidelity, robust, security etc. we have also presented through this paper various encryption and decryption models for the watermarking. But since there may be many techniques and algorithm through which we can develop many models of Digital Watermarking.

REFERENCES

[1] Topic on “Robustness and Security of Digital Watermarks” ftp:// cm.belllabs.com / cm / ms /who/francis/ papers/fc98.pdf

[2] Topic on “Digital Watermarking” www.cl.cam.ac.uk/teaching/0910/R08/.../essay-ma485-watermarking.pd

[3] Topic on "Digital Watermarking and Self-Authentication using Chirp Coding" ISAST TRANSACTIONS ON ELECTRONICS AND SIGNAL PROCESSING, VOL. 1, NO. 1, 2007

[4] Topic on "Nested Digital Image Watermarking Technique Using Blowfish Encryption Algorithm" International Journal of Scientific and Research Publications, Volume 3, Issue 4, April 2013 ISSN 2250-3153

[5] Topic on "blowfish encryption algorithm"pocketbrief.net/related/BlowfishEncryption.pdf