ISSN: 0974-2115
www.jchps.com Journal of Chemical and Pharmaceutical Sciences

Covert data communication through image and audio based on watermarking scheme

S.Venkatesh
Department Of Computer Science and Engineering, Jeppiaar Engineering College
***Corresponding author: E-Mail:venkyjep@gmail.com**

ABSTRACT

In these document, we introduce the solitude of the data protection during the transmission through a network based on stego analysis. The given text data is to be embedded on the image and audio should be encrypted. The data is divided into two parts and one part of data is stored in image and another part of data in the audio. The encryption of the data is done by Chaos Encryption method. Image water marking is done by Adaptive Least Significant Bit Replacement method and audio watermarking is done by Singular Valued Decomposition method. Lifting wavelet transformation is applied to the host signal in order to decompose it and then obtain the coefficients.

KEY WORDS: Adaptive LSB Replacement, SVD technique, chaotic encryption, image and audio water marking.

1. INTRODUCTION

In recent days, secret data communication is involved in our day-to-day activities like banking, e-commerce and telecommunication. Since there is a gradual increase in the network technology, the security of the data has become weak. So the digital watermarking has been considered to be the best and safe method of data communication from side to side a system.

The process of embedding the information on another signal is known as watermarking. The watermarking should have the properties such as imperceptibility, robustness and security. The watermarking is done based on the transformation, so that a higher quality will be achieved and it will be more robust .The lifting wavelet transform is applied to decompose the original image into the sub-band images. The main applications of the digital watermarking are copyright protection and data authentication.

The chaos based encryption method provides an efficient and secured data. The data that is required for encryption is known as plain-text the encrypted data is known as cipher-text. This chaotic based systems has some properties like pseudorandom property, no periodicity and system parameters. The advantages of this method is high efficiency and simplicity.

The audio watermarking is done by the SVD method and by using this method a matrix is produced for the transformation applied signal. The SVD transformed values are more sensitive and it is difficult to be calculated from some other form of transforms. Generally the audio watermarking is done in the larger singular values. The Human Auditory System is compared to be added receptive than the person Visual System and therefore embedding on the audio is difficult. But many new methods are now available to perform the audio watermarking.

Architecture for Proposed System:

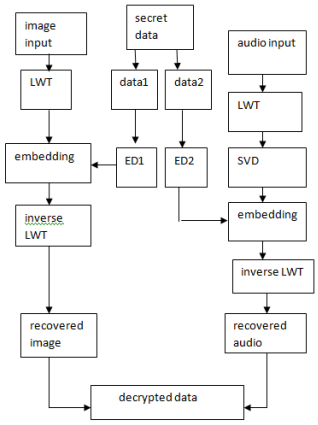

Figure.1. Proposed Block Diagram of architecture

This section explains about the overall architecture of the proposed system. The above diagram is the proposed architecture.

The input image is taken and a transformation is performed. For better performance, the Lifting wavelet transformation is performed. Simultaneously, the secret data that is to be transferred should divided into two fragments and then those data are encrypted by the chaos encryption method. After applying the transformation, one part of the encrypted data is embedded on the image by adaptive LSB method.

From the given input audio signal, a sample host signal is taken and the audio watermarking is done in it. Here too the lifting wavelet transformation is done in order to convert the floating point values into integer values.

Then the singular valued decomposition is done so that it converts the host audio signal into a matrix with non-negative scalar values. After this stage, we must embedded the another part of the embedded data to it.

Once we complete the embedding of the encrypted data on the image and audio, the inverse transformation should be done so that we can obtain the recovered image and audio signal. During this period, we obtain the encrypted data and we decrypt the data and combine them.

Algorithm: This section explains about all the algorithms that are used in the proposed system.

Stimulating base Wavelet Convert: Earlier days Fourier Transform was implemented, but it was not suitable for the non-stationary signals. In order to overcome the problems found in the Fourier Transform the Short Time Fourier Transformation was proposed. The STFT differs from the FT by dividing the signals into small segments of signals and they are considered to be stationary.

The Wavelet Transformation was implemented to overcome the limitations of the STFT. The major work of the Lifting wavelet Transform is that it decomposes the image into many different sub-band images. The sub-bands are LL, LH, HL and HH, where the L and H corresponds to the low frequency and high frequency respectively. A lower frequency small-band contain the significant part of the spatial field picture and the higher frequency small-band contain the edge information of the input image. The lifting wavelet converts the floating point co-efficient into the integer co-efficient without losing their information. These converted co-efficients are reserved for data hiding and the secret data is generally embedded on the high frequency region. The properties of the LWT are easily invertible and real time possessions.

- Vertical wise process to obtain X and Y

X = Ao - Be

Y= Be + [X/2]

- Horizontal wise process to obtain LL,LH,HH,HL

Adaptive LSB Method: The idea of flexible LSB is to put in the bit of the secreted point into the least significant bits of the pixel. Now a fake random producer is use to erratically distributed and cover the bit of a covert point keen on the lower significant bits of the pixel surrounded by a delivery service picture called the envelop picture.

Now the confidential data is embed at the rightmost bits so that the original pixel value is not affected. The Least bit is proficient with double corresponding technique:

- Encrypt of the point.
- Randomize the position of the bits by means of a cryptographic random purpose.

LSB Replacement: In a dreary plane picture, each pixel consist of 8 bits. Single pixels can display 28=256 variation. The arithmetical illustration for least bit technique is:

- a represent the p'th pixel charge of the stego picture.
- p a represent the unique wrap picture.
- p q represent the decimal rate of the p'th slab in secret information.
- The numeral of least bit to be substitute is denoted as r.
- A Easy variation of the extract p q gives the unique secret information.

Chaos Encryption: This algorithm is an advanced one used for encryption of information. Commotion encryption is use to mix up a picture apart from set aside space to make guard of picture particulars during communication. This encrypts the unique picture pixel value with encryption solution value generate from confused series with doorstep purpose by bitxor process. Now logistic chart is use for production of confused chart series.

The wide chaos encryption technique is the easiest method to encrypt film data or point by chaotic formula. The chaos encryption process flow is as follows, the input image is bitxored with the threshold function and the encrypted image is obtained. It is given as

$E_{ij} = P_{ij}$ (bitxor) I

For calculating threshold function, we first need to find chaotic sequence generation. The chaotic sequence generation is

$X_{n+1} = u*x(1-x)$

From here using the values of X_{n+1} the threshold function is calculated. The threshold function is calculated as

$(I/255) < X_{n+1} < (I+1)/255$

Here for each iteration I value increments and for what value the condition satisfies is the value of X. Likewise the threshold function is calculated. Now both the chaotic sequence value and the threshold value is bitxored. And the encrypted image is obtained.

SVD method: The SVD is a numerical analysis tool for matrices. The properties of SVD are transpose, scaling, rotation, flipping and stability. SVD is used to transform the input audio signal into a matrix with non-negative scalar values. The SVD of the N*N matrix is

$$I = USV^T$$

where U and V are unitary matrices, S is the diagonal matrix and T is the transpose of the matrix. The diagonal elements are arranged in the decreasing order. SVD should satisfy the following

- audio quality should not be affected
- should satisfy intrinsic algebraic properties

The SVD is applied on the host audio signal and three matrices U, V and S are obtained. The data to be embed is inserted into the diagonal matrix and SVD is applied to it and new matrices are obtained. Finally the matrices U, V^T and S are multiplied.

2. EXPERIMENTATION

This section describes about the experimentation and implementation of this paper.

Implementation: This paper has been implemented in the MATLAB R2007b on an intel core i5 processor windows 7 workstation. The blue plane is separated from the color image using the commands in the MATLAB tool.

3. EXPERIMENTATION RESULTS

This section deals with the outcome that are obtain by implement the algorithm. The subsequent outcome are obtain in MATLAB. The above screen shot represents the choosing of an input image. This is the wrap image in which the manuscript data is secreted. Here the indigo plane is divided from the tint picture. The records is secreted in the blue plane because of its high intensity. When the plane is separated the single plane becomes a gray image. Since its intensity is high, the information that is store in the blue plane cannot be hacked.

Figure.2.Choose an input image

Figure.3. Plane Partition

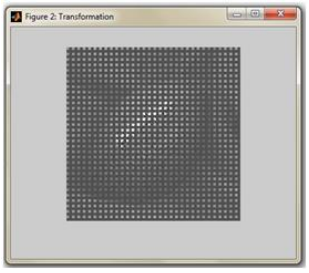

Figure.4. Transformed image

The image is transformed using Lifting Wavelet Transform. The data is hidden in the high frequency regions. The transformed image contains 256 pixels. Here the data is hidden in HH, HL and LH regions.

The data is hidden in the cover image. And the above image is the stego image in which the data is hidden. The data that is hidden is encrypted by using Chaos encryption method. After data hiding the quality of the image should not be reduced.

Figure.5. Stego Image

Figure.6. Recovered Image

Using Inverse Lifting Transformation, the cover image is recovered. Similarly, by using Chaos decryption the hidden data is recovered.

4. CONCULSION AND FUTURE WORK

In this paper, the data can be transmitted more securely, using the adaptive LSB method and SVD techniques for watermarking the image and audio respectively. The quality of the original image and the audio is maintained even after the watermarking. By applying the transformation before SVD we can obtain the optimal performance in the robustness and transparency. The performance metrics such as hit the highest point signal to sound ratio, mean square mistake and correlation are calculated.

In future we can use different algorithms to encrypt the data before embedding it on the image and audio.

REFERENCES

Amy Tun and Yadana Thein, Digital Image Watermarking Scheme Based on LWT and DCT, IACSIT International Journal of Engineering and Technology, 5(2), 2013.

Baiying Lei, Student Member, IEEE, Ing Yann Soon and Ee-Leng Tan, Robust SVD-Based Audio Watermarking Scheme With Differential Evolution Optimization, IEEE transactions on audio, speech, and language processing, 21(11), 2013.

Chih-Chin Lai, A digital watermarking scheme based on singular value decomposition and tiny genetic algorithm", Elseiver, 2011.

Gnanajeyaraman R, Prasadh K, Ramar, Audio encryption using higher dimensional chaotic map, International Journal of Recent Trends in Engineering, 1(2), 2009.

Sakthidasan K and Santhosh Krishna B.V, A New Chaotic Algorithm for Image Encryption and Decryption of Digital Color Images, International Journal of Information and Education Technology, 1(2), 2011.

Vivekananda Bhat K, Indranil Sengupta, Abhijit Das, An adaptive audio watermarking based on the singular value decomposition in the wavelet domain, Elseiver, 2010.