ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization

Vol. 3, Special Issue 3, April 2014

International Conference on Signal Processing, Embedded System and Communication Technologies and their applications for Sustainable and Renewable Energy (ICSECSRE '14)

Organized by

Department of ECE, Aarupadai Veedu Institute of Technology, Vinayaka Missions University,

Paiyanoor-603 104, Tamil Nadu, India

Data Hiding on RBG Images Using Improved Generation Technique

Dany Thomas Koshy, S. Vijayananth

Department of Telecommunication and Networks, SRM University Chennai, India

ABSTRACT- Data hiding on RBG image using generation method, where a secret RBG image is hidden in a generated cover image. Generated cover image is a unique image thereby providing more capacity and security. The generated cover image provides high capacity as the whole image is RBG for hiding data by keeping low visual changes. Using RBG image gives more security which is widely used in military purpose. The algorithm used here is highly resistant against RS, Sample pair, X2 and DCT based attacks.

KEYWORDS-Steganography, RBG Image, Generation technique.

Steganography is the art of hiding information in such a way that the existence of information is known only to a legitimate user. Steganography uses different type of files for hiding the message, such as image, video, audio etc., image format is the most popular one. In image there is lot of space to hide data also it provides high security. A new algorithm is proposed here which has high capacity, low visual changes and security [1].

Steganography is used in digital form with development of processing of digital signals and information theory and coding theory. Different methods are used in digital medias which should have enough strength against Steganalyist. There are different application of Steganography [2]. It can be used to protect rights of copying. The major drawbacks of Steganography is that little space can be used for media selected.

I. INTRODUCTION

C. *Authorisation*

It is to verify authorisation of a content of multimedia authentication. It will verify that transmitted one is same as received one.

D. *Tracking of Broadcast*

To track the assigned number of files broadcasted in a assigned time period.

III. TYPES OF IMAGES USED

II. APPLICATIONS

Steganography can be used in following areas:

A. *Protection of Copying*

The protection of copyrights and ownership of a content of multimedia. This is one of the application where Steganography is widely used.

B. *Conversion of Communication*

For securing transmission of information from sender to receiver.

The light intensities at various points as an array of numbers is referred as digital image. The different forms of images that are used in Steganography are JPEG, BMP and GIF. JPEG is a lossy compression one which saves more space where by losses its originality[3].

Normally there are three colours used in any image red, green, and blue. An image is generally described as amount of pixels. It is very important to select image that are ordinary[1]. In this RBG image is used as the image for Steganography.

RBG images can be thermal images where they are amount of infrared energy emitted, transmitted and reflected by an object visual display and there are only three colours in it they are red, green, blue.

IV. STEGANOGRAPHIC TECHNIQUES

Basicialy there are threetechniques that are used in Steganography and they are:

- *Substitution Technique*: Bits that are least significant are replaced by the bits of the secret image which causing least effect in resolution.
- *Injection Technique*: In this technique, we are utilising the space that are ignored by the processing application. Therefore utilising space makes the technique more efficient.
- *Generation Technique*: This technique generates a cover file for the sole purpose of hiding the secret file[3] instead of using a existing cover file.

The Steganography technique that are used here is of generation technique which need only key image and that of key image where by produces cover image which is used for the purpose of hiding the thermal image.

V. ATTACKS

Attacks on Steganography is like that of destroying the hidden file or modifying it. This can be defined in terms as follows

1. *Message known attack*: The message that is hidden in cover file is known.
2. *Medium known attack*: The Steganography tool and medium are both known.

VI. IMPLEMENTATION

In the generation technique a new image Steganography scheme is introduced. A values of arrays are used to represent images in computer. These values usual represent red, green, blue colours intensities. Each pixel is a combination of three colours[4].

In this technique, thermal image is being hidden by processing with that of the key image which produces a cover image along with that of the embedded thermal image(stego image). The stego image is a unique image which cannot be compared with that of any other image for attacking, which ensures security.

There are two phases in Steganography they are embedding phase and extracting phase.

A. *Embedding phase*

Inputs: Thermal image and the key image

Output: Embedded image which contains thermal image

Procedure:

Step 1: Thermal image is read which is used to hide.

Step 2: Separate the thermal image to three layers red, green, blue.

Step 3: The three planes red, green, blue is converted to binary form using halftone method.

Step 4: Key image is read which is of BMP format.

Step 5: The transformation technique that are used is of XOR operation which is used between each of the three layers with that of the BMP image .

Step 6: The above process which leads to generates a cover image which contains the thermal image.

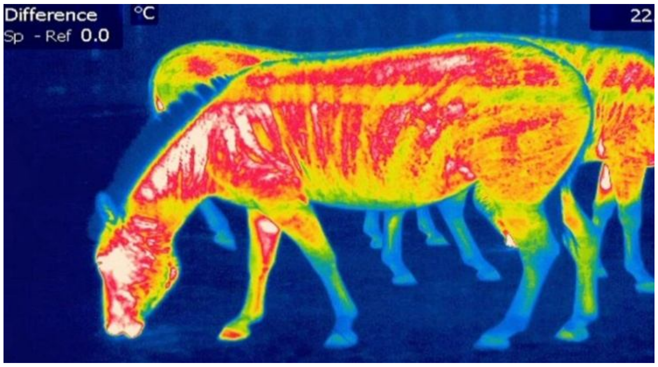

Fig 1. Thermal image to be embedded(Temperature is shown at the top in degree celcius)

Fig 1 shows the thermal image to be hidden, which is read first. Thermal image is then splitted in to red, green, blue layers..

The planes are then converted in to binary using half tone method. In half tone we are comparing with athreshold value and gradually converting to binary without clarity of the image. The key image is used that of BMP format.

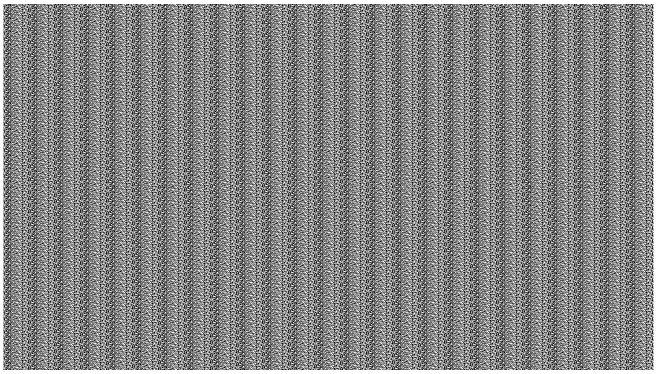

Fig 2. BMP image which is used as key image

The above three layers are processed with the key image thereby generates a cover image which contains the thermal image, which is the stego image. This embedded image is a unique image The embedded image is the stego image which has highly secured and also highly utilised in space of the cover image thereby leads to highly efficient technique. The embedded is the transmitted from the sender through the channel where noise is added which effects the quality of the signal.

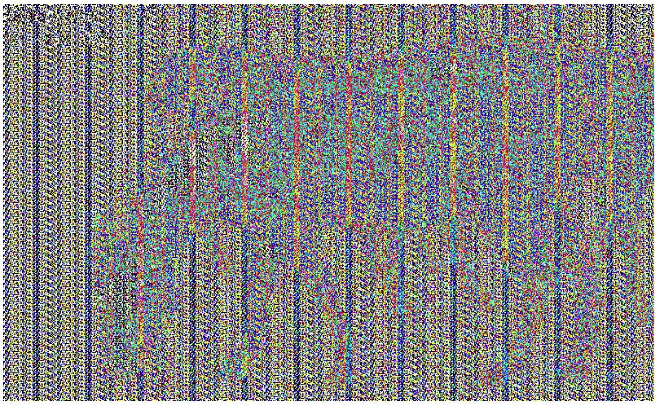

Fig 3. Stego image which contains the thermal image

Fig 3 shows the stego image which has embedded thermal image thereby the embedded image is a unique one, which ensures security as it cannot be compared with any other image and also the capacity is high as the the technique generates cover for only the purpose of data hiding.

B. Extraction phase

Inputs: Embedded image(Stego image)

Output: Secret thermal image file

Procedure:

Step 1: The stego image is given as the input, which is read is the first extraction process.

Step 2: Splitting the embedded image in to different layers red, green, blue.

Step 3:The above separated layers are processed with the key image .

Step 5: The resultant three layers which after processing with key image are combined, which leads to secret thermal image.

In the extraction process, the embedded image that is received at the receiver through channel is separated into different layers red, green, blue are then processed with the key image to get back the hidden thermal image.

The embedded image which is send from the sender is received at the receiver through the channel where it adds the noise at the intial stage of reciver,

The efficiency of a method are identified using the parameters that of the security and the capacity and that of visual changes of the stego image which is all sanctioned in this new method.

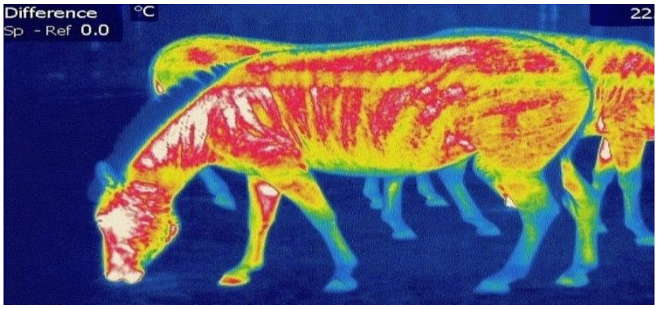

Fig 4. Extracted thermal image(Temperature is shown at the top in degree celcius

The extracted thermal image has less clarity compared to that of the input thermal image, as due to the noise in the channel.

X. CONCLUSIONS

In this, a new technique in Steganography is proposed, which is known as generation technique which has high capacity and security. The generated cover image is a unique one which leads to the property that it cannot be compared with any other image thereby ensuring security which makes this technique dominant over other technique.The embedded image has high capacity compared to other methods as the cover image generated for the sole purpose of hiding secured data. The thermal image which is extracted has improved PSNR value compared to other method. The stego image which is obtained by using the generation technique cannot be identified using steganalysis. The computational complexity is reduced as only few steps are used.

A new approach of Steganography on thermal image using generation technique provides a good balance between image quality and security.

REFERENCES

[1] Amir Farhad Nilizadeh and Ahmad Reza Naghsh Nilchi, "Steganography on RGB Images Based on a "Matrix Pattern" using Random Blocks", Department of Computer Engineering, Arak Branch, Islamic Azad University, Arak, Iran , I.J.Modern Education and Computer Science, 2013, DOI: 10.5815/ijmecs.2013.04.02.

[2] Nagham Hamid , Abid Yahya, R. Badlishah Ahmad, Osamah M. Al-Qershi "Image Steganography Techniques: An Overview", International Journal of Computer Science and Security (IJCSS), Volume (6) : Issue (3) : 2012,p168-187

[3] Vipul Singhal, Dhananjay Yadav, Devesh Kumar Bandil," Steganography and Steganalysis: A Review" International Journal of Electronics and Computer Science Engineering ,pp399-404

[4] Dr. Ekta Walia a, Payal Jainb "An Analysis of LSB & DCT based Steganography ",Global Journal of Computer Science and Technology, 4 Vol. 10 Issue 1 (Ver 1.0), April 2010, p4-8

[5] S. Bhattacharyya, and G. Sanyal, "A Robust Image Steganography using DWT Difference Modulation (DWTDM)", International Journal of Computer Network and Information Security (IJCNIS) 4.7 (2012): 27. DOI: 10.5815/ijcnis.2012.07.04

[6] R. Radhakrishnan, K. Shanmugasundaram, and N. Memon. " Data masking: a secure-covert channel paradigm." in IEEE Workshop on Multimedia Signal Processing, 2002. pp. 339-342.