Indian Journal of Science and Technology, Vol 9(7), DOI: 10.17485/ijst/2016/v9i7/84152, February 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Performance Analysis of a Combined Cryptographic and Steganographic Method over Thermal Images using Barcode Encoder

S. Vijay Ananth[1*] and P. Sudhakar[2]

[1]PRIST University, Thanjavur – 613403, Tamil Nadu, India; vidhuranila@gmail.com
[2]Department of Computer Science and Engineering, Annamalai University, Annamalai Nagar – 608002, Tamil Nadu, India; kar.sudha@gmail.com

Abstract

Objective: Security of hidden data and the quality of the Stego image still is a challenge. This proposed research design implements Barcode encoder based steganography method that uses thermal images as cover image instead of often used colour images. **Methods/Analysis:** The data or text to be hidden is first encoded into equivalent barcode image. After the encoding process, the barcode image which has the original data is watermarked over a thermal image using improved Least Significant Bit (LSB) substitution process and generates distortion less Stego image. In reverse, De-Watermarking extracts and decodes the bar-coded data image from the Stego image to recover the original data. **Findings:** Use of both the barcode encoder for Cryptography and Thermal image for Steganography provides more security for the hidden data. Experimental outcomes of this research provide high performance on data security with improved PSNR and MSE. **Application:** Implementation of Thermal Image steganography can be utilised in Video data hiding with high data rate, thermal image to colour image conversion and temperature monitoring of power transformers.

Keywords: Cryptography, Barcode Encoder, LSB, Steganography, Stego Image, PSNR, MSE

1. Introduction

Cryptography and Steganography are the two major techniques to cipher and hide the information before transmission[1].Cryptography changes a message or information in a way by which that cannot be understood where as the Steganography hides the information by which that cannot be seen. Cryptography encodes message and allows the person who has the key. Conventional image steganography uses RGB and Gray scale images as cover image. Our goal in this proposed research is to test the thermal images in steganography with encryption the data to be embedded and Least Significant Bit Substitution technique[2-3]. Spatial domain data hiding technique involve management of pixel values commenced like Complementary robustness properties[4] of both low frequency and spread spectrum generated watermarks to obtain watermarked image capable of surviving an extremely wide range of severe image distortions. Bhattacharyya in[5] have implemented a region of interest based data hiding in RGB images. Huang in[6] focused on a distortion less image data hiding algorithm using integer wavelet transform without any distortion after data extraction. Tiwari and Shandilya in[7] proposed reversible data hiding technique using a vector quantization compression code to obtain the final cover image without any distortion. Many transforms were proposed like Shearlet Transform, Discrete Cosine Transform, Contourlet Transform, Discrete Wavelet Transform Curvelet Transform, Fast Fourier Transform, Ridgelet Transform, in transform domain data hiding. Cox and Miller in[8] have proved Contourlets transform has significant edge over general techniques. Mehdi Hussain and Mureed Hussain[9] have focused on an adaptive least significant bit substitution method in spatial domain embedding. The strength of that method is its integrity of secret hidden information and high hidden data rate capacity. All

*Author for correspondence

the above mentioned developments were analyzed with the RGB visual images not in thermal images[10]. Our goal in this proposed research is to test the thermal images in steganography with encryption the data to be embedded and Least Significant Bit Substitution technique.

2. Thermal Images Vs Normal Colour Images

Thermal images are captured by a thermo-graphic camera using infrared radiation where as the normal images are captured by using visible light cameras. Visible light camera works in the 450nm to 750nm range[11]. The infrared cameras work in as maximum as 14,000 nm, i.e., 14μm. Thermal images are generally a visual display of the amount of IR energy emitted and reflected by an object. In thermal image unlike the visual image, every parameter is taken with a temperature value greater than zero when it emits heat. The colours in the thermal image describe various temperature levels in the image. The temperature level of a thermal image is shown in Figure 1. The normal visual image and thermal images are shown in Figure 2.

3. Novelty of the Proposed Research

This proposed research design and implements Cryptography based Digital image watermarking over the thermal images instead of RGB images to increase security of watermarked data. In the typical data hiding techniques, the data is generally the text image, where as in this research, it is the image which is encrypted by barcode encoder.

The data to be hidden is first encoded into equivalent barcode image. After the encoding process the barcode image which has the original data is watermarked over a thermal image using Least Significant Bit (LSB) substitution and generates the Stego image. De-Watermarking process extracts the bar-coded data image from the Stego image and decodes the barcode image to recover the original data.

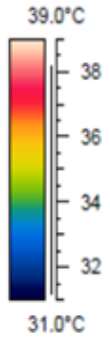

Figure 1. Temperature level of the thermal image.

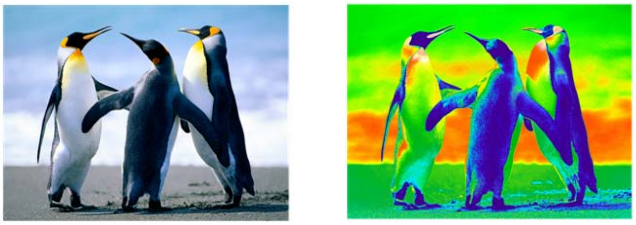

Figure 2. Normal colour and Thermal image of Penguins.

4. Barcode Encoder based Cryptography

Bar-code and image processing techniques are combined to create barcode steganography. Lossless data to be embedded into a cover image is converted as barcode using barcode encoder. While decoding process takes place, the data will not have distortion and it will resemble the original data. Recently barcodes are used effective to secure the shared information in the internet. The output of the text to barcode conversion process using barcode encoder is shown in Table 1.

Table 1. Text to Bar-code conversion process using barcode encoder

Type of message	Original Message	Bar-code Output of the Original Message
Alphabets	"Research"	
Numbers	"50379"	
Special characters	"!@#$%^&"	

5. Least Significant Bit Substitution Process

The least significant bit (LSB) technique embeds information into a cover image in which pixels are changed by bits of the secret information[12-15]. The changes made after cannot be perceived by the human being visibility system. Information can be the numbers, text, image, audio or video.LSB can store 65,536 bits (8,192 bytes) in a 256 × 256 pixel image by inserting or storing 1-bit in each pixel.

6. Selection of Cover Image

It is well known that getting a Stego-image as most similar as to the cover image depends upon the selection of the cover image before watermarking process. The conventional watermarking techniques existed already uses only the 8 bit colour image as the cover image[16].This research paper is deals with a steganographic approach in thermal images for information hiding. Thermal images are used as cover images and images/messages to be hidden are inserted using LSB. So the selection of thermal image rather colour image implies this research to test and analyse a new way of steganography. In 8 bit colour image, there is Red, Green and Blue (RGB) colour components. In which the red component has 3 bits, green component has 3 bits and blue component has 2 bits enabling 8 × 8 × 4 = 256 different colours. Other than 8 bit image, there is 24 bit colour graphic that can be used as the cover image (Thermal Image in this research). This cover image is split into its 3 region as Red (8 bits), green (8 bits), and Blue (8 bits) enabling 8× 8 × 8 = 512 different colours. According to the research of Hecht, it is proved that the human eyes are 65%, 33% and 2% sensitive to Red, Green and Blue respectively[17]. There is a notable point that the visual readings of blue objects are less distinct than red and green which helps us to decide and choose the 24 bit thermal image as the cover image to embed the information using Least Significant Bit (LSB). So, Selection of 24 bit thermal image as cover image provides zero percent or negligible amount of change in the colour intensity of the stego image than 8 bit colour graphic as described in the below example.

Cover=imread('thermalimg.jpg');
disp(Cover(1,1,1)); = 1 = 0x01
disp(Cover(1,1,2)); = 226 = 0xE2
disp(Cover(1,1,3)); = 0 = 0x00

From Figure 3, the first pixel of the message image (bar-coded image)is1, 226 and 0.It is the value of its R, G, and B channel respectively. They are written in binary form as follows,

0000 0001 1110 00100000 0000

As already mentioned the message converted into bar-code. There will be two colours black and white. '255' is white and '0' is black. From Figure 3 the first pixel of the message image (bar-coded image) is 255, 255, and 255. It is the value of its R, G, and B channel respectively. For example, if we consider the pixel of the message image as black (normally the barcode image will have black and white pixels only), then we can get from MATLAB as follows

Msg=imread(msgimg.jpg');
disp(Msg (1,1,1)); = 0 = 0x00
disp(Msg (1,1,2)); =0 = 0x00
disp(Msg (1,1,3)); =0 = 0x00

0000 00000000 00000000 0000

For white pixel, we can get,

Msg=imread(msgimg.jpg');
disp(Msg (20,20,1)); = 255 = 0xFF
disp(Msg (20,20,2)); =255 = 0xFF
disp(Msg (20,20,3)); =255 = 0xFF

1111 1111 1111 1111 1111 1111

For the LSB Substitution, let us assume the white pixel of the barcode image. To get the stego image we replace last two LSB of each RGB channel of cover image with the first two R channel's MSB pixel of barcode image, then next two MSB of first pixel of secret image to G channel and finally the next two MSB of first pixel of B channel. By doing this process we get,

[0000 0011 1110 0000 0011]

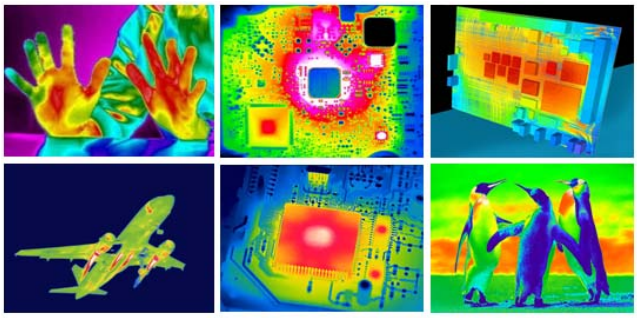

Figure 3. Various Thermal images used in this research as cover image.

In this way we can hide the bits of secret image into the thermal image to get the stego image which is visually impossible to differentiate from the original thermal image. Figure 4 shows the proposed research simulation result which takes 'Secret', 'Success', '12345', '09876' and '*#@%' as the message to be converted into the message image. Images PCB-1, Penguin, Airplane, PCB-2 and PCB-3 are used as the cover image (thermal).Embedding and extracting procedures of LSB with thermal image and bar-coded message image are described below.

7. Embedding Procedure

Thermal image and the Message image from barcode encoder are used here.

Steps:

S1: Input text is read and converted in to barcode image using barcode encoder.
S2: Message image is converted to R, G and B channels.
S3: All three channels are converted to binary format.
S4: Thermal image is read and the R, G and B channels are separated as Message image.
S5: MSB substitution of message image into LSB of thermal image in its RGB channels
S6: The above process is repeated until the generation of Stego image which contains message.

Extraction procedure:

The Stego image is used as the source for the Extraction phase to retrieve the message.

Steps:

S1: Stego image is fed as the input in this phase.
S2: Separation of R, G and B channel from the Stego image.

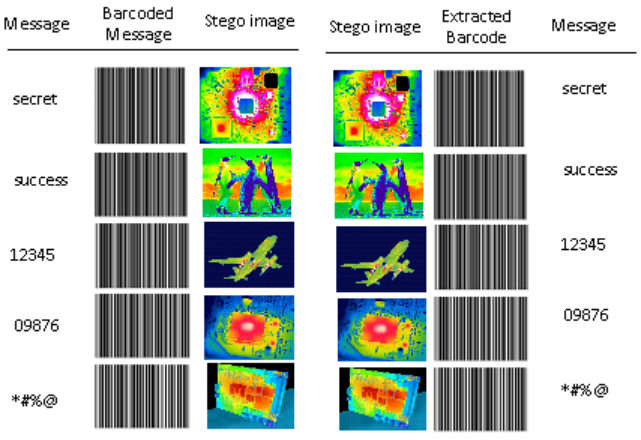

Figure 4. Simulation Results of the proposed research.

S3: All the channels are processed with the key to retrieve the message image.
S4: Output three channels received after the above process are combined
S6: Above process is carried out until the message image is retrieved completely
S7: Barcode decoding process is done at last to retrieve the original message inserted at the transmitter side

8. Peak Signal to Noise Ratio (PSNR) and MSE Calculation

Original message image and the watermarked / stego image should not have visible differences that could be seen by human eye[18]. For the first two LSB substitutions we did not have distortion in the watermarked image. If we increase the bits substitution order we found some visible distortion while we calculated the PSNR. Here the PSNR value is used to check the quality of the watermarked image. PSNR is normally a measurement of the image reconstruction ratio and mostly defined by the Mean Square Error value (MSE). MSE is calculated for the two mxn images. The first image is the original image I and the second image is the watermarked or stego image K.MSE and PSNR are defined as in the following equation (1) and (2). Table 2 shows various PSNR, MSE and RMSE values for the thermal cover image versus stego image created by LSB of bar-coded message and cover image[19].

$$\mathrm{PSNR} = 10 * log10\left(\frac{s^2}{MSE}\right) \quad (1)$$

$$\mathrm{PSNR} = 20 * log10\left(\frac{S}{\sqrt{MSE}}\right)$$

Where S stands for maximum possible pixel value of the image

Table 2. Various PSNR, MSE and RMSE values of Stego vs. Cover image comparison

Cover Image	Message	PSNR	MSE	RMSE
PCB-1	Secret	31.062417	60.07833	7.75102
Penguin	Success	31.709631	53.64573	7.32432
Airplane	12345	30.679364	62.80616	7.92503
PCB-2	09876	30.612447	63.78138	7.98632
PCB-3	*#@%	30.156725	69.79624	8.35441

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

Where I = original image and K = watermarked image

9. Conclusion and Future Work

In this proposed research we have analyzed both Cryptography and Steganography. Here the Cryptography is used to change the information into a format that could not be understandable and Steganography is used to hide information in to an image. In Cryptography side, the data to be hidden is encoded into equivalent barcode image using barcode encoder. At Steganography side, Least Significant Bit (LSB) substitution uses this barcode image to hide over the thermal image to generate the Stego image. Extraction process retrieves the barcoded data image from the Stego image and decodes the barcode image to recover the original data. The experimental result of proposed method does not alter the quality of the Stego image. The proposed method is also tested using PSNR and MSE after the message retrieval and is compared with the conventional method which uses the colour image as the cover image and found better to use.

10. References

1. Zain. Strict authentication watermarking with JPEG compression for medical images. European Journal of Scientific Research. 2010; 42(2):232-41.
2. Coatrieux, Le Guillou, Cauvin, Roux. Reversible watermarking for knowledge digest embedding and reliability control in medical images. IEEE Transactions on Information Technology. 2009; 13(2):158-65.
3. Emam. Hiding a large amount of data with high security using steganography algorithm. Journal of Computer Science. 2007 Apr; 3(4):223-32.
4. Gope, Kumar, Luthra. An Enhanced JPEG Steganography Scheme with Encryption Technique. International Journal of Computer and Electrical Engineering. 2010; 2(5):924-30.
5. Bhattacharyya, Banerjee, Chakraborty, Sanyal. Biometric Steganography Using Variable Length Embedding International Scholarly and Scientific Research & Innovation. 2014; 4(4):24-30.
6. Huang. A novel image steganography method using triway pixel value differencing. Journal of Multimedia. 2008; 3(6):1-7.
7. Tiwari, Shandilya. Secure RGB Image Steganography from Pixel Indicator to Triple Algorithm-An Incremental Growth. International Journal of Security and Its Applications. 2010; 4(4):111-19.
8. Cox, Miller. A review of watermarking and the importance of perceptual modelling. Proc. of Electronic Imaging. 1997 Feb; 4(7):111-18.
9. Hussain, Hussain. A Survey of Image Steganography Techniques. International Journal of Advanced Science and Technology. 2013 May; 5(4):113-24.
10. Osamah, Al-Qershi. Authentication and Data Hiding Using a Hybrid ROI-Based Watermarking Scheme for DICOM Images. 2009; 24(1):114-25.
11. Chetan. Pattern Matching with External Hardware for Steganography Algorithm. International Journal of Information Technology and Knowledge Management. 2009; 2(2):289-95.
12. Acharya, Renuka. Comparison of Secure and High Capacity Colour Image Steganography Techniques in RGB and YCBCR domains. International Journal of Advanced Information Technology. 2013; 3(3):1-9.
13. Jain, Ahirwal. A Novel Image Steganography Method With Adaptive Number of Least Significant Bits Modification Based on Private Stego-Keys. International Journal of Computer Science and Security (IJCSS). 2010 March; 4(3):111-119.
14. Zhao Z. Efficient construction of provably secure steganography under ordinary covert channels. Science China Information Sciences. 2012; 7(2):39-49.
15. Kumar Nawlesh, Kalpana. Novel Reversible Steganography Method using Dynamic Key Generation for Medical Images. Indian Journal of Science and Technology. 2015 July; 8(16):61-74.
16. Ramalingam Mritha. A Steganography Approach over Video Images to Improve Security. Indian Journal of Science and Technology. 2015 January; 8(1):79-86.
17. Bilal Ifra, Kumar Rajiv. Audio Steganography using QR Decomposition and Fast Fourier Transform. Indian Journal of Science and Technology. 2015 December; 8(34):696-04.
18. Valarmathi, Nawaz Kadhar. Secure Data Transfer through Audio Signal with LSA. Indian Journal of Science and Technology. 2015 January; 8(1):17-22.
19. Kumar Nawlesh, Kalpana. A Novel Reversible Steganography Method using Dynamic Key Generation for Medical Images. Indian Journal of Science and Technology. 2015 July; 8(16):617-25.