RESEARCH ARTICLE OPEN ACCESS

RSA Based Secured Image Steganography Using DWT Approach

E. Yuva Kumar, P. Padmaja
Department of Electronics & Comm Engg. Sree Vidyaniketan Engineering College. Tirupati, Andhra Pradesh, India
Department of Electronics & Comm Engg Sree VidyaNiketan Engineering College. Tirupati, Andhra Pradesh, India

Abstract
The need for keeping safe secrecy of secret and sensitive data has been ever increasing with the new developments in digital system. In this paper, we present an increased way for getting embedding encrypted secret facts in gray scale images to give high level safety of facts for news over unsecured narrow channels Cryptography and Steganography are two closely related techniques are used in proposed system. Cryptography gets into making one of religion the secret note into a non-recognizable chipper. Steganography is then sent in name for using Double-Stegging to fix this encrypted data into a cover thing by which something is done and keeps secret its existence.

Keywords: Steganography, Cover Image, Information, Stego Image, Discrete Wavelet Transform (DWT), RSA Approach, Bit Length.

I. INTRODUCTION

In information hiding watermarking and Steganography are two closely related techniques. The basic difference between the two is that former is a way used for copyright system of care for trade while the latter is a way of getting fixed secret data into a covered media so that purposeless recipients will not have way in to the data. Steganography not only keeps secret the data, but also keeps secret the fact that a secret data is being sent. However, cryptography is different from Steganography since a chipper text has undetectable from and the existence of a secret data is measurable by bad attackers. Still, Cryptography techniques can be did, gave effect to on secret data before getting fixed in to still image; to make stronger safety level and also to put out of the way the energy compaction of secret data. This paper uses the idea of RSA Algorithm for data encryption, where the data will be converted into a chipper, which will be then put out of the way into an image. In order to enable large amount of room of data and supporting good seeing quality of the cover image, embedding is sent in name for by modifying the details coefficients in make great change lands ruled over of Two–Dimensional DiscreteTransform (DWT). Furthermore, to give greater value to the safety level of the data, the idea of Double-Stegging is used to fix the data into the image. The best advantages chances of this system are that it does not have need of the first form cover image for good extraction of the secret data.

II. CRYPTOGRAPHY

Cryptography is the art of safe-keeping of information by transforming into an unpredictable form. This unpredictable form is named as “cipher text”. It gets into the use of a “key “by which the encryption and decryption is done. The purpose of Cryptography is to keep not to access contents of secret data by unauthorized person. Cryptography plays an major role in secret data through untrusted media.

The requirements of a Cryptographic system are:

a. Authentication: the process of making identity to one who gets in.
b. Privacy: making certain that data is not getting stretched to any purposeless one who gets.
c. Integrity: making certain that the one gets is able to get out the what is in of the decrypt the note in its first form.

The different types of Cryptography used are:

1. Symmetric Cryptography: It uses a single key far both encryption and decryption.
2. Asymmetric Cryptography: it uses two keys one for encryption and one for decryption.
3. One-way Cryptography: it uses mathematical transforms change so that the fact is not retrievable.

III. RSA ALGORITHM

RSA Algorithm is developed by three sciencetis Ronald Rivest, Adi Shamir and Leonard Adleman. This method uses public key cryptography; it involves two keys private key and public key [6]. The key- pairs are derived from a large integer which

is the product of two prime numbers chosen as per some special rule.
The step by step process of the RSA algorithm is as follows

1. Select two prime numbers, x and y from these numbers multiple x and y and calculate the modulus, n=xy
2. Select a third numbers 'e' that is relatively prime to the product (x-1)(y-1).The number 'e' is the public exponent.
3. Generate a private key by choosing a number d, which is multiple inverse of e mod ϕ(n).
4. Encrypt a message m, raise m to the power e under modulo n. the result is the chipper text(c).
5. Decrypt the chipper text, raise the cipher to the power d under modulo n..

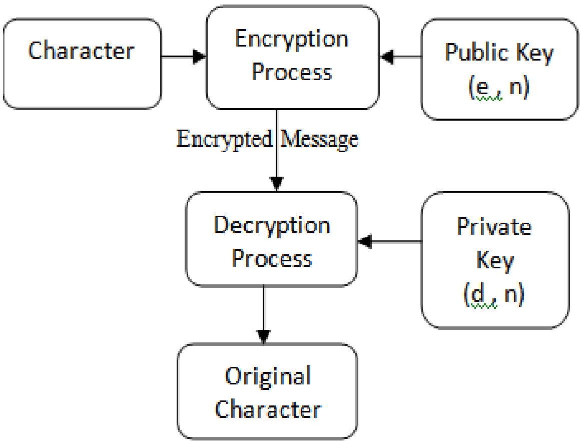

Fig1: RSA Message

IV. STEGANOGRAPHY

Steganography is type of hiding data that means "covered writing" it is taken from Greek words stego means "covered" and graphos means " to write" .The purpose of Steganography is to embed S secret data into a cover image in such a way that it will not be able to discover that a secret data has existence in the image. The Steganographic, system necessarily needs a cover media which has redundant bits i.e., bits which can be made an adjustment without causing destruction the good nature of the media [4]. The way of doing is to put back the redundant bits of the media with that of the secret data to be embedded. A Steganographic system is represented by three different parameters which are deeply related, viz. capacity, security, and robustness.

Capacity refers to something about to the amount of data which can be safely stored in the media. Security is the notable of an undesired one going into get out the put out of the way data from the media and robustness is the amount of adjustments that the stego-media can take without causing destruction the secret data.

V. STEGANOGRAPHY SYSTEM

Steganography uses secret key to encrypt the hidden message that that will be encapsulated inside a cover media. Modern steganographic system, as shown in figure 2 is detectable only if secret information is namely "secret key". In this case cryptography should be involved which holds that a cryptographic system's security should trust on the key matter. Steganography is a technique used to store the secret data in the enclosed image and secret data in to undetectable form. Steganography [2] takes cryptography a step farther by hiding an encrypted message so that no one suspects it exists. Ideally, anyone scanning your data will fail to know it contains encrypted data.
Three basic types of stego-systems are available:
Pure stego systems - no key is used.
Secret-key stego systems - secret key is used.
Public-key stego systems - public key is used.

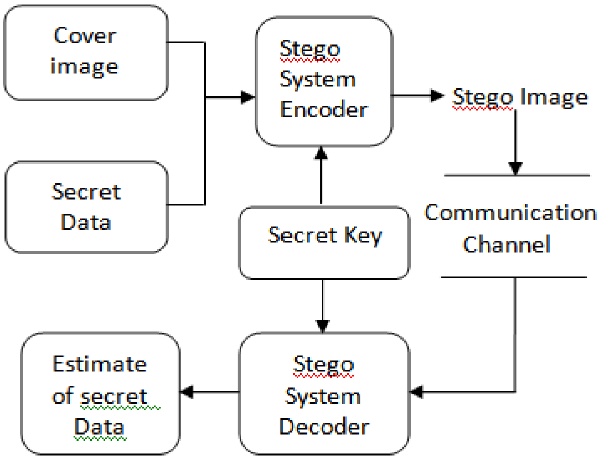

Fig2: Modern Stego-System

The various Steganography techniques used are:

A. Spatial Domain Technique:

In this method the pixels of the covered image is to store the secret data. There are various such techniques are namely LSB, PVD, and GLM

Least significant bits (LSB):

In least significant bit (LSB), each pixel of an image is transformed into the binary value and data [5] is hidden into the least significant position of the binary value of the pixels of the image in such a manner that, it doesn't destroy the reliability of the cover image but this scheme is sensitive to a variety of image processing attacks like compression, cropping etc.

Pixel Value Differencing (PVD):

In addition, our new method avoids the falling-off-boundary problem by using pixel-value differencing and the modulus function. First, we derive [3] a difference value from two consecutive pixels by utilizing the pixel-value differencing technique (PVD). The hiding capacity of the two consecutive pixels depends on the difference value. In other words, the smoother area is, the less secret data can be unseen; on the contrary, the more edges an area has, the more secret data can be embedded. The stego image quality dilapidation is more imperceptible to the human eye.

Gray Level Modification (GLM):

A new image steganography method for hiding data using Gray Level Images in Spatial Domain is proposed in this paper. This method is an improvement over in advance methods like least significant bit (LSB) method and gray level modification (GLM) method [6]. This method retains the advantages of above said methods but discards the disadvantages related with above methods and provides us the better results.

B. Transform Domain Technique:

The transform domain techniques make use of the transform coefficients to hide the data. The secret data is embedded by modifying the transform coefficients of the image, which makes this technique more strong to attacks like compression, filtering etc. The different techniques used are DCT and DWT.

Discrete Cosine Transform (DCT):

The discrete cosine transforms (DCT) & discrete wavelet transform (DWT) are mathematical utility that transforms digital image data from the spatial to the frequency domain. In DCT, after transforming the image in frequency domain, the data is embedded in the least significant bits of the medium frequency components and is individual for lossy compression.

Discrete Wavelet Transform (DWT):

In DWT, secret messages are embedded in the high frequency coefficients resulted from Discrete Wavelet Transform and make available maximum robustness. wavelet is simply, a small wave which has its energy got, came jointly at one point in time to give a person used by another for the analysis of transient, non-stationary or time-varying events. The DWT [2] core may be used for image processing operations, such as denoising and image compression. The wavelet transform way makes great change the original signal using selected before wavelets by sending at special quick rate the first form signal as sum and product of coefficients and function. A two parameter system is made such that one has a double sum and coefficient with two indices. The groups of coefficients are called the Discrete Wavelet Transform (DWT) [1] of the signal. Thus the signal is calculated by analyzing these coefficients. encrypted secret data. The proposed method combines the features of cryptography and Steganography were encryption and embedding are done in two stages stenographic model lies in the actuality that the wavelet transform clearly separates the high frequency and low frequency in order on a pixel by pixel basis.

VI. PROPOSED METHOD

To provide high level security of data proposed method processes gray scale image as covered object for embedding

DWT:

Wavelet transform is used to convert a spatial domain into frequency domain. The use of wavelet in image Since the LPF is a half band filter [4], there are two output data sub sampled are generated. So the output data contains only half the original number of samples. Next, HPF is applied for the same row of data and separate high pass component and low pass section is placed beside the high pass component. This is done for all rows. The resulting two-dimensional array of coefficient contains four sub-bands [3] of data each as labeled as LL (Low-Low), LH (Low-High), HL (High-Low), HH (High-High). The LL can be decomposed once again in the same manner, the process can be done up to any level that will result in a pyramidal decomposition.

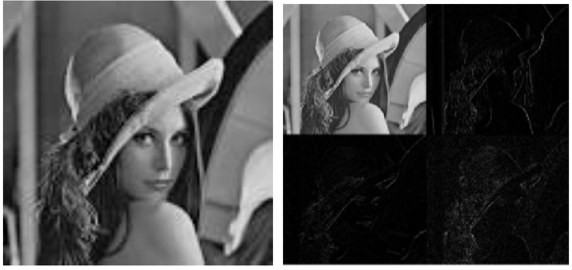

Fig: DWT

Stage-1: Encryption using RSA Algorithm

In this first stage, the secret data is encrypted using the public key in RSA algorithm. This proposes a cipher text along with the public encryption and private decryption keys. This cipher text is converted into 8-bit binary codes for further use in the second stage.

Stage-2: Embedding using Double Stegging.

In this stage, the data in the binary form is embedded into the cover image and hides its existence. It utilizes transform coefficients of 2-Dimensional Discrete Wavelet Transform (2-DWT) by using Haar,s wavelet for embedding process. The chosen cover image is decomposed [6] by DWT transform. This transform provides one approximation and three detail coefficients (horizontal, vertical, and diagonal) on each decomposition level. Generally, approximation coefficients are not suitable for embedding because they carry the majority information content of the whole cover image. Therefore, the detail coefficients are the most convenient area for secret message embedding.

Fig: Stego- Image

A Extraction Process:

The extraction process requires two stage of decoding in order to recover the original secret data. The first stage decoding is done to recover the first details coefficient from the second details coefficient.

$$S_{ij} = \begin{cases} 0\ If\ c_{ij}\ mod1 = 0 \\ 1\ If\ c_{ij}\ mod1 \neq 1 \end{cases}$$

The second stage decoding involves recovering the original secret data from the first details coefficient. The criteria for extraction of the secret data are. The process consists of the simple modulo operation of stego image coefficients. The advantage of this method is that the original cover image does not have to be nearby on the receiver side for the successful rebuilding of the original data. Therefore, the risk of disclosure of secret communication is lower.

B Decryption:

This cipher text is decrypted by using the private key by RSA algorithm. One important necessity which has to be considered is the in order capacity of the method. The distortion of cover object caused by embedding the secret data increases as the amount of data being embedded increase. Comparison of method could be individual by payload in relation to PSNR value.

VII. Results and Discussions

In this project analysis we propose a new steganography technique which embeds the secret messages in frequency domain. According to different users' stress on the embedding capacity and image eminence, the proposed algorithm is divided into two modes and 5 cases. Unlike the space domain approaches, secret messages are embedded in the high frequency coefficients resulted from Discrete Wavelet Transform. Coefficients in the low frequency sub-band are preserved unaltered to get better the image quality. Some basic mathematical operations are performed on the secret messages before embedding. These operation and a well-designed mapping Table keep the messages away from theft, destroying from unintended users on the internet and hence provide acceptable security by using stego-key analysis.

VIII. CONCLUSION

The proposed method posses with very good visual excellence of the stego-image and also the algorithm allow variety in accomplishment to acquire desired robustness, and fault open-mindedness The capacity of the method remains the same and it is represented by ¼ of cover image size for 1-level decomposition of the cover image. The payload is 0.25 bit/pixel incase of using the maximum capacity and it also varies depending on number of detail coefficient are used during the embedding phase. The proposed algorithm employs 1-level decomposition of the image hence the total ability is represented by ¼ of image size number of DWT detail coefficient, which are altered.

REFERENCES

[1] Chandra M. Kota and Cherif Aissil. "*Implementation of the RSA algorithm and its Cryptanalysis*", ASEE Gulf southwest Annual Conference on 2002, Houston, USA.

[2] Vladimfr BANOCI, Gabriel BUGAR, Dusan LEVICKY, "*A Novel Method of Image Steganography in DWT Domain*", Technical University of Kosice, Slovak Republic.

[3] Colm Mulcahy Ph.D, "*Image Compression using Haar Wavelet Transform*", Spelman Science and Math Journal, 22-31.

[4] Mamta Juneja, Parvinder S. Sandhu, Ekta Walia, "*Application of LSB Based Steganographic Technique for 8-bit Color Images*", World Academy of Science, Engineering and Technology, 2009.

[5] R. L. Rivest. A. Shamir and L. Adleman, "*A method for obtaining digital signatures and public key cryptosystems*," Commun. ACM, Vol. 21, No. 2, pp. 158-164, Feb 1978.

[6] Ismail Avcıbas, Member, IEEE, Nasir Memon, Member, IEEE, and Bulent Sankur, Member, "*Steganalysis Using Image Quality Metrics*," IEEE Transactions on Image Processing, Vol 12, No. 2,February 2003.

[7] Calderbank R., Daubechies I., Sweldens W., and YeoL.,"*Lossless Image Compression Using Integer to Integer Wavelet Transforms*," in Proceedings of International Conference on Image Processing, USA, pp. 596-599, 1997.

[8] Lin T. and Delp J., "*A Review of Data Hiding in Digital Images*," in Proceedings of the Image processing, Image Quality, and Image Capture conference, Georgia, pp. 274-278, 1999.

[9] Vijay Kumar Sharma, Vishalshrivastava, "*A Steganography Algorithm for Hiding Images by improved LSB substitution by minize detection*."Journal of Theoretical and Applied Information Technology, Vol. 36 No.1, ISSN: 1992-8645, 15th February 2012.