Transform Domain Based Digital Image Watermarking For Data Hiding Progression

Sabarinathan.R[1], Anbukaruppusamy.S[2], Kandasamy.R[3]

[1, 2, 3]Dept of ECE

[1, 2, 3] Excel Engineering College, Namakkal, Tamil Nadu, India

Abstract*- The project proposes the enhancement of protection system for secret data communication through encrypted data concealment in encrypted images. The image is then separated into number of blocks locally and lifting wavelet will be used to detect approximation and detailed coefficients. Then approximation part is encrypted using chaos encryption method. The proposed encryption technique uses the chaos encryption and enhances the safety of secret carrier information by making the information inaccessible to any intruder having a random method. After image encryption, the data hider will conceal the secret data into the detailed coefficients which are reserved before encryption. Although encryption achieves certain security effects, they make the secret messages unreadable and unnatural or meaningless. This system is still enhanced with encrypt messages. This is the reason a new security approach called data hiding arises. It is the art of hiding the existence of data in another transmission medium to achieve secret communication. The data hiding technique uses the adaptive LSB replacement algorithm for concealing the secret message bits into the encrypted image. In the data extraction module, the secret data will be extracted by using the encrypted pixels to extract the data. Finally the performance such as PSNR, MSE, CORRELATION of this proposal in encryption and data hiding will be analyzed based on image and data recovery.*

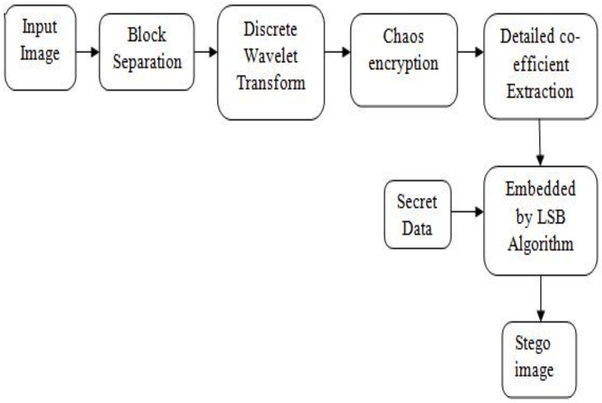
Keywords*-* chaos encryption, DWT based watermark embedding, LSB algorithm, MSE, PSNR.

I. INTRODUCTION

Steganography is the technique of hiding confidential information within any media. Steganography is often confused with cryptography because the two are similar in the way that they both are used to protect confidential information. The difference between the two is in the appearance in the processed output; the output of steganography operation is not apparently visible but in cryptography the output is scrambled so that it can draw attention. Steganalysis is process to detect of presence of steganography. Most of the steganography techniques use images a steno-medium. Information can be hidden in images through many different ways. The most common approaches to information hiding in images are: LSB Algorithm insertion, Masking and filtering techniques, Algorithms and transformations. Masking and filtering techniques hide information by marking an image in a manner similar to paper watermarks. The LSB insertion is the most widely used image steganography technique. It embeds message in the least-significant bits of each pixel. In order to increase the embedding capacity, two or more bits in each pixel can be used to embed message, which has high risk of delectability and image degradation. The LSB techniques might use a significant bit insertion scheme, in which the bits of data added in each pixel remains constant, or a variable least significant bit insertion, in which the number of bits added in each pixel vary on the surrounding pixels, to avoid degrading the image fidelity In this paper we discuss the embedding of text into image through variable size least significant bit insertion. The process of insertion of text in our proposed approach is not sequential; rather it follows a random order, based on a random algorithm. The technique proposed aims at providing not only maximum insertion capacity, but also performs a maximum analysis of surrounding pixels to determine the embedding capacity of each pixel. The process results in a stego-image which is very much similar in appearance to the original image. We propose a steganography model that ensures maximum embedding of information in both gray scalable and colored images, and also ensures that maximum pixels are analyzed to determine the embedding capacity. This would lead to a reduction of the overall error induction in the image. The stego-image obtained after application of this analysis would not only have maximum amount of information, but would also have the minimum difference in appearance with the original image. Steganography is one of the most vital research subjects in the field of security communications. It differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret. Another form of information hiding is digital watermarking, which is the process that embeds data called a watermark, tag or label into a multimedia object such that watermark can be detected or extracted later to make an assertion about the object. The object may be an image, audio, video or text only.

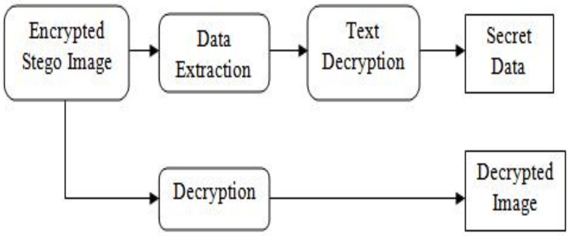
II. PROPOSED METHODS

The sender side is designed to ensure secure information hiding with use of LSB algorithm. Before that DWT can be used, it allows the image decomposition in different kinds of coefficients preserving the image information. Such coefficients coming from different images can be appropriately combined to obtain new coefficients so that the information in the original images is collected appropriately. Moreover, the chaos encryption technique contains an authentication stage to prevent unauthorized users from extracting the hidden information.


Input Image
Block Separation
Discrete Wavelet Transform
Chaos encryption
Detailed co-efficient Extraction
Secret Data
Embedded by LSB Algorithm
Stego image

(A) Block Diagram of Sender side

The receiver side first extracts the co-efficient same as that of generated in the sender side. After that, extract the secret data that was hiding in the image .The watermark extraction process is almost similar to the watermarking embedding process**.**



(B) Block Diagram of receiver side

III. TREE STRUCTURE BASED WATERMARK EMBEDDER

The tree structure based watermark embedder is designed to embed the binary watermark bits into the selected bitplanes of the selected DWT coefficients of the selected trees. In the pro-posed scheme, the tree structure based watermark embedder has three functions: forming the tree structure, selecting the trees and the DWT coefficients for the watermark embedding, and

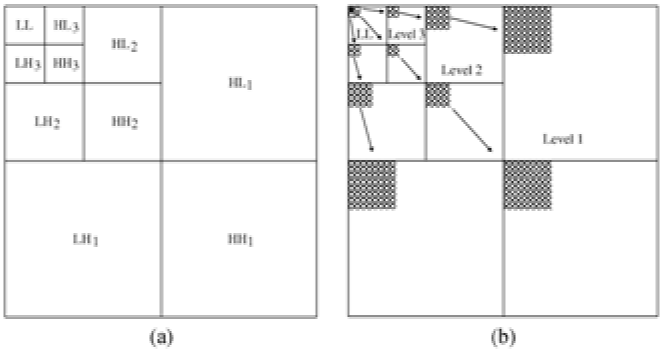


Illustration of the 3-level DWT decomposed subbands (a) and the for-mation of tree structure (b).

efficients with both odd horizontal and odd vertical coordinates have no descendants. Only the coefficients with at least one even coordinate have descendants and we define these coefficients as the roots of the trees. For the DWT coefficients with odd horizontal and even vertical coordinates, all their descendants are located in the detail subbands.

For the coefficients with even horizontal and even vertical co-ordinates, all their descendants are in the detail subbands. Correspondingly, all the descendants for the coefficients with even horizontal and odd vertical coordinates are in the subbands. Each root has descendants in the corresponding detail subbands on level, where is the total number of DWT decomposition levels and in this paper. Therefore, 3072 trees can be formed for a 512 X 512 image. The number of the selected trees can be evenly distributed in the three orientations, and or more in some orientation(s) and less in the other(s). With the formation of the tree structure, the locations for the watermark embedding can be more flexibly chosen. Moreover, the watermark bits can be embedded into the selected trees with different embedding strengths.

IV. CHAOTIC ENCRYPTION SCHEME

The broad chaos encryption method is the simplest technique to encrypt video data or message by chaotic equation. This method can facilitate to discover some essential information and establish the crucial stage of security. The advantage of chaotic encryption is High level security. The encryption is achieved by iteration. Simplest. No short cuts are available. Whereas the requirement of large cipher storage and slow in speed are considered the major disadvantages. The properties of chaos are slightly producing some changes in the entire cryptography.. In an initial condition, chaotic is always sensitive. Hence it will produce a slight difference in trajectory. It gives the totally different trajectory sectional value. Identical trajectory only can produce the same values. The topology transitivity defines that the state points reside in a bounded space state and approaches the chaotic encryption method is proposed by (Baptista). It seems to be a much better encryption algorithm than traditional algorithms were used. We first identify the mapping scheme for a trajectory to encrypt the message. Subsequently decide the initial state and parameters for the key. We assume the initial condition as the current route (trajectory). Iterate the chaotic equation until the path reaches the target site and then store the amount of iterations as a code for each message symbol. Encrypt the next message by iterating the recent trajectory. Produce the next cipher according it and so on.

V. LSB EMBEDDING

Least Significant Bit (LSB) embedding is a simple strategy to implement steganography. Like all steganographic methods, it embeds the data into the cover so that it cannot be detected by a casual observer. The technique works by replacing some of the information in a given pixel with information from the data in the image. While it is possible to embed data into an image on any bit-plane, LSB embedding is performed on the least significant bit(s). This minimizes the variation in colors that the embedding creates.

For example, embedding into the least significant bit changes the color value by one. Embedding into the second bit-plane can change the color value by 2. If embedding is performed on the least significant two pixels, the result is that a color in the cover can be any of four colors after embedding. Steganography avoids introducing as much variation as possible, to minimize the likelihood of detection. In a LSB embedding, we always lose some information from the cover image. This is an effect of embedding directly into a pixel. To do this we must discard some of the covers information and replace it with information from the data to hide. LSB algorithms have a choice about how they embed that data to hide. They can embed lossless, preserving all information about the data, or the data may be generalized so that it takes up less space.

VI. PERFORMANCE MEASURES

(A) PSNR – PEAK SIGNAL TO NOISE RATIO

Peak signal-to-noise ratio, often abbreviated PSNR, is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. Because many signals have a very wide dynamic range, PSNR is usually expressed in terms of the logarithmic decibel scale.

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

Where,

I Corresponds to original image.
K Corresponds to stego image

$$PSNR = 20.\log_{10}(MAX\ I) - 10.\log_{10} MSE$$

(B) CORRELATION

Digital image correlation (DIC) techniques have been increasing in popularity, especially in micro- and nano-scale mechanical testing applications due to its relative ease of implementation and use. Advances in computer technology and digital cameras have been the enabling technologies for this method and DIC has been extended to almost any imaging technology.

The correlation coefficient between A and B, where A and B are matrices or vectors of the same size is defined as

$$r = \frac{\sum_m\sum_n\left(A_{mn} - \bar{A}\right)\left(B_{mn} - \bar{B}\right)}{\sqrt{\left(\sum_m\sum_n\left(A_{mn} - \bar{A}\right)^2\right)\left(\sum_m\sum_n\left(B_{mn} - \bar{B}\right)^2\right)}}$$

Where $\bar{A} = mean(A), and\ \bar{B} = mean(B)$.

VII. SOFTWARE DESCRIPTION

A. MATLAB SIMULATOR (VER 8.0)

MATLAB is a high-performance language for technical computing. It integrates computation, visualization, and programming in an easy-to-use environment where problems and solutions are expressed in familiar mathematical notation.

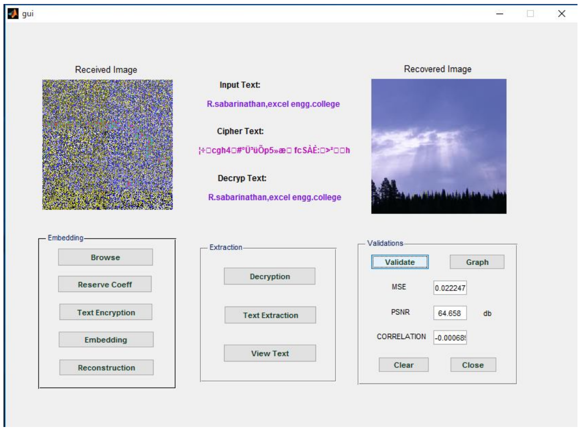
B. GUI

A graphical user interface (GUI) is a user interface built with graphical objects, such as buttons, text fields, sliders, and menus. In general, these objects already have meanings to most computer users. For example, when you move a slider, value changes; when you press an OK button, your settings are applied and the dialog box is dismissed. Of course, to leverage this built-in familiarity, you must be consistent in how you use the various GUI-building components.

Applications that provide GUIs are generally easier to learn and use since the person using the application does not need to know what commands are available or how they work. The action that results from a particular user action can be made clear by the design of the interface.

C. IMPLEMENTATION & RESULT

In Wavelet transforms there is a push toward the use of wavelets in signal processing and analysis in place of (or in addition to) the Discrete Wavelet Transform (DWT), which is used in the JPEG standard for image compression.
Recently, many algorithms have been proposed to use wavelets for image compression. The techniques that are currently being used in working with images can be generalized for use with wavelet transforms.



Input Text:
R.sabarinathan,excel engg.college

Cipher Text:
¦÷□cgh4□#°Ü³üÕp5»æ□ fcSÀÈ:□>²□□h

Decryp Text:
R.sabarinathan,excel engg.college

MSE 0.022247

PSNR 64.658 db

CORRELATION -0.00068!

VIII. CONCLUSION

The steganography is used in the covert communication to transport secrete information. In this project, Data hiding using Watermarking is proposed. The secret message is embedded into input image. The chaos encryption and LSB algorithm process were added with it. Presently, this application supports hiding data in images and videos. The improvement of this application would be extending its functionality to support hiding data in video files or in other file format.

REFERENCES

[1] Sha Wang, Dong Zheng, Jiying zhao, "Adaptive Watermarking and Tree structure Based Image Quality Estimation", (2014) IEEE Transactions on Multimedia, vol. 13, no. 2.

[2] Ming Li, Shucheng Yu, Yao Zheng, Kui Ren, and Wenjing Lou, „„Scalable and secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption", (2013) vol. 24, no. 1, pp. 131-143.

[3] Xinpeng Zhang,"Seperable Reversible Data hiding in Encrypted Image",(2012) IEEE Transactions on Security And Information Forensics, vol.7, no.2.

[4] Zhenxing Qian, Xinpeng Zhang, Shuozhong Wang ,"Reversible Data Hiding in Encrypted JPEG Bit stream", (2014) IEEE Transaction on Multimedia, vol.13, no.2.

[5] W.Lee and C.Lee, "A Cryptographic key management Solution for hipaa security Regulations"", (2008) vol. 12, no. 1, pp. 34-41.

[6] I.J.Cox, M.L.Miller, J.A.Bloom, "Digital Watermarking and Steganography", (2008) San Mateo, CA, USA: Morgan Kaufmann.

[7] A.Mishra, A.Jain, C.Agarwal ,"An Experimental Study into Objective Quality Assessment of Watermarked Images", (2011), Int.Journal Image Process.,Vol.5,no.2, pp.199-219.

[8] X.Zhang,"Data Hiding With Optimal Value Transfer", (2013) IEEE Trans. Multimedia,vol.15, no.2,pp316-325.

[9] T.Bianchi, A.Piya," On the implementation of the discrete Fourier Transform in the encrypted domain",(2009) IEEE Trans. Inform. and Security, Vol.4, no.1,pp.86-97.