# Data Hiding in Thermal Image using Levenberg Marquardt Technique

S. Vijay Ananth, P. Sudhakar, K. Sundari, Nibi Maouriyan, R. Raghavi, S. Arivuselvan

***Abstract---*** ***In the ocean of technology, nothing stays secret for a long duration of time. Valuables always been hacked or stolen for it is increasing its value on its own and remains getting ones attraction at the peak. This creates an intention of knowing more about the hidden secrets with in it. Therefore, the security system plays a vital role in hiding the information from hackers or the unauthorised individuals or groups. Cryptography, deals with text of any language while Steganography, deals with the images. In this analysis the input secret data is transformed to a graphical and numerical representation, and embedded into a cover image and further fused with a thermal image before transmission. There ensuring a two level security by summing up the Cryptography and Steganography algorithms under one roof, and provides the best results on implementation.***

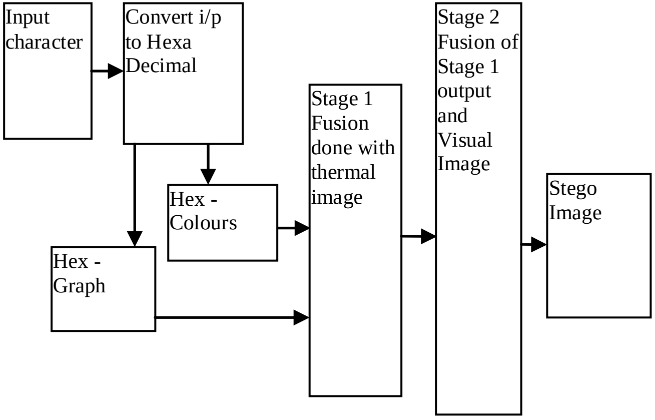
## I. INTRODUCTION

Steganography provides domain for much exploration. It is widespread in the field of digital secured communication in which image steganography has caught an immediate attention. There are cover image, steganographic algorithm and stego image in this technique. Different techniques have to be used for colour image steganography and grey scale image Steganography, since they are stored as 24 bit depth for colour image and 8 bit depth for grey scale image respectively [5]. The first image fusion research is simple image fusion, performing the basic pixel by pixel related operations such as addition, subtraction, averaging and division [3].

The pixel value of an image is valued as 24-bitmap, of three bytes, representing the colours of Red, Green and Blue respectively. The maximum RGB value of a pixel shows that it has larger intensity [4]. It utilises a secretive key or steganographic key to control the embedding and extraction process. To remove the security of steganographic algorithms from the appearance of the hidden message, we use pseudo random bit-strings to generate these messages LSB embedding explains that changing the values in the Least Significant Bit(LSB) of the primary colours, produce only an unnoticeable changes in the colour intensity by the human eye [10]. On the other hand, even one bit changes in the Most Significant Bit, will produce a huge change in the intensity of the colours, which in turn gives clue about the existence of the secret information to the intruder.

## II. BASIC BLOCK DIAGRAM

The basic block diagram of the proposed idea is given below in Figure.


Input character
Convert i/p to Hexa Decimal
Hex - Colours
Hex - Graph
Stage 1 Fusion done with thermal image
Stage 2 Fusion of Stage 1 output and Visual Image
Stego Image

The basic idea is to carry secret information between the source and the desired destination, neglecting the unauthorized interveners trying to hack the information. Moreover, a technique is followed in which, no clue of existence of any information is identified. In the way, the input secret information is undergone with several stages of manipulation to add robustness to the secret data being carried. Hence, the input data is converted to hexa-decimal numbers, and they are classified into two parts. One, the hexa-decimal numbers are plotted as as graph, using Levenberg Marguardt technique and stored as an image. Two, the hexa-decimal numbers are transformed and tabulated as colours. Both the results we fused in the stage 1, where they are fused with the thermal image using LSB.

The LSB technique embeds information into a cover image in which pixels changes its values with the bits of the secret information[3,5-9]. The Most Significant Bits of the R,G & B of the embedded image is fused with LSB of the Thermal Image. The resultant is further fused with the visual or coloured image to hide the existence of the thermal image, thereby increasing the robustness in the stage 2 and produces the Stego Image that can be transmitted or sent towards the destination.

## III. HEXA-DECIMAL TO GRAPH

Trigonometric analysis on numbers is a very old technique of maths, that literally analyse about the triangle measurement [1].

**Manuscript received June 10, 2019.**

**S. Vijay Ananth*,** Research Scholar, PRIST University, Thanjavur, Tamil Nadu, India. (e-mail: vidhuranila@gmail.com)

**P. Sudhakar,** Department of Computer Science and Engineering, Annamalai University, Annamalai Nagar, Tamil Nadu, India. (e-mail: kar.sudha@gmail.com)

**K. Sundari,** Department of Electronics and Communication Engineering, SRMIST, Kattangulathur., Tamil Nadu, India.

**Nibi Maouriyan,** Department of Computer Science Engineering, Valliammai Engineering College. Kanchipuram, Tamil Nadu, India. (e-mail: nibirule@gmail.com)

**R. Raghavi,** Department of Electronics and Communication Engineering, SRMIST, Kattangulathur, Chennai, Tamil Nadu, India.

**S. Arivuselvan,** Department of Computer Science Engineering, Annamalai University, Annamalai Nagar, Tamil Nadu, India. (e-mail: arivucseau@gmail.com)

The text or image or audio on any platform can be named with a valid number that goes on the way called trigonometry. Similar to Steganography trigonometry is also a wide area. Aiming to ensure a high secured system, on thermal imaging Steganography using trigonometric view is a movel methodology. An example to enhance the implementation for the proposed idea is given below. The alphabets are assigned with a random values and plotted in X-axis.

P,R,I,S,T = 1,2,3,4,5 respectively.

Note: when a character is repeated twice in the phrase, those cases a median value shall be taken. Following to the step, the ASCII or values of the above given alphabets is taken. Say,

P = 80 ; R = 82 ; I = 73 ; S = 83 ; T = 84 ;

The estimated numbers are plotted in Y axis. The intersection of both the x and y axis is when plotted, a graphical structure is viewed and the stored as an image, as picturised in the Figure 1. A transformation technique that can covert the resultant to an image is applied, in order to achieve the goal.

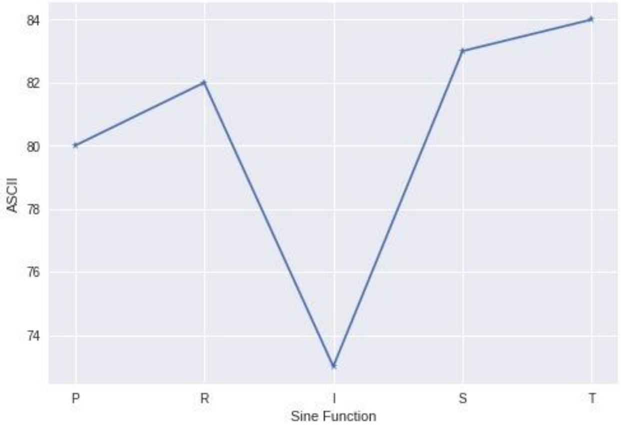


**Figure 1: Graphical Representation**

## IV. LEVENBERG MARQUARDT (LM) TECHNIQUE

The Levenberg-Marquardt (LM) algorithm is an iterative technique that locates the minimum of a multivariate function that is expressed as the function of sum of squares of non-linear real value [5].

The given data is analysed using LM algorithm. The graphical representation is basically achieved by several iteration, taking care of repetitive characters [4]. During each iterations a chi-square is calculated by reducing its value in order to adjust the parameter value.

Sine func = Y = $Y_0$ + A.sin [ pi. ( X-$X_c$)/w],

Where,

A = amp (-0.130 ± 0.304)

W = period(1751 ± 0.103)

$X_c$ = phase shift (9.387 ± 1.775)

$Y_0$ = offset (77.948 ± 1.303)

The LV technique is mathematically given as,

LM = [ (measured data – calculated data)/ weight]; Where, weight = 1.

The chi-square minimizer is,

∑[ weight (measured data – calculated data)] ;Where, weight = 1.

The filled data ranges from 75 to 84, from the example data taken and the value range between the limits is 12. Later, assume the prime number in the place of 1,2,3,4 & 5, as 1,3,5,7 & 9.

Calculations,

$$S = \sum_{I=0}^{5} Primenumber - (TotalRange - 1)$$

Plot the range S in Y axis, against estimated value of Y, in X axis.

LM is the combination of steepest decent method and gauss- Newton method based on the solution being far or closer to the correct one. However generates the convergence of data.

## V. HEXA-DECIMAL TO COLORS

The data manipulated is graphically plotted, while these values and variables are expressed in terms of colours. The hexadecimal values and its corresponding colour values are given below in the Table.1. while0's in all the bit locations represents black, the presence of 1's in all the bits represents the white colour. The variances in between at any bit locations represent some grey value, different colours.

**Table 1: Table of Colours for Hexa-decimal**

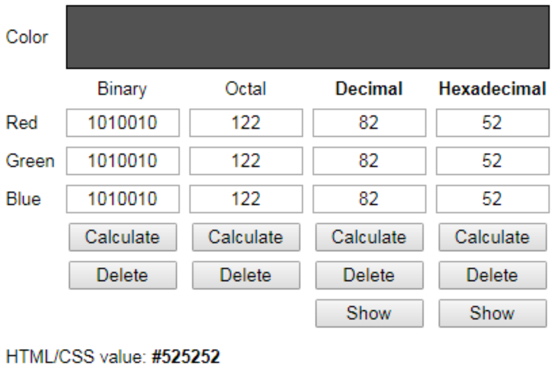
| S.No | Hexadecimal | Decimal | Color |
|---|---|---|---|
| 01. | 000000 | 0,0,0 | BLACK |
| 02. | 0000FF | 0,0,255 | BLUE |
| 03. | FFFF00 | 255,255,0 | YELLOW |
| 04. | FF0000 | 255,0,0 | RED |
| 05. | FFFFFF | 255,255,255 | WHITE |

Similarly, the decimal value of the sample data taken shall be converted to its hexadecimal value, correspondingly the grey value of those hexadecimal values is calculated and estimated. The conversion of the sample data and its estimated colour value is given below in table.2.

**Table 2: Colour Value of Hexa-Decimal**

| S.No | Decimal | Hexadecimal | Colour |
|---|---|---|---|
| 01. | 80 (P) | 50 | 01010000 |
| 02. | 82 (R) | 52 | 01010010 |
| 03. | 73 (I) | 49 | 01001001 |
| 04. | 83 (S) | 53 | 01010011 |
| 05. | 84 (T) | 54 | 01010100 |

From the above table, a sample value is taken. Say R, the decimal value, its Hexadecimal value and the colour representing the character is shown below.



| Color | | | | |
|---|---|---|---|---|
| | Binary | Octal | Decimal | Hexadecimal |
| Red | 1010010 | 122 | 82 | 52 |
| Green | 1010010 | 122 | 82 | 52 |
| Blue | 1010010 | 122 | 82 | 52 |

HTML/CSS value: **#525252**

**Figure 2: Colour of Numbers**

The colour of the decimal number 82 is given to R,G and B is shown above in Figure 2. This could be calculated with higher complexity by assigning any one colour with the decimal value., say either R or G or B. But, the concentration of the colour becomes high and thereby the intensity of the colour will increase more which may attract the interpreter, and may give a hint of the existence of some information in it. Hence, this article possess the method of combining all the three colours with same value, thereby the concentration of all the colours is equally distributed and transformed into a grey value. This colour transformed from the numbers converted are fused with the thermal image, [Figure 3.] only at the 5 locations where the nodes meet up the thermal image exactly after fusion, and pattern locked using a password, since the stego key in embedding process provides better security [6]

## VI. FUSION OF THERMAL IMAGE AND EMBEDDED IMAGE

The main difference between the colour image and the thermal image is, the thermal image holds three colours at the max, they are R,G and B, Figure 4. Whereas the visual image or the colour image is the collection of combinations of R, G and B as in Figure 3. The colours extracted from the ASCII numbers were converted to its corresponding binary values as given in the Figure 2. These values are substituted in the Least Significant Bit of the thermal or the Cover Image. Any changes in the MSB is easily traceable while changes in the LSB is not visible as in MSB [7]. The working principle of the LSB technique shall be narrated in reference [2], which explains the fusion process of the thermal image with the information image. The resultant image Figure 6, will be a thermal image, holding the invisible information signal, i.e, the graphical representation and the colour of the values extracted from different characters.

## VII. FUSION OF THERMAL IMAGE AND VISUAL IMAGE & RESULTS

This resultant image is further fused with a visual image [Figure 3] using spatial domain data fusion technique. Basically, the spatial domain's main advantage of this technique is, its simplicity for real-time processing. The visual image taken here is a Tamil proverb written by thiruvalluvar, which has been secured by providing a password locking system. To unlock the file, the transmitting and receiving end share the stego key and random key [7], and in this paper, the desired users shall use the first letter of the last word of each Thirukkural. Basically, the main advantage of spatial domain technique is its simplicity for real-time processing. Also, the simple addition process will reduce the signal to noise[3] of the resultant image, and provides an improved method to compute each pixel with more focus.

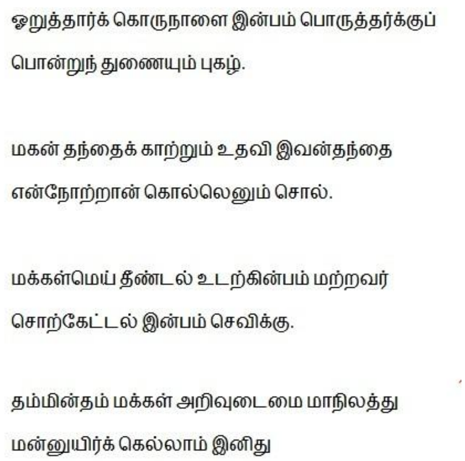
The combination or fusion of the thermal image and a visual image can be done by using the simple equation

$$F(x,y) = FwT(x,y) + (Fw-1)V(x,y)$$

Fused image = weight of fusion(values range from 0 to 1) of thermal image + weight of Fusion(values range from 0 to 1) of visual image.

The resultant of this process will produce a visual image, hiding the thermal image holding the secret information.

[Figure.3] +[Figure.4]+ [Figure.5] = [Figure.6] or [Figure.7]


ஓறுத்தார்க் கொருநாளை இன்பம் பொருத்தர்க்குப்
பொன்றுந் துணையும் புகழ்.

மகன் தந்தைக் காற்றும் உதவி இவன்தந்தை
என்நோற்றான் கொல்லெனும் சொல்.

மக்கள்மெய் தீண்டல் உடற்கின்பம் மற்றவர்
சொற்கேட்டல் இன்பம் செவிக்கு.

தம்மின்தம் மக்கள் அறிவுடைமை மாநிலத்து
மன்னுயிர்க் கெல்லாம் இனிது

**Figure 3: Visual Image**

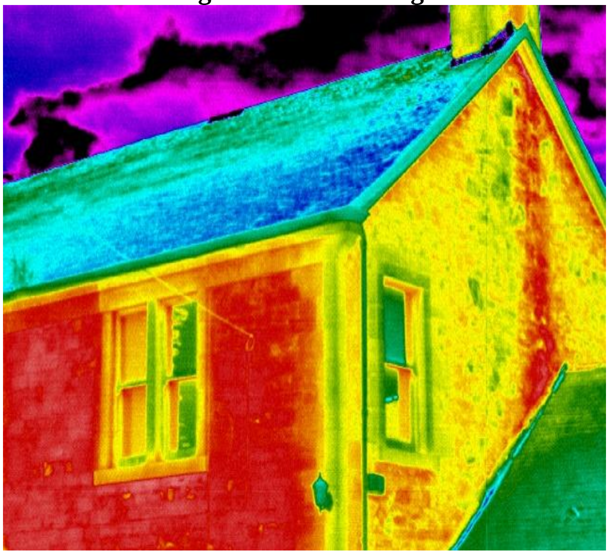
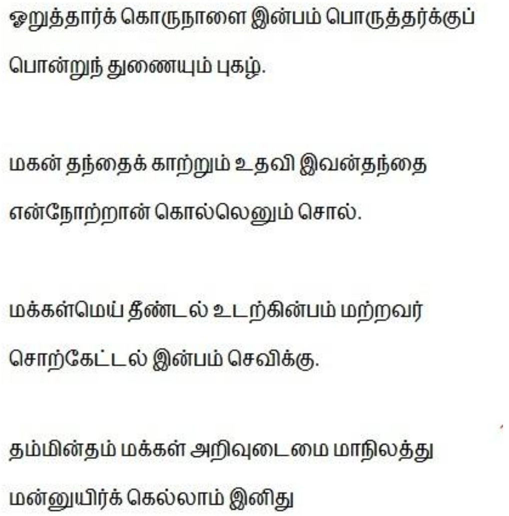


**Figure 4: Thermal Image**


ஓறுத்தார்க் கொருநாளை இன்பம் பொருத்தர்க்குப்
பொன்றுந் துணையும் புகழ்.

மகன் தந்தைக் காற்றும் உதவி இவன்தந்தை
என்நோற்றான் கொல்லெனும் சொல்.

மக்கள்மெய் தீண்டல் உடற்கின்பம் மற்றவர்
சொற்கேட்டல் இன்பம் செவிக்கு.

தம்மின்தம் மக்கள் அறிவுடைமை மாநிலத்து
மன்னுயிர்க் கெல்லாம் இனிது

**Figure 5: Visual image**

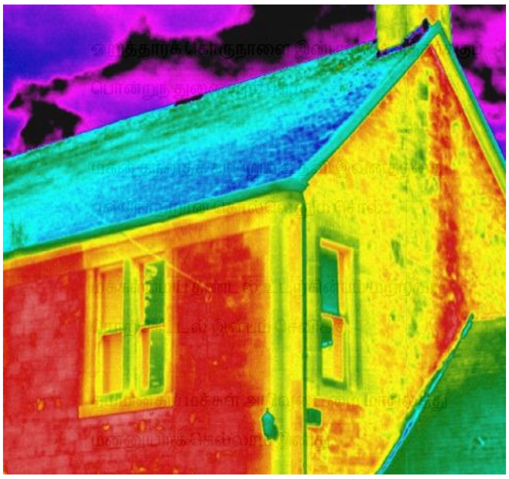


**Figure 6: Stego Image 1**

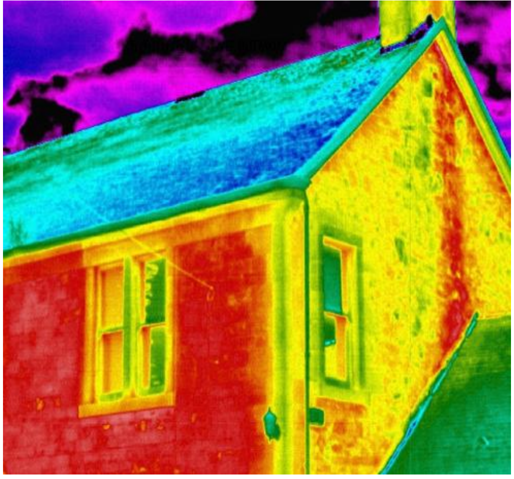


**Figure 7: Stego Image 2**

It can be seen in[Figure.6] that the visual image is slightly seen. This has been corrected by Alpha bending, a process where, overlaying a foreground image (Thermal image) with transparency over a background image (Thirukkural Image). The math behind alpha blending is straight forward. At every pixel of the image, we need to combine the foreground image colour (F) and the background image colour (B) using the alpha mask(α). Note: The value of used is actually the pixel value in the alpha mask divided by 255.

$$g(x) = (1 - \alpha)f_0(x) + \alpha f_1(x)$$

For realistic blending, the alpha value lies between 0 to 1, so we have taken the alpha value as 0.98 so as to completely hide the Thirukkural background image while retaining its value in the blended image. Fully hidden stego image can be seen in Figure.7.

## VIII. CONCLUSION

The proposed model of Steganography on thermal image and locking using cryptography technique has been implemented and verified the resultant's standard and manipulated to find the accuracy for the non existence of the information hidden to guarantee the standard of security, and improvised by adding layers of algorithms and techniques. This paper is elaborated the practical implementations and its applications that could be used in the domain where surveillance is highly in demand. Furthermore the model can be standardised by applying the high level encryption algorithms and also can be analysed using various Steganography transformation techniques.

## REFERENCES

1. RengarajanAmritharajan, S.Deepak Roy, Noel Nesakumar, M.Chandrasekar, R.Sridevi,J.B.B.Rayappan, “Mind game for cover steganography: A Refuge”, Research Journal of Information Technology 5(2),137-148,2013.
2. S. Vijay Ananth and P. Sudhakar, “ Performance Analysis of a Combined Cryptographic and Steganographic Method over Thermal Images using Barcode Encoder” in Indian Journal of Science and Technology, Vol 9(7), DOI: 10.17485/ijst/2016/v9i7/84152, February 2016.
3. R.JohnsonSuthakar, J.Monica Esther M.E, D.Annapoorani, F.Richard Singh Samuel, “Study of Image Fusion- Techniques, Method and Applications” in IJCSMC, Vol. 3, Issue. 11, November 2014, pg.469 – 476.
4. K. Levenberg. “A Method for the Solution of Certain Non-linear Problems in Least Squares”, Quarterly of Applied Mathematics, 2(2):164–168, Jul. 1944.
5. S. Hemalatha, U. Dinesh 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.
6. 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.
7. Yan Zhu, MengYang Yu, HongXin Hu, Gail-Joon Ahn, HongJia Zhao, “Efficient construction of provably secure steg¬anography under ordinary covert channels”, Science China Information Sciences. 2012; 7(2):39-49.
8. 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.
9. RamalingamMritha, “A Steganography Approach over Video Images to Improve Security” , Indian Journal of Science and Technology, Volume 8, Issue 1, January 2015.
10. Natarajan Meghanathan, Lopamudra Nayak, “Steganalysis algorithms for detecting the hidden information in image, audio and video cover media”, Jackson State University, 1400 Lynch St, Jackson, MS, USA.

*Published By:*
*Blue Eyes Intelligence Engineering*
*& Sciences Publication*