Advanced Data Security Using Hybrid Cryptography and Steganography

ITHUPUDI CHAKRA LAKSHMI[1], S. SURYA GODHA DEVI[2]

#1 M.Tech Scholar (CSE), Department Of Artificial Intelligence & Data Science,
#2 Assist. Prof, Department of Artificial Intelligence & Data Science, KIETW, Kakinada, AP, India.

Abstract:
Steganography is the science that includes imparting mystery information in a suitable sight and multimedia bearer, e.g., picture, sound, and video records. In this paper, we propose a changed secure steganography plan concealing a largesize dim picture into a little size dark picture. Preprocessing is initially performed both on spread and mystery pictures. Arnold change is performed on the mystery picture and the high security and vigor accomplished by utilizing this change. Integer Wavelet Transform (IWT) is performed in spread picture. The spread picture Coefficients of the wavelets are adjusted with the commotion inside average level. Apply Integer wavelet change (IWT) to get the Stego-picture. The limit of the proposed calculation is expanded as the main estimation band of mystery picture is considered. The extraction model is really the opposite procedure of the inserting model. Exploratory results demonstrate that our strategy gets stego-picture with perceptual intangibility, high security and certain power. Ideal Pixel Adjustment procedure is likewise received to minimize the distinction mistake between the data spread picture and the inserted picture and to expand the concealing limit with low twists individually.

Keywords — *Cryptography, Steganography, LSB, Hash-LSB, RSA Encryption -Decryption*

I. Introduction

Steganography is a procedure that shroud the mystery data or message into a spread media.Cover media can be a picture or a sound or video record. There are two primary steganography procedures: Spatial Domain and Transform Domain. Spatial – space strategies insert messages in the power of the pixels specifically, while for change – otherwise called recurrence – area, pictures are initially changed and afterward the message is installed in the picture. Picture space procedures incorporate piece insightful strategies that apply bit insertion and commotion control and are at times portrayed as "straightforward frameworks". The picture arranges that are most suitable for picture space steganography are lossless and the systems are regularly subject to the picture group. Steganography in the change area includes the control of calculations and picture changes. These techniques stow away messages in more huge regions of the spread picture, making it heartier. Numerous change space routines are free of the picture position and the installed message might survive transformation in the middle of lossy and lossless pressure. In the following areas steganographic calculations will be disclosed in classes as per picture document groups and the space in which they are performed. Despite the fact that there are couple of exploration being led in past [6][7] in the range of steganography, yet greater part of the earlier research work has some or other constraint as far as subtlety. On the other hand, the looks into directed in wavelet change [8][9] and Genetic Algorithm [10] can be considered as benchmark for further extensibility of the current framework. Another examination hole in the comparative issue is greater part of the former work don't consider hearty RS-investigation [1], which is a standout amongst the most conspicuous achievement component for steganography application. RS examination is an uncommon instance of Sample pair investigation, which additionally utilizes slightest huge piece alteration as a part of request to ascertain an expected installing rate. Test pair investigation [10] sends limited state machines to characterize gatherings of pixels adjusted by a given example.

II. RELATED WORK

Taras Holotyak e.t. al [13] propose another strategy for estimation of the quantity of implanting changes for nonadaptive ±k installing in pictures. The comparative creator [4] has additionally advocate another way to deal with visually impaired steganalysis in view of arranging higher-request measurable components got from an estimation of the stego signal in the wavelet space. Agaian and Perez [5] propose another steganographic approach for palette-based pictures. This new technique has the benefit of inserting secure information, inside of the file, the palette or both, utilizing extraordinary sorting plan. The displayed system additionally fuses the utilization shading demonstrate and cover picture measures keeping in mind the end goal to choose the best of the contender for the insertion of the stego data. Chen and Lin [6] propose another steganography method which installs the mystery messages in recurrence space to demonstrate that the PSNR is still a palatable esteem even the most noteworthy limit case is connected. As per the reproduction comes about, the PSNR is still a palatable esteem even the most elevated limit case is connected. This is because of the diverse qualities of DWT coefficients in distinctive sub-groups. Since the most fundamental divide (the low recurrence part) is kept unaltered while the mystery messages are inserted in the high recurrence sub-groups (comparing to the edges bit of the first picture), better PSNR is not an astounding result. Moreover, respectable security is kept up too since no message can be separated without the ―Key matrix‖ and deciphering rules. Kathryn Hempstalk [7] explores utilizing the spread's unique data to abstain from making blemishes on the stegoobject, by concealing crude electronic documents inside advanced shading pictures. This paper has presented two new strategies for picture steganography, FilterFirst and BattleSteg. These two methods endeavor to enhance the viability of the using so as to cover up edge recognition channels to create better steganography. Wang and Moulin [8] demonstrated that the freely and indistinguishably dispersed unit exponential dissemination model is not an adequately exact portrayal of the measurements of the standardized periodogram of the full-casing 2-D picture DFT coefficients. Park e.t. al [9] propose another picture steganography system to confirm whether the mystery data had been erased, produced or changed by assailants. The proposed strategy shrouds mystery data into spatial space of advanced picture. In this paper, the uprightness is checked from removed mystery data utilizing the AC coefficients of the discrete cosine change (DCT) space. Ramani, Prasad, and Varadarajan [20] propose a picture steganography framework, in which the information concealing (installing) is acknowledged in bit planes of subband wavelets coefficients acquired by utilizing the Integer Wavelet Transform (IWT) and Bit-Plane Complexity Segmentation Steganography (BPCS). Farhan and Abdul [1] has exhibited their work in message covering systems utilizing picture based steganography. Anindya e.t. al [2] exhibit further expansions of yet another steganographic plan (YASS), a system in view of inserting information in randomized areas to oppose blind steganalysis. YASS is a JPEG steganographic procedure that shrouds information in the discrete cosine change (DCT) coefficients of arbitrarily picked picture pieces. Adnan Gutub e.t. al. [3] converge between the thoughts from the arbitrary pixel control systems and the stego-key ones to propose our work, which utilizes the minimum two noteworthy bits of one of the channels to demonstrate presence of information in the other two channels. This work indicated appealing results particularly in the limit of the information bits to be covered up with connection to the RGB picture pixels. Mohammed and Aman [4] utilizes the Least Significant Bits (LSB) insertion to conceal information inside encoded picture information. Aasma Ghani Memon e.t. al. [25] gives another skyline to safe correspondence through XML steganography on Internet. Zaidan e.t. a.l. [6] has exhibited a model for insurance of executable records by securing spread document without constraint of concealed information size utilizing calculation in the middle of cryptography and steganography. Vinay Kumar and Muttoo [27] has talked about that chart theoretic way to deal with steganography in a picture as spread item helps in holding all bits that take part in the shading palette of picture. Wang e.t. al. [8] presents another steganography in light of hereditary calculation and LSB. Souvik Bhattacharyya and Gautam Sanyal [9] propose a novel steganographic technique for concealing data in the change area of the dim scale picture. The proposed approach works by changing over the dark level picture in change space utilizing discrete whole number wavelet system through lifting plan. Nadia M. Mohammed [3] has displayed four new routines in steganography frameworks to insert mystery information in compacted pictures. Two techniques are working in spatial area, known as moving window and odd/even LSB, others are working in change space, known as odd/even DCT and DCT+DWT. Zaidan e.t. al.[3] has proposed a multi-spread steganography utilizing remote detecting picture. Shaamala e.t. al. [2] has considered the impact DCT and DWT spaces on the impalpability and heartiness of Genetic watermarking. Aftereffects of watermark picture quality and assaults taking into account top sign to-clamor proportion (PSNR) numerical connection (NC) is broke down, and the DWT results indicated more strength high intangibility than DCT in watermarking in light of GA. Shiva Kumar e.t. al [3] propose Performance Comparison of Robust Steganography Based on Multiple Transformation Techniques (PCRSMT). The spread picture is partitioned into 64 pieces of 4*4 each and DWT is connected to every square. The subsequent 64 squares of vertical band of 2x2 each are secluded and IWT is connected to get 1x1 pieces. The DWT and IWT are connected to payload and IWT coefficients of payload are installed with that of spread picture. IDWT and IIWT are connected to infer stego picture. Moreover blunder recognition and rectification system is additionally connected to guarantee more secured correspondence. It is watched that the vigor and limit are enhanced with next to no tradeoff.

III. EXISTING TECHNOLOGIES

Hiding of data inside an image is simply called steganography. A lot of steganography techniques are used frequently to cover an information, [7] is an image steganography technique and [8] is an JPEG based steganography technique. Several spatial domain techniques are considered. In that the easiest method is LSB (Least Significant Bit) Steganography. In this paper for discussion we have considered LSB steganography and

RGB steganography. There exists two types of LSB steganography methods – LSB1 Steganography and LSB2 steganography. RGB Steganography also have a lot of variations similarly.

LSB-1 STEGANOGRAPHY

This is the simplest of the steganography methods based in the use of LSB, and therefore the most vulnerable. Embedding process consists of the sequential substitution of each Least Significant Bit (LSB-1) of the image pixel for the bit message [17][2] [9] [12]. For its simplicity, this method can camouflage a great volume of information. The guidelines are given below:
Step1: Convert the data from decimal to binary.
Step 2: Read cover image.
Step 3: Convert the cover Image from decimal to binary.
Step 4: Break the byte to be hidden into bits.
Step 5: Take first 8 byte of original data from the cover Image.
Step 6: Replace the least significant bit by one bit of the data to be hidden.
First byte of original information from the Cover image:
E.g.:-1 1 0 11 0 0 0
First bit of the data to be hidden: 1 Replace the least significant bit

1	1	0	1	1	0	0	0

□

1	1	0	1	1	0	0	1

This process will be continued for first 8 byte of data and conceal the first byte of data.
Step 7: Continue the step 6 for all pixels.
Images after embedding data using LSB-1 Steganography.

Fig.1. Cover Image

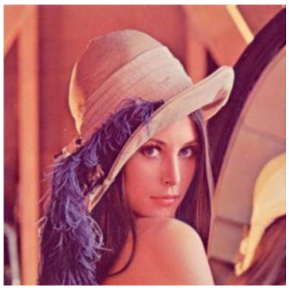

Fig.2. Stego Image

LSB –2 STEGANOGRAPHY

In LSB-2 Steganography the data embedding process is slightly different. It alters the 2nd bit from right for all pixels [17]. The algorithm is as follows:
Step1: Convert the data from decimal to binary.
Step 2: Read Cover image.
Step 3: Convert the Cover Image from decimal to binary.
Step 4: Break the byte to be hidden into bits.
Step 5: Take first 8 byte of original data from the Cover Image.
Step 6: Replace the least significant bit by one bit of the data to be hidden.
First byte of original information from the Cover Image:
E.g.:- 1 1 0 1 1 0 0 0
First bit of the data to be hidden: 1 Replace the least significant bit

1	1	0	1	0	0	0	0

□

1	1	0	1	1	0	1	0

This process will be continued for first 8 byte of data and conceal the first byte of data.

Step 7: Continue the step 6 for all pixels.

After applying the algorithm the images are

Fig.3. Cover image

Fig.4. Stego image

RGB STEGANOGRAPHY

To a computer an image is an array of numbers that represent light intensities at various points (pixels) these pixels makeup the image‟s data. Digital images are normally stored in either 24-bit (RGB) or 8-bit (Grayscale) files. A 24-bit image provides the most space for hiding information; however it can be quite large (except JPEG images). All colors are derived from three primary colors: red, green, and blue. Every primary color is represented by one byte i.e. each pixel represents a combination of (R, G, B).

Different RGB based algorithms are used [10] [11] etc for steganography. Each have advantages and disadvantages from the existing techniques. Dynamic RGB based approach [11] is used to change the least significant bits of pixel values (3) or sometimes (4) of the rearrangement of colors to create parity bit patterns or least significant bit which correspond to the message being hidden. Also variable bit steganography technique is used in RGB based steganography [4].

Image after embedding the data using RGB steganography technique.

Fig.5. Cover image

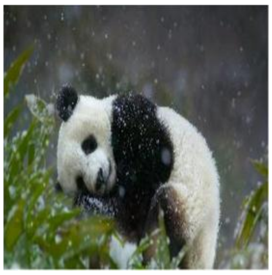

Fig.6. Stego image

IV. PROPOSED TECHNIQUE

The proposed a technique in this paper is RGB pixel value based steganography method. The specialty of this algorithm is that we do not change the pixels like other steganography algorithms except if it is absolutely needed. To a computer an image is a collection of data/information that represents light intensities at various points (pixels) these pixels making up the image‟s raster data. All Digital images are typically stored in either (24-bit) RGB or (8-bit) known as Grayscale files. A 24-bit image provides the most space for hiding information; however it can be quite large (with the exception of JPEG images). All color combinations are derived from three primary colors - red, green, and blue. Each of this primary color is represented by one byte.

Because RGB values are all represented by numbers, we can make use of this numbers to represent text using a modbit algorithm. So what is a modbit algorithm? A modbit algorithm is very similar to the Luhn mod n algorithm. Traditionally a Luhn mod algorithm is widely used for generating checksum formula for validating credit card numbers, IMEI numbers etc. As part of this paper we have taken the concept used in Luhn mod N algorithm [18] but for finding the pixels which can represent a character. Each character from the input text will be mapped to a set of numbers and this mapping will be maintained internally in the Stegano program [15]. For example letter „a‟ could be represented by digit 10, letter „b‟ could be represented by digit 12 and so forth. During the encryption process the Stegano program will scan the image and will add the RGB values, divide it and find the mod value. If mod matches the character, that location in the image could be used to represent the character.

But then problem arises on how will we be able to store the location of a pixel which can identify a character? We can either store it in a separate text file or make it as part of the image metadata itself. To make it easy in this paper we are proposing to make it part of the image metadata itself.

Finally there will be also cases when we may not find a pixel in an image that might not be able to represent a particular character. In these cases the work around is to alter some of the places in an image to a nearest possible pixel such that it can represent the character and at the same time will be not identifiable by human eye.

ENCRYPTION PROCESS

Step 1: The application prompts for the text and image from the sender who wants to hide the message.
Step 2: Steganographic program encrypts the text using DES or RSA or any other encryption algorithm.
Step 3: Steganographic program analyses the image to find the pixel value of all the pixels within the image.
Step 4: Steganographic program uses the unique RGB modbit method to find out whether each letter of the message can be represented in the image and records the position to a field in the image metadata itself. For calculation of modbit the program adds the RGB values of each pixel and divides it to get the mod. If the mod value matches with that represented for the character internally, the position for that character is recorded.
Step 5: If the image does not have pixel values to represent a particular character, the steganographic program finds and changes a pixel that almost matches with the image pixel and which can represent the character of text.
Step 6: Finally when all the pixels which can be identified on the image and its position is recorded along with the image metadata, the user is informed that the encryption part is
complete.

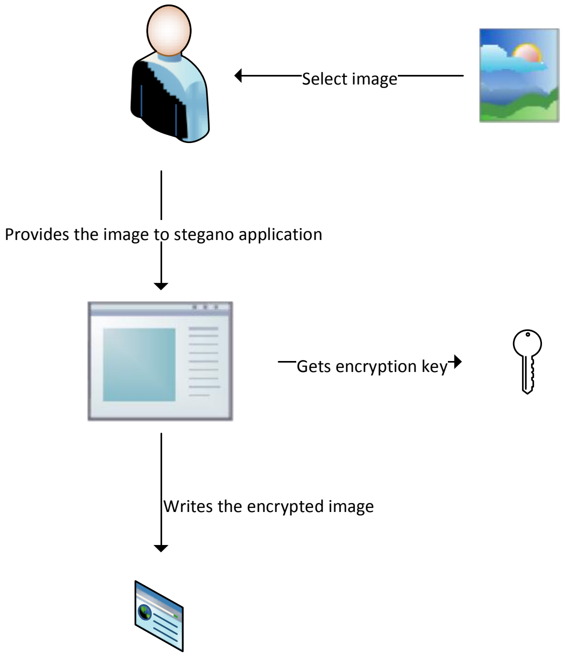
Select image
Provides the image to stegano application
Gets encryption key
Writes the encrypted image

Fig.7. Data Embedding process

```
For all characters in the message text
{
        for all pixels in the image (all rows and columns)
                {
        Add the RGB values and find mod by division.
Compare with modbitvalue with the internal table of values for the character maintained inside the stegano program.  if values match then encrypt the pixel position and add it to the image meta data and exit this loop continue with next character
        exit the loop and continue with next character
                        else
                                Continue with next pixel end if
If none of pixel can represent the text change a pixel towards the edges to the nearest value which can represent the character and store it.
                }
 }
```

Embedding Algorithm:

The advantage of this proposed technique is that it will not degrade the image quality as it depends on the pixel values. Hence the covering image and the stego image will not have any visual difference and will also be prone from any sort of attacks.

DECRYPTION PROCESS

Step 1: The receiver opens the image.
Step 2: The steganographic software asks for key to decrypt the image file.
Step 3: Steganographic software decrypts the metadata first and finds the pixel positions.
Step 4: Using the pixel positions, get the RGB values and decodes by reverse modbit and finds the corresponding encrypted text.

Step 5: Decrypt this text and provide back the message to the user.

```
Get the key
For all characters in the image metadata
{
        For all pixels in the image
    {
      Find the modbits from the pixels positions specified
      Decrypt the modbits
     Display the character continue with next character
    }
}
```

Extracting Algorithm:

Since the reverse modbit algorithm is hidden within the software only this decryption program will be able to decrypt the message. Any other method of trying to get the text will result in failure

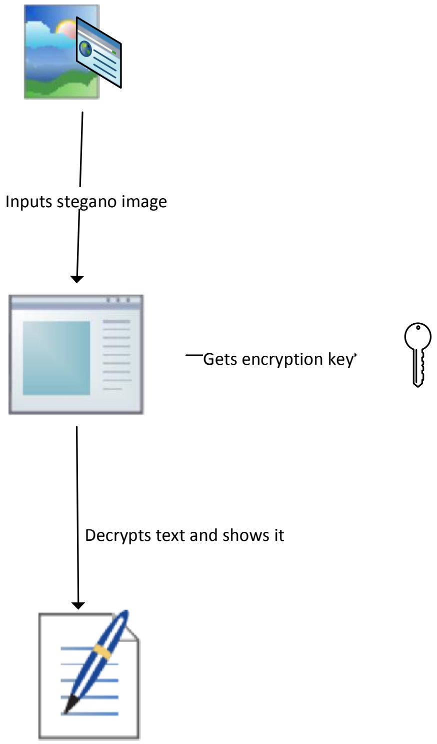

Fig.8. Data extraction process

V. Conclusion and Future Scope

A secured Hash based LSB technique for image steganography has been implemented. An efficient steganographic method for embedding secret messages into cover images without producing any major changes has been accomplished through Hash-LSB method. In this work, a new way of hiding information in an image with less variation in image bits have been created, which makes our technique secure and more efficient. This technique also applies a cryptographic method i.e. RSA algorithm to secure the secret message so that it is not easy to break the encryption without the key. RSA algorithm itself is very secure that’s why we used in this technique to increase the security of the secret message. A specified embedding technique uses hash function and also provide encryption of data uses RSA algorithm; makes our technique a very much usable and trustworthy to send information over any unsecure channel or internet. The H-LSB technique have been applied to .tiff images; however it can work with any other formats with minor procedural modification like for compressed images. Performance analysis of the developed technique have been evaluated by comparing it with simple LSB technique, which have resulted a very good MSE and PSNR values for the stego images. The future scope for the proposed method might be the development of an enhanced steganography that can have the authentication module along with encryption and decryption. Meanwhile the work can be enhanced for other data files like video, audio, text. Similarly the steganography technique can be developed for 3D images. The further work may contain combination of this method to message digesting algorithms.

References

[1]. S. M. Masud Karim, Md. Saifur Rahman, Md. Ismail Hossain “A New Approach for LSB Based Image Steganography using Secret Key”, International Conference on Computer and Information Technology (ICCIT), Pages No. 286 – 291, 22-24 Dec., 2011.

[2]. Kousik Dasgupta, J. K. Mandal, Paramartha Dutta, “Hash Based Least Significant Bit Technique for Video Steganography (HLSB)”, International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, Issue No. 2, April, 2012.

[3]. Mamta Juneja, Parvinder Singh Sandhu, “Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption”, International Conference on Advances in Recent Technologies in Communication and Computing, Pages No. 302 – 305, 27-28 Oct., 2009.

[4]. Swati Tiwari, R. P. Mahajan, “A Secure Image Based Steganographic Model Using RSA Algorithm and LSB Insertion”, International Journal of Electronics Communication and Computer Engineering (IJECCE), Vol. 3, Issue No. 1, 2012.

[5]. N. F. Johnson, S. Jajodia, "Steganography: seeing the unseen”, IEEE Computer, Vol. 31, Issue No. 2, Pages No. 26 - 34, Feb., 1998.

[6]. Wien Hong, Tung-Shou Chen, "A Novel Data Embedding Method Using Adaptive Pixel Pair Matching", IEEE Transactions on Information Forensics and Security, Vol. 7, Issue No. 1, Pages No. 176 - 184, Feb., 2012.

[7]. Amr A. Hanafy, Gouda I. Salama, Yahya Z. Mohasseb, "A Secure Covert Communication Model Based on Video Steganography", Military Communications Conference, IEEE, Pages No. 1 – 6, 16-19 Nov., 2008.

[8]. R. Chandramouli, N. Memon, "Analysis of LSB based image Steganography techniques", International Conference on Image Processing, Vol. 3, Pages No. 1019 – 1022, 07 Oct 2001-10 Oct, 2001.

[9]. Weiqi Luo, Fangjun Huang, Jiwu Huang, "Edge Adaptive Image Steganography Based on LSB Matching Revisited", IEEE Transactions on Information Forensics and Security, Vol. 5, Issue No. 2, Pages No. 201 – 214, June, 2010.

[10]. Ross J. Anderson, Fabien A. P. Petitcolas, "On the Limits of Steganography", IEEE Journal on Selected Areas in Communications, Vol. 16, Issue No. 4, Pages No. 474 – 481, May, 1998.