ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

The Improved Image Steganography with Encryption Method and to Overcome the Compression Technique

Ashwini W, Nagraj Kyasa

M.Tech Student, Department of ECE, Don Bosco Institute of Technology, Bangalore, India

Asst. Professor, Department of ECE, Don Bosco Institute of Technology, Bangalore, India

ABSTRACT: The security of the secret data has been an important subject of concern since the antiquity. Steganography and cryptography are the two techniques used to reduce the security threat. Cryptography is an art of turning the secret message into a form other than human. Steganography is an art of concealing the existence of the secret message. These techniques are necessary to protect data theft in a fast growing network. To achieve this there is a need of such a system which is very susceptible to human visual system. The secret data is compressed first using SPIHT algorithm before embedding it behind any media cover. Data is compressed to reduce its size. After compression data encryption is performed to increase the security. Encryption is performed with the help of a key which makes it difficult to get the secret message even if the existence of the secret message is revealed.

I. INTRODUCTION

Steganography is an art of hiding information in a way that prevents the detection of hidden messages and this is achieved by hiding one piece of information within another piece of innocent-looking information. There are several methods of embedding data, such as spatial and time domain methods, Transform domain methods and fractal coding methods. These methods hide / embed information in different types of media such as text, image, audio, video, etc. Varieties of different file formats, digital images are considered the most popular type of carriers because of their size and frequency of distribution.
A digital image is a two-dimensional function f (x, y) where, x and y are spatial coordinates, f is the amplitude in (x, y), also called intensity or gray level of the image at that point yx, Finite and discrete quantities. Digital image processing is the use of computer algorithms to perform the image processing in digital images. It allows a wider range of complex and sophisticated algorithms that are applied to digital images easily and in a much more effective way compared to analog signal processing.

Image steganography is the steganography subdivision where digital images are used as information carrier file formats. The joint image format (JPEG), the graphics exchange format (GIF), the bitmap (BMP) image format and the Portable Network Graphics (PNG) format are the most popular image file formats Share on the Internet.

Steganography is the art of hiding messages in a medium called a cover object in such a way that the existence of the message is undetectable. Imperceptibility is clearly the most important requirement. In steganographic schemes. The cover object can be a digital image, an audio file or a video archive. The secret message called payload could be plain text, an image, a video file or an audio. Steganographic methods are classified in the domain spatial domain and domain incorporation Embedding In the frequency domain, images are transformed into frequency components DCT, FFT or DWT and then the messages are embedded in the bit level or in the block level. In Space domain LSB replacement is the most widely used data hiding method. However, most of the LSB techniques are prone to seizures. Due to the low computational complexity and high This work is mainly concerned with the LSB steganography method.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

Steganography is a special branch of hidden information where a secret message is embedded in a cover image based on a shared stego key, resulting in a stego image. In contrast to steganography, steganography aims to detect or extract hidden data in these stego images. The steganographic algorithm is considered to be broken if an attacker can decide whether a given image is an image of stego, based on steganalysis with a greater probability of detection rather than just random guessing. Steganography requires a carrier object, secret data and an inclusion algorithm. It also requires an encryption algorithm and a secret key in some cases, increasing the steganography security levels. The applications of steganography include the secure transmission of secret documents between national and international governments, subtitling, tampering, online banking assurance, voting systems and time stamps. Watermarking and cryptography are two areas closely related to steganography. The main theme of steganography and cryptography is the same, that is, to obscure the secret information, but the corresponding techniques used in both areas are different. The procedure of steganography and the watermark are similar, with different purposes. Steganography deals with the inclusion of secret data, while the watermark refers to the protection of copyright Author of the digital data.

Today steganography is of enormous importance due to the increasing use of the Internet and other new technologies. National, corporate, personal information security is a major concern. It is necessary to employ novel methods to confine the access to the data through a channel of communication. Steganography has many applications in the domain of hidden information. In the steganography of the image there are typically two categories: The spatial domain and the second is called the domain of transformation. The spatial domain has methods that tend to work directly in pixels. In the spatial domain incorporation steganography algorithm is based on modification of the least significant bit layer (LSB) of the images. This technique mainly uses the fact that LSBs in an image can be considered as random noise and any alteration to them would not result in any significant or insignificant effect on the image. This phenomenon becomes evident by looking at the image that appears to have remained unchanged visually even after LSB alteration. It is made evident by examining notable modifications in the statistical properties of the image. Statistical changes can be used to detect Stego images. LSB is used for creating Stego images where the LSB of the pixels is replaced by the message to be sent. The message bit permutation is performed prior to embedding, resulting in uniform bit distribution. Popular steganography tools based on LSB differ significantly in the approach of information concealment. In an effort to have a more robust technique, steganography, it is required to have security, satisfactory ability, pivotal detection capability, peculiar robustness and level of visibility against unintentional and malicious attacks. In the spatial domain, many of the steganography methods are presented, but the difficulty lies in providing better viewing quality in the steganography image to maintain sharpness and maintain continuity across regions that are noisy.

II. METHODOLOGY

In this methodology SPIHT algorithm for the image compression technique is used. The SPIHT is the combination of DWT and SPIHT algorithm. Set Hierarchical Tree Partitions (SPIHT) is a wavelet-based image compression method that provides good image quality, fast coding, and high PSNR. It is used for lossless image compression. For higher performance, the high-speed arithmetic encoder architecture is designed. Encryption of the secret message from compressed data is now performed using the RSA algorithm. RSA is one of the first practical public key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and differs from the decryption key that is kept secret. In RSA, this asymmetry is based on the practical difficulty of factorizing the product of two prime numbers The problem of factoring.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

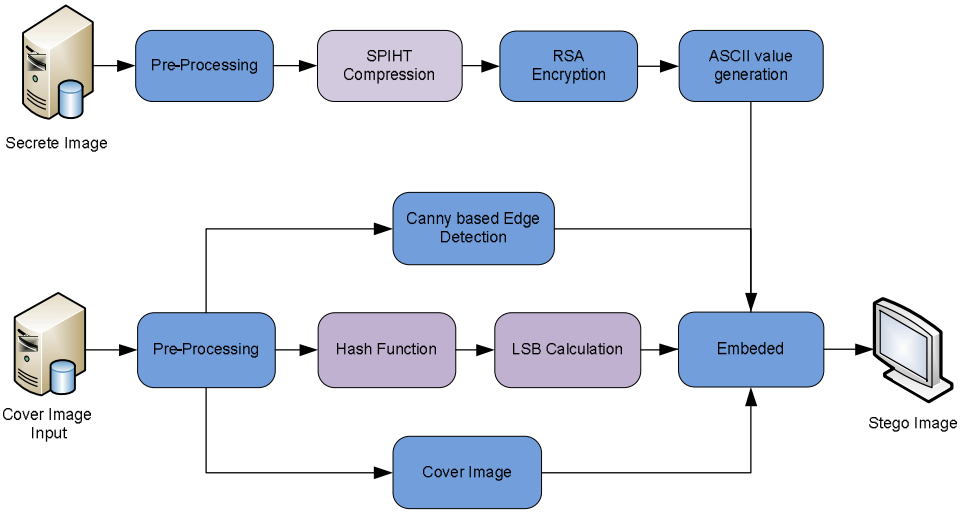

Fig 1: Block Diagram shows the Encryption for Proposed System

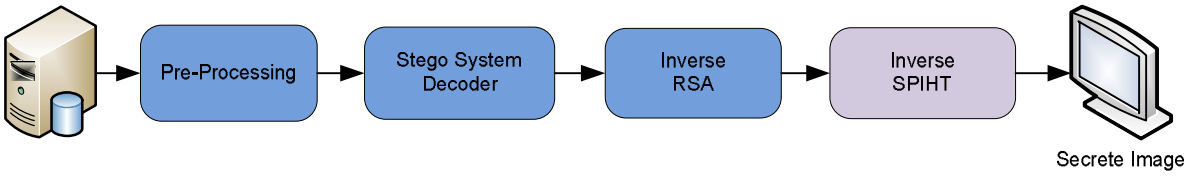

Fig 2: Block Diagram shows the Decryption for Proposed System

Steganography is a technique used to transmit a secret message from a sender to a receiver in such a way that a potential intruder does not suspect the existence of the message. Usually this can be done by embedding the secret message into another digital medium such as text, image Gen, audio or video.

RSA Algorithm:

The RSA algorithm is a cryptosystem of message encryption in which two prime numbers are taken initially and then the product of these values is used to create a public key and a private key, which is also used in encryption and decryption. The RSA algorithm could be used in combination with Hash-LSB so that the original text is embedded in the cover image as ciphertext. By using the RSA algorithm we are increasing security to an earlier level. In the case of steganisis, only ciphertext can be extracted that is in encrypted form and is not legible, so tThen it will be safe.

RSA algorithm procedure can be illustrated in brief as follows:

(i) Select two large strong prime numbers, p and q. Let $n = p\,q$.

(ii) Compute Euler's totient value for n: $f(n) = (p-1)(q-1)$.

(iii) Find a random number e satisfying $1 < e < f(n)$ and relatively prime to f (n) $i.e., gcd\,(e, f\,(n)) = 1$.

(iv) Calculate a number d such that $d = e - 1\, mod\, f\,(n)$.

(v) Encryption: Given a plain text m satisfying $m < n$, then the Cipher text $c = me\, mod\, n$.
Decryption: The cipher text is decrypted by $m = cd\, mod\, n$.

Hash LSB Process:

The least significant bits (H-LSB) technique based on hash for steganography in which the position of LSB to hide the secret data is determined using the hash function. The Hash function finds the least significant bit positions of each RGB pixel and the message bits are embedded in these RGB pixels independently. The hash function then returns hash values in accordance with the least significant bits present in the RGB pixel values. The cover image will be broken

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

down or fragmented into RGB format. The Hash LSB technique will then use the values given by the hash function to embed or hide the data. In this technique, the secret message is converted into binary form as binary bits; Each 8 bits at a time are embedded in less significant bits of RGB pixel values of cover image in the order of 3, 3 and 2 respectively. According to this method, 3 bits are embedded in the red LSB pixel. The following formula is used to detect positions to hide data in LSB of each RGB pixels of the cover image. Following formula is used to detect positions to hide data in LSB of each RGB pixels of the cover image

$$k = p \% n \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (1)$$

Where, k is the position of the LSB bit within the pixel; P represents the position of each hidden pixel and n is the number of bits of LSB which is 4 for the present case. After embedding the data in the cover image, a stego image will be produced. The recipient of this image has to use the hash function again to extract the positions where the data has been stored. The information extracted will be in cipher-text. After decrypting it, the combination of bits in information will produce the secret message required by the receiver.

Embedding Algorithm:

Step 1: Choose the cover image & secret message.
Step 2: Encrypt the message using RSA algorithm.
Step 3: Find 4 least significant bits of each RGB pixels from cover image.
Step 4: Apply a hash function on LSB of cover image to get the position.
Step 5: Embed eight bits of the encrypted message into 4 bits of LSB of RGB pixels of cover image in the order of 3, 3 and 2 respectively using the position obtained from hash function given in equation 1.
Step 6: Send stego image to receiver.

Hash-LSB Decoding and RSA Decryption:

Step 1: Receive a stego image.
Step 2: Find 4 LSB bits of each RGB pixels from stego image.
Step 3: Apply hash function to get the position of LSB's with hidden data.
Step 4: Retrieve the bits using these positions in order of 3, 3, and 2 respectively.
Step 5: Apply RSA algorithm to decrypt the retrieved data. Step 6: Finally read the secret message.

III. RESULTS

Fig 3: Input image

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

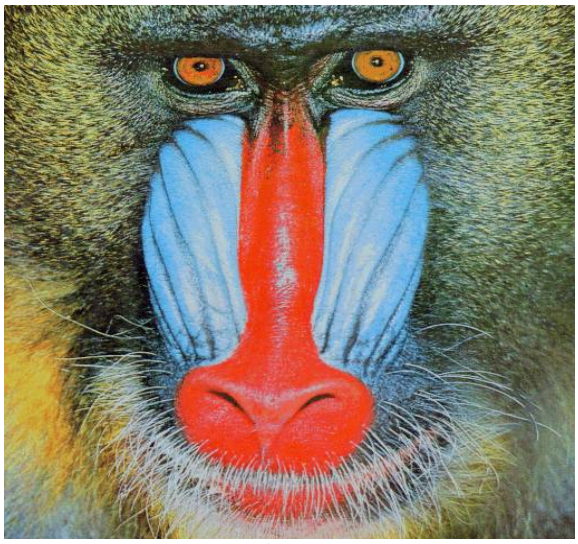

Fig 4: Secret Data

Fig 5: Stego Image

IV. CONCLUSION

The secret data is pre-processesd before masking it behind the cover image. Compression reduces the size of text data and allows more data to be hidden behind the cover image. After data compression several modification are performed in cover image. Due to this if the adversary detects the presence of hidden data behind the cover image and succeeds to get it, he has to apply lots of efforts on it to recover the original message which is not possible as long as exact encryption key is not available. The data is hidden in the edge by finding location using hash function thus a huge amount of compressed data can be stored there with some changes in original and Stego image. It makes the technique more robust and secure.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

REFERENCES

[1] Minati Mishra, Ashanta Ranjan Routray and Sunit Kumar, "High Security Image Steganography with Modified Arnold's Cat Map", International Journal of Computer Applications, Vol. 37, No. 9, 2016.
[2] Sachin Mungmode, R. R. Sedamkar and Niranjan Kulkarni, "An Enhanced Edge Adaptive Steganography Approach using Threshold Value for Region Selection", IEEE, 2016.
[3] Debiprasad Bandyopadhyay, Kousik Dasgupta, J. K. Mandal and Paramartha Dutta, "A Novel Secure Image Steganography Method Based On Chaos Theory In Spatial Domain", Vol. 3, No. 1, IJSPTM, 2014.
[4] HayatAl-Dmour and AhmedAl-Ani, "A Steganography embedding method based on edge identification and XOR coding", ELSEVIER, 2016.
[5] A.J. Umbarkar, Pravin R. Kamble and Aniket V. Thakre, "Comparative Study Of Edge Based LSB Matching Steganography For Colour Images", ICTACT JOURNAL, Vol. 6, No. 3, 2016.
[6] Kumar, Anil, and Rohini Sharma, "A secure image steganography based on rsa algorithm and hash-lsb technique", International Journal of Advanced Research in Computer Science and Software Engineering Vol. 3. Issue 7, 2013.
[7] Chhillar, Rajender Singh, "Data hiding using advanced lsb with rsa algorithm", International Journal of Computer Applications, Vol 122, Issue 4, 2015.
[8] Chitra S and Narasimhalu Thoti, "Implementation of video steganography using hash function in lsb technique", International Journal of Engineering Research and Technology, Vol. 2, Issue 11, 2013.
[9] Vyas Krati and B L Pal, "A proposed method in image steganography to improve image quality with lsb technique", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, Issue 1, pp. 5246-5252, 2014.
[10] Chaudhary Ankit, and Jaldeep Vasavada, "A hash based approach for secure keyless image steganography in lossless RGB images", In Ultra Modern Telecommunications and Control Systems and Workshops, IEEE , pp. 941-944., 2012.