COVERT INFORMATION COMMUNICATION THROUGH IMAGE AND AUDIO BASED ON WATERMARKING SCHEME

S. Venkatesh[1] and M. A. Dorairangaswamy[2]
[1]Department of Computer Science, Sathyabama University, Chennai, India
[2]St peter's University, Avadi Chennai, India
E-Mail: venkyjep@gmail.com

ABSTRACT

In this paper, we present the privacy 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 watermarking 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 inorder to decompose it and then obtain the coefficients.

Keywords: adaptive LSB replacement, SVD technique, chaotic encryption, image, audio watermarking.

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 way of data transmission through a network.

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 system has some properties like pseudorandom property, no periodicity and system parameters. The advantage 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 more sensitive than the Human Visual System and therefore embedding on the audio is difficult. But many new methods are now available to perform the audio watermarking.

2. ARCHITECTURE FOR PROPOSED SYSTEM

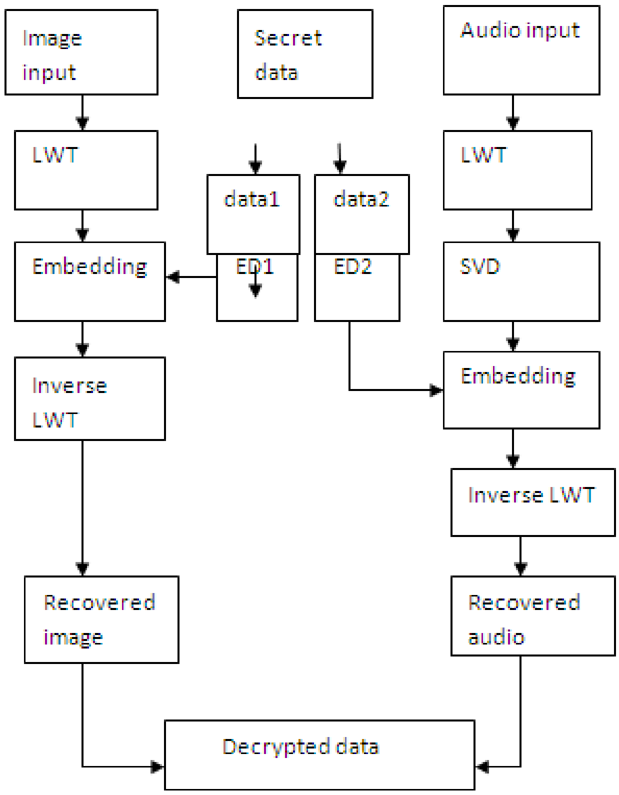

Figure-1.

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.

3. ALGORITHM

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

A. Lifting based wavelet transform

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 correspond to the low frequency and high frequency respectively. The low frequency sub-band contains the important parts of the spatial domain image and the high frequency sub-band contains 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 property.

- Column wise processing to obtain H and L

H = Co - Ce
L = Ce + [H/2]

- Row wise processing to obtain LL,LH,HH,HL

LH = Lodd - Leven
LL = Leven + [LH/2]
HH = Hodd - Heven
HL = Heven + [HH/2]

B. Adaptive LSB method

The idea of Adaptive LSB is to insert the bits of the hidden message into the least significant bits of the pixels. Here a pseudo random generator is used to randomly distribute and hide the bits of a secret message into the least significant bits of the pixels within a carrier image called the cover image.

Here the confidential data is embedding at the rightmost bits so that the original pixel value is not affected. The LSB is accomplished with two complementary techniques:

- Encryption of the message.
- Randomizing the placement of the bits using a cryptographical random function.

LSB substitution

In a gray level image, every pixel consists of 8 bits. One pixel can hence display 28=256 variations. The mathematical representation for LSB method is:

- x represents the i'th pixel value of the stego image.
- i x represents the original cover image.
- i m represents the decimal value of the i'th block in confidential data.
- The number of LSB's to be substituted is denoted as k.

A simple permutation of the extracted i m gives the original confidential data.

C. Chaos encryption

This algorithm is an advanced one used for encryption of data. Chaos encryption is used to scramble an image except reserved space to make protection of image details during transmission. It encrypts the original image pixel values with encryption key value generated from chaotic sequence with threshold function by bitxor operation. Here logistic map is used for generation of chaotic map sequence.

The broad chaos encryption method is the simplest technique to encrypt video data or message by chaotic equation. 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.

VOL. 11, NO. 21, NOVEMBER 2016 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

Likewise the threshold function is calculated. Now both the chaotic sequence value and the threshold value is bitxored. And the encrypted image is obtained.

D. 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.

4. EXPERIMENTATION

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

A. 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.

B. Experimentation results

This section deals with the results that are obtained by implementing the algorithms. The following results are obtained in MATLAB.

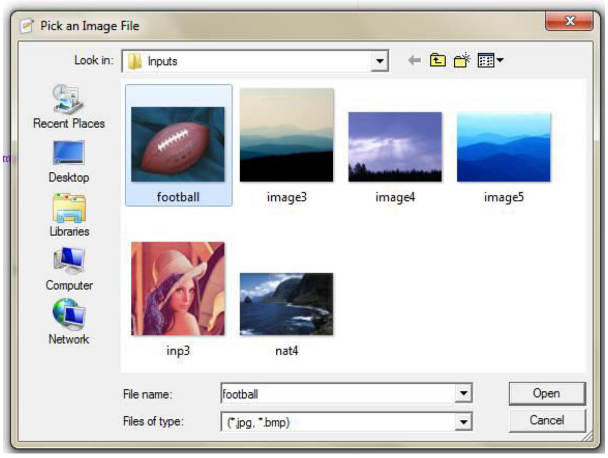

Figure-2. Choose an input image.

The above screen shot represents the choosing of an input image. This is the cover image in which the text data is hidden.

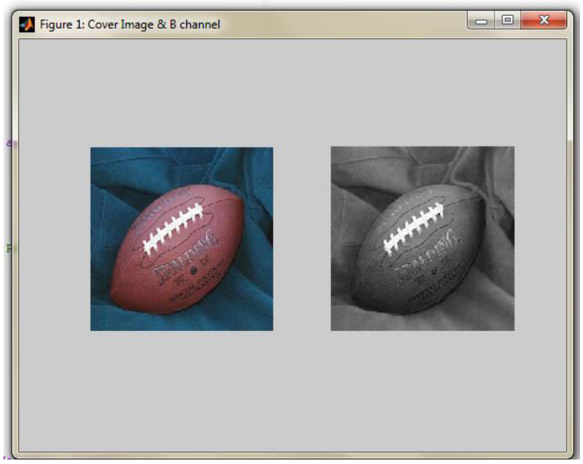

Figure-3. Plane separation.

Here the blue plane is separated from the color image. The data is hidden 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 data that is stored in the blue plane cannot be hacked.

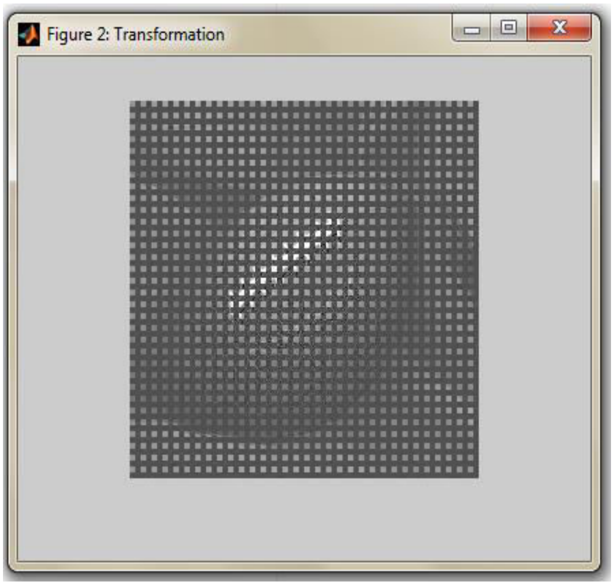

Figure-4. Transformed image.

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.

ARPN Journal of Engineering and Applied Sciences

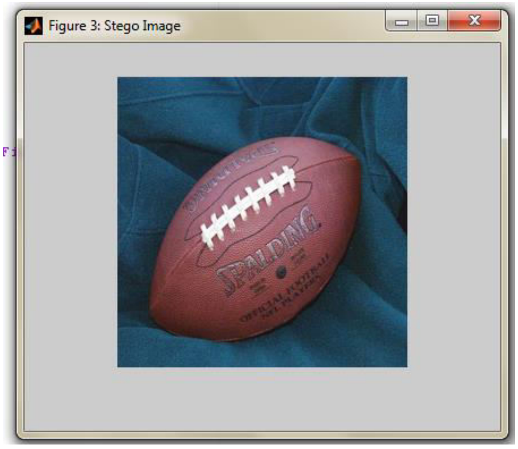

Figure-5. Stego image.

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.

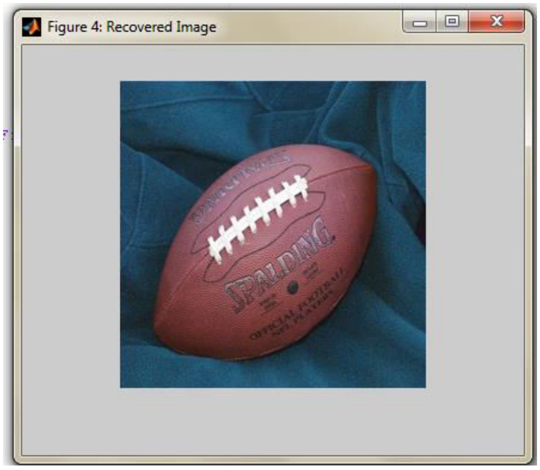

Figure-6. Recovered image.

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

5. CONCLUSION 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 peak signal to noise ratio, mean square error and correlation are calculated.

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

REFERENCES

Jila Ayubi, Shahram Mohanna, Farahnaz Mohanna and Mehdi Rezaei. 2011. A Chaos Based Blind Digital Image Watermarking in The Wavelet Transform Domain. IJCSI International Journal of Computer Science Issues. 8(Issue 4, No 2).

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

Niladri Ghosh and K. Pradeep Vinaik. 2012. A Lifting Based Wavelet Transform VLSI architecture for image processing", IMACST. 3(3) June.

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

V. Padmanabha Reddy and Dr. S. Varadarajan. 2010. An Effective Wavelet-Based Watermarking Scheme Using Human Visual System for Protecting Copyrights of Digital Images. International Journal of Computer and Electrical Engineering. 2(1).

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

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

Bai Ying Lei n, Ing Yann Soon, Zhen Li. 2011. Blind and robust audio watermarking scheme based on SVD–DCT. Elseiver.

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

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

Huan Zhao, Fei Wang, Zuo Chen, Jun Liu. 2014. A Robust Audio Watermarking Algorithm Based on SVD-DWT. Elektronika Ir Elektrotechnika, ISSN 1392-1215, 20(1).