

Enhanced security in Image Steganography using Raspberry pi

Sowmiya.R^a, Umamakeswari.A^{b*}

^aM.Tech - Embedded Systems, ^bDean, School of Computing,
SASTRA Deemed University, Thanjavur 613401, India

Article Info

Volume 82

Page Number: 4077- 4083

Publication Issue:

January-February 2020

Article History

Article Received: 18 May 2019

Revised: 14 July 2019

Accepted: 22 December 2019

Publication: 21 January 2020

Abstract:

Information security scores more since, the growth of digital world is ever-looming. An efficient scheme is proposed to increase the Image appearance and Image data Security concurrently using Raspberry pi. The final cipher image is obtained by merging RGB pixels followed by Zigzag scanning which is more secure than the ancient. This enhances the visual appearances of the cipher image and it is same as the size of plain image so, it doesn't require any further transmission bandwidth and repository space. Yet, Hardware Implementation is more in demand to achieve its constants than analytical calculations; this algorithm is realized and tested strongly for efficient encryption standards using a leading Raspberry Pi3 domain. The results obtained highlight the reliable traits of the proposed framework. It is advisable for real-time secure circumstances. Compared to traditional algorithms, the proposed algorithm has an excellent encryption and decryption performance that increases the efficiency of image security.

Keyword: Image appearance security; Secured Image encryption; Zigzag scanning

I. INTRODUCTION

In contemporary world, the requirement of secure communication is in a high raise. Image application has reached its heights in recent years. With the immense technological raise, deportation of the confidential information securely and hindering it from eavesdropper's attention (i.e., from unintended users) must be given utmost importance. In everyday life, Security plays a vital role. This project dispatches with one of the main security issues like that of strengthening the cipher image from getting hacked by the eavesdropper. When encryption is deployed by using many traditional cryptographic standards, it exhibits a low security level and also reclines to various security attacks. To overcome this drawback, specialized cryptographic algorithms are employed [20,21]. One such method is RGB pixels merged followed by zigzag scanning algorithm. Zigzag scanning has its influence majorly in lowering the time complexity, giving good scrambling effect, better anti-interference performance which increases the security level of the algorithm and so on [1]. These advantages evaluate the reliable features of this

algorithm in encrypting image. It is also termed as confidential information hiding technology.

By examining the efficient outlook of Zigzag confusion algorithm in encrypting image, hardware implementation of Zigzag scanning algorithm with increase in security level using Raspberry Pi3 is set up straightforwardly. Raspberry Pi is deployed to analyze more regarding IoT and WoT applications [2]. Raspberry Pi3 Model B is a single-board computer with Bluetooth and wireless LAN connectivity. Here, it is used to implement the proposed algorithm. This model of Raspberry Pi makes use of BCM 2837 chip, which is nothing but the Quad core Cortex A53 – 64 bit processor. This hardware is commonly used for encrypting image. Raspberry Pi involves Raspbian OS. Further, it is a Linux variant and it uses Python as programming language. This proposed work specifically makes use of Open CV-Python which is the Python API of Open CV. It is more advantageous in handling images using python commands. It combines the best qualities of Open CV C++ API and Python language. The proposed work also uses packages such as CLICK (Command Line Interface Creation Kit) and Pillow. The main advantages of this package CLICK is

nesting of commands, automatic help page generation and subcommands are not required.

Therefore, this paper deals with the hardware implementation of encrypting and decrypting RGB images using Zigzag scanning technique using Raspberry Pi framework. It is found that, this algorithm holds good for Real time medical image with reduced CPU clock time. The main objective of proposed work is to enhance the efficiency of the algorithm and to produce a clear visual appearance of the final cipher image which reduces the hacker's attention. The description of the proposed framework is analyzed well and conferred below.

II. RELATED WORK

In today's scenario, Normally Encrypting image plays a necessary tool in providing security. The texture-like or noise-like feature is a perceptible trace that indicates the residence of an encrypted image containing information is more confidential, which captivates the people's attentions and thus leading to a large number of attacks and modification. It further, reduces the image quality. Rather, a new Image encryption scheme described by Long Bao and Yicong Zhou [3] generates the visually secured image which doesn't produce any noise-like encrypted images. This secured image is obtained from the original image that reduces the encrypted image being hacked or attacked. Original image contents are protected by pre-encrypting with diffusion and confusion properties, and a DWT based transformation is employed to produce a visually meaningful encrypted images (VMEI). Since VMEI is very much alike to a normal image, but although attackers are facing extreme crisis in differentiating VMEIs from a normal image due to the visual feature. Similarly, many standard cryptographic techniques are developed to overcome these issues. They are called as Chaos transformation methods and some are known as non-chaos transformation methods that are employed for encrypting images [4-8].

In [9], Robby Candra et al. describes the framework for efficient Zigzag scan. The main objective is to reduce the processing time. IC-FPGA resources used for Zigzag scan with mapping are found to be more efficient. It accelerates the sorting process of DCT

coefficients which is quantized. Since the commencing location for the repetition of zigzag confusion plays a crucial role to increase its efficiency. The processing time is approximately found to be 4 ns per byte data (~ 12 ns per pixel) with the latency (~ 64 clocks). Mario Mastriani, an independent scholar describes in [10] about 3D zigzag for multi-slicing, multi-band and video processing. Compared to traditional 2D zigzag scanning algorithm, an unprecedented 3D technology in Zigzag scanning exhibiting the virtual nature is deployed. The consequent benefits are the transmission of video upon internet and through any mobile medium with any resolution and frames per second rate is possible.

Jian-Jiun Ding et al. [11] describes about Context-Based Adaptive Zigzag Scanning for Image Coding. The results obtained shows that the coding efficiency of proposed method is prominent than the traditional Zigzag scanning algorithm. This algorithm can be combined with other block-based image and video coding systems to upgrade the efficiency in coding. Various Zigzag algorithms are developed and deployed. Each technique labelled is dominant in various aspects. Commonly used is Zigzag Saw tooth Wave (ZZSW) and Zigzag Raster Diagonal (ZZRD) is conferred with their merits and demerits in [12].

In [13], Zhuosheng Lin et al. refined a standardized algorithm in designing and implementing secure video communication system using an advanced RISC (Reduced Instruction Set Computing) machine embedded Cortex-A9 processor operating on Linux (ARM-EMBEDDED Hardware). This technique comes under Chaos transformation. It involves encrypting the tricolor (R, G, B) pixel values with an 8-dimensional matrix. The main objective is to exhibit simultaneous scrambling and encryption. It suits for real time scenario.

III. PROPOSED SYSTEM

In the proposed technique, initially, two color images are seized. One is taken as cover image and other is considered as hidden image (i.e., Size of the Hidden image < Size of the Cover image). The two color images are divided into dominant tricolor (Red, Green, and Blue) planes. RGB pixel rate values are calculated

for each pixel. Then, RGB pixels of the two Images are merged (RGB pixel values ranges from 0 to 255). Finally, the obtained integer values by merging the RGB pixel values (Integer) are converted into binary (0's & 1's). Then, the binary representation of the RGB pixels is produced. Further, these pixels are done with Zigzag scanning which is more secure than traditional cryptographic algorithms. RGB pixels are processed using one byte array (contains 8 bits). For instance, if the pixel values can be represented only in 4 bits, then four zeroes are added additionally and finally an 8 bit

array is formed. Therefore, encryption of image is done completely. Decryption is done by inverse Zigzag scanning followed by unmerging the RGB pixels of the images. ARM chip embedded Raspberry Pi hardware; this designed work is implemented in a Raspbian OS [14] over python programming. Performance metrics are determined. The main objective of this technique is to provide high level security and to reduce the time complexity of the algorithm. Reconstruction of original image is simple. The proposed framework is sketched in Fig.1.

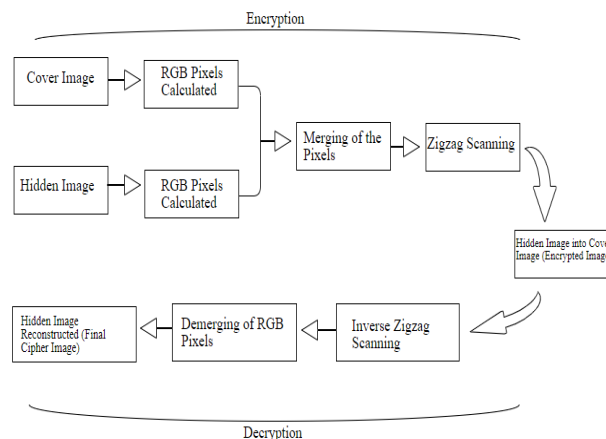


Fig. 1. Architecture of the proposed algorithm

A. Zigzag scanning

Zigzag confusion, which is employed in existing work, is also known as a key masking technique that comes in steganography as sketched in Fig. 2 further. Its main objective is to provide low time complexity, high level security, good scrambling effect, and better anti-interference performance. Some of the Zigzag confusion transformations are conferred in [15-16].

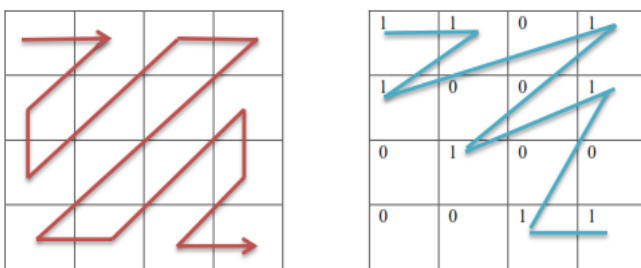


Fig. 2. (a) Conventional Zigzag Path; (b) Proposed Zigzag Path

The zigzag scanning algorithm employed in this implementation is done by checking whether the pixel map position is valid or not. Further, by representing the integer tuple into binary bits,

Case 1: If the bit is 0

Leave the black pixel (0) as default.

Case 2: If the bit is 1

Follow zigzag path only in the place where 1 resides in the binary representation as in Figure 3.

Zigzag merge and encrypt the pixels. Finally, convert it into an integer tuple.

B. Importance of RGB pixel rate value calculation

Red, Green and Blue intensity denotes the color's RGB value. Image intensity value is the mean pixel intensity. It is the amount of gray intensity to be maintained for the particular portion of the image. It ranges from 0 (Black) to 255 (White). This range indicates a single byte (8 bits). In this proposed method, RGB values are calculated for the source image and for the image to be hidden. Then, it follows Image blending. It can be collage overlapping, disproportional merging, and gradient blending. Further, it is briefly discussed in

<http://courses.cs.vt.edu/~masc1044/L20-BlendingChroakey/Blending.html> by N. Dwight Barnette.

The performance metrics calculated and analysed in this framework are CPU clock time, efficiency of the algorithm (execution speed) etc. But, for the hardware implementation, Raspberry pi doesn't contain any hardware clock on board. So, it uses either Internet Access Network Time Protocol (NTP) or from the Personal Computer in which CPU time is measured in clock ticks or seconds.

Normally, calculating pixel values for an image appears to be dominant in image processing. In similar case, S. Jeyalakshmi et al. [17] explained about aligning apparent regions of grayscale images using pixel rate values. Intervening shades of gray are portrayed using three mandatory color's (RGB) or three essential pigments (CMY). Further, it details about Regionprops for measuring the objects property in a grayscale image using pixel values. The problem lies in the result obtained which is not exact. So, the whole color source image is converted into matching texture information instead selecting RGB color's from a group to an individual. This method is further enhanced by letting the user to pair the areas of two images with elongated and rounded patterns.

S. Balamohan et al. reviewed about Melanoma Detection Using RGB Color Model in Medical Imaging [18]. The proposed work is all about the precise segmentation depending on the RGB color model for determining the melanoma in a medical dermoscopy images. This paper has an analogy of two different techniques. The result obtained is compared to validate the reality of the algorithm in a medical field.

C. The proposed encryption scheme

STEP 1: Two color images are taken; one is taken as hidden image and the other is cover image. (Size of hidden image < Size of cover image) and they are divided into tricolor planes.

STEP 2: RGB pixel rate values are calculated for the images separately.

STEP 3: Merge two RGB tuples. Then an integer tuple with the two RGB values merged are obtained.

STEP 3: Two images are merged.

3.1: Check the Dimensions of the images.

3.2: Get the pixel map of the two images.

STEP 4: Zigzag merge and create a new image which will be obtained as an output.

4.1: Use a black pixel as default.

4.2: Zigzag merge and check if the pixel map position is valid or not.

4.3: Encrypt the pixels and convert it into an integer tuple

D. The proposed decryption scheme

STEP 1: To unmerge the images, load the pixel map.

STEP 2: Create the new image and load the pixel map. Tuples are used to store the image original size.

2.1: Get the RGB (as a string tuple) from the current pixel.

2.2: Extract the last 4 bits (corresponding to the hidden image)

2.3: Concatenate 4 zero bits since, 8 bits are used for processing commonly. Convert it to an integer tuple. Finally, crop the image based on the valid pixels.

IV. EXPERIMENTAL SETUP AND RESULTS

The framed image encryption and decryption technique is implemented by using Raspberry Pi. This Experimental scheme runs in a Raspbian OS. It is done with python programming using Raspberry Pi 3 embedded hardware. This hardware also contains serially connected monitor, USB-connected mouse and USB connected keyboard. Raspbian OS image to be processed is downloaded to an SD card and encapsulated into Raspberry Pi board. The entire preliminary structure and the coding background are pictured below in Figure 3a and 3b respectively.



Fig. 3. (a) Experimental Setup; (b) Python Coding in Raspbian OS







The specification of the performance is Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), Quality factor, Average difference and Maximum deviation are calculated and analyzed. These

parameters are calculated using the formulae's conferred in [19]. The quality factor (Q factor) is a number that determines the degree of loss in the compression process. Further, it is briefly described in <https://www.eprintdriver.com/help/v6.0/ScreenCapture-Toolbar/Dllintr3/19Compression.html>.

Thinking about, the main goals of proposed work closely three different cases are taken as in Table 1 and the result obtained is shown in following Figure 5, 6 and 7. Execution time required in this method also evaluates the efficiency of the algorithm.

This secure image encryption and decryption system is tested for various images and the performance metrics after encryption are given in Table 2. This proposed work also exhibits good encryption and decryption performance even when it is checked with a medical image.

Table 1. Three different Input Cases

	Cover Image	Hidden Image
Case 1 (Common in Image processing)	 Baboon	 Lena
Case 2	 RT Image (Natural city Image)	 Brain
Case 3	 Embryo model (Twin)	 Embryo model (single)

Case 1 (Common in image processing)

When baboon image is taken as cover image and Lena image as hidden image

In Initial phase, Lena image is hidden into Baboon image using the proposed algorithm. Then, in second phase the hidden Lena image is recovered securely by decryption. The execution time is low compared to

conventional algorithm and hence, it reduces its time complexity. This proposed algorithm holds good for the images which are commonly used in image processing as shown in Fig.4(a)-(d). The efficiency of the algorithm is enhanced.

Case 2

When a random natural image is taken as a cover image and a medical image as hidden image

First phase deals with hiding of a medical image considered into a random image taken as a cover image, followed by Reconstruction. In this processing, the execution time took for encryption is more compared to decryption. But, the quality of the decrypted image is high compared to the target image as shown in Fig.5(a)-(d).

Case 3

When both the images taken are medical images (For instance, Embryo model is employed)

Initially, the image whose size is less is taken as hidden image and the larger one is taken as cover image. The image to be hidden is encapsulated into cover image by the proposed technique. The recovering of the hidden image is done securely as shown in Fig.6(a)-(d).

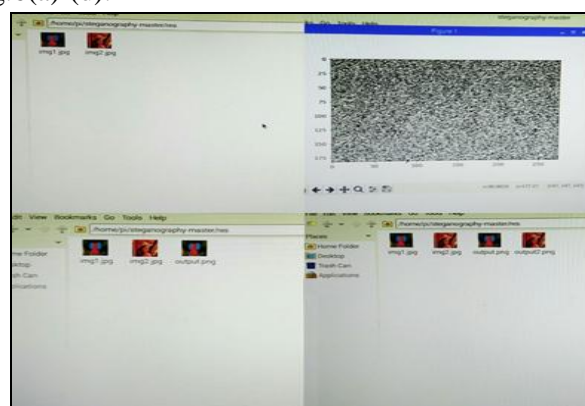


Fig. 4. (a) Two Input images taken; (b) Encrypted Result of the image; (c) Encrypted Output showing the embedding trait of hidden image into cover image; (d) Decrypted Output showing the reconstruction of Hidden image securely

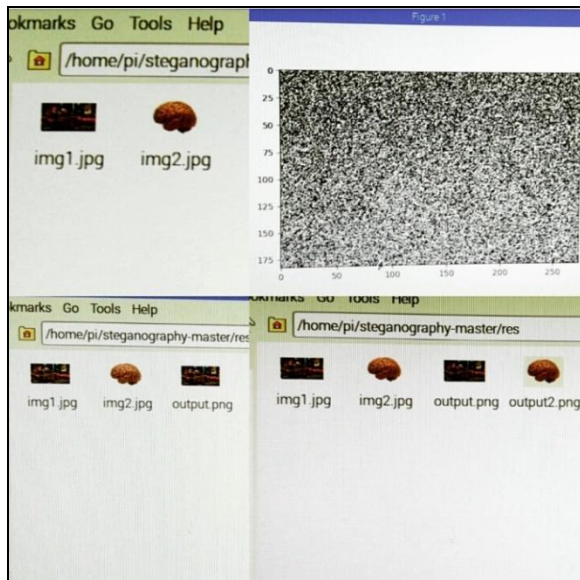


Fig. 5. (a) Two Input images taken; (b) Encrypted Result of the image; (c) Encrypted Output showing the embedding trait of hidden image into cover image; (d) Decrypted Output showing the reconstruction of Hidden image securely.

The decryption time is less compared to encryption time. It reduces the time complexity of the algorithm and thereby enhancing the efficiency. The quality of the final cipher image is high. This designed work holds good for medical images. The results may vary for different medical images. To reinforce the encryption of medical image, further the technique framed is intensified.

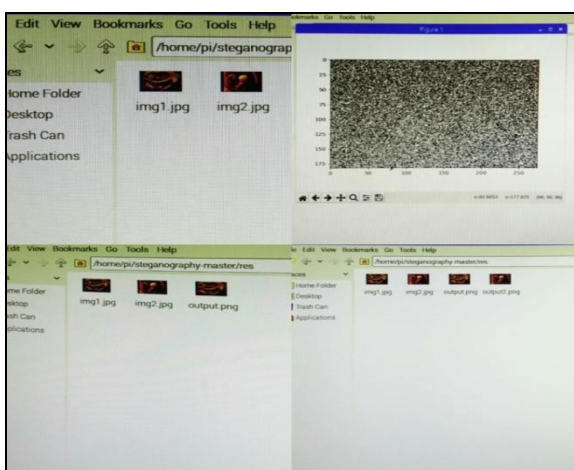


Fig. 6.(a) Shows the two Input images taken; (b) Showing Encrypted Result of the image; (c) Encrypted Output showing the embedding trait of hidden image into cover image; (d) Decrypted Output showing the reconstruction of Hidden image securely

Table2.Performance parameters of various test images

Test Image	Original Entropy	Mean Square Error (MSE)	Peak Signal to Noise Ratio (PSNR) dB	Entropy after encryption	Encryption CPU clock time (Seconds)	Decryption CPU clock time (Seconds)
Baboon	5.2235	28624.0944	11.1739	6.1676	77	37
RT Image	5.7460	25613.0057	29.1725	6.1258	80	35
Medical Image	5.9	25506.0007	25.3136	6.0593	3	2

The efficiency of the algorithm is visualized due to the reduction in complex trait of time. It saves more time in case of decryption compared to encryption since; time required for decryption covers a smaller part in total time. This proposed work holds good for a medical image (For instance, Embryo model is taken in this paper) and the results obtained will be varying for different medical images. Power consumption is less. Reconstruction of original image is easy compared to conventional methods due to Zigzag scanning which is more secure and suited for Real time scenario. It also shows High security level with dominance in image appearance and image data security. The final cipher image is of same size as plain image, so it does not require any additional BW for transmission and space for storage. The visual appearance of the decrypted image is high compared to the target image.

V. CONCLUSION AND FUTURE WORK

The designed work is implemented using Raspberry Pi3 embedded hardware exhibiting image security and low power consumption by encrypting and compressing image simultaneously. More efforts have been taken to high spot the method's significance. It is found that, the proposed work holds good for real time medical image i.e., CPU clock time required for the execution is less compared to other. A visual appearance of the final cipher image is clear than the target image. It provides high security and better image quality. The final cipher image is of same size as plain image so, additional BW and memory is not required for transmitting and storing fast over network. Further, this work can also be enhanced in future to increase the security of the algorithm. Therefore, the trade-off is made between different performance metrics based on real time circumstances and can be actively deployed. This implementation can also serve as a platform for

future enhancements in the domain of producing a secured image irrespective of eavesdropper's attention.

Acknowledgement

The authors are grateful to the Department of Science & Technology, New Delhi, India (SR/FST/ETI-371/2014). They also wish to acknowledge SASTRA University, Thanjavur, India for extending the infrastructural support to accomplish this work.

References

- [1] Narendra K. Pareek, Vinod Patidar, Krishnan K. Sud, "Diffusion-substitution based gray image encryption scheme," *Digital signal processing*, 2013, pp.894-901.
- [2] Cheah Wai Zhao, Jayanand Jegatheesan, Son chee Loon, "Exploring IoT application using Raspberry Pi," *International Journal of Computer Networks and Applications*, 2015, pp.27-34.
- [3] Long Bao, Yicong Zhau, "Image encryption: Generating visually meaningful encrypted images," *Information Sciences*, 2015, pp. 197-207.
- [4] Miao Zhang, Xiaojun Tong, "Joint image encryption and compression scheme based on IWT and SPIHT," *Optics and lasers in Engineering*, 2017, pp.254-274.
- [5] Xiuli Chai, Zhihua Gan, Yiran Chen, Yushu Zhang, "A visually secure image encryption scheme based on compressive sensing," *Signal Processing*, 2017, pp.35-51.
- [6] Shahryar Toughi, Mohammad H. Fathi, Yoones A. Sekhavat, "An image encryption scheme based on elliptic curve pseudo random and advanced Encryption system," *Signal Processing*, 2017, pp.217-227.
- [7] Guodong Ye, Xiaoling Huang, "An efficient symmetric image encryption algorithm based on an intertwining logistic map," *Neuro computing*, 2017, pp.45-53.
- [8] Zia Bashir, Tabasam Rashid, Sohail Zafar, "Hyperchaotic dynamical system based image encryption scheme with time-varying delays," *Pacific Science Review A: Natural science and Engineering*, 2016, pp.254-260.
- [9] Robby Candra, Sarifuddin Madenda, Sunny Arief Sudiro, Muhammad Subali, "The Implementation of an efficient Zigzag scanning," *Journal of Telecommunication, Electronic and Computer Engineering*, 2014, pp.95-98.
- [10] Mario Mastriani, "3D zigzag for multi-slicing, multi-band and video processing," <https://www.researchgate.net/publication/304018142>, 2016.
- [11] Jian-Jiun Ding, Wei-Yi Wei, Hsin-Hui Chen, "Context-Based Adaptive Zigzag Scanning for Image Coding," *Visual communications and image processing (VCIP)*, 2011.
- [12] Dr. S Nagarajan, S. Sankar, "ZZRD and ZZSW: Novel Hybrid Scanning Paths for Squared Blocks," *International Journal of Applied Engineering Research*, 2014, pp.10567-10582.
- [13] Zhuosheng Lin, Simin Yu, Jinhu Lu, Shuting Cai, Guanrong Chen, "Design and ARM-Embedded Implementation of a Chaotic Map-Based Real-Time Secure Video Communication System," *IEEE transactions on circuits and systems for video technology*, 2015, pp.1203-1216.
- [14] Guruprasad K. Basavaraju, "Introduction to Raspberry Pi with Raspbian OS" in <https://www.codeproject.com/Articles/839230/Introduction-to-Raspberry-Pi-with-Raspbian-OS>.
- [15] Smila Mohandhas, Sankar. S, "Novel Algorithms For Finding An Optimal Scanning Path For Jpeg Image Compression," *International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)*, ISSN: 0976-1353 Volume 8 Issue 1, 2014, pp. 229-236.
- [16] Xiaolin Xu, Jiali Feng, "Research and Implementation of Image Encryption Algorithm Based on Zigzag Transformation and Inner Product Polarization Vector," *IEEE International Conference on Granular Computing*, 2010, pp. 556-561.
- [17] S. Jeyalakshmi, S. Prasanna, "Measuring distinct regions of grayscale images using pixel values," *International Journal of Engineering & Technology (IJET)*, volume 7 Issue (1.1), 2018, pp.121-124.
- [18] B. Ananthi, S. Balamohan, M. Hemalatha, "Melanoma Detection Using RGB Color Model in Medical Imaging," *Middle-East Journal of Scientific Research*, 2014, pp.1982-1987.
- [19] Image Fusion Using Approximation and Detail, http://shodhganga.inflibnet.ac.in/bitstream/10603/20682/13/13_chapter%204.pdf chapter 4, pp. 92-117.
- [20] P. Harish, R. Subhashini and K. Priya, "Intruder detection by extracting semantic content from surveillance videos," *2014 International Conference on Green Computing Communication and Electrical Engineering (ICGCCEE)*, Coimbatore, 2014, pp. 1-5. doi: 10.1109/ICGCCEE.2014.6922469.
- [21] R. Subhashini, V. Milani, "Implementing Geographical Information System to Provide Evident Support for Crime Analysis", *Procedia Computer Science*, Volume 48, 2015, Pages 537-540, ISSN 1877-0509, <https://doi.org/10.1016/j.procs.2015.04>.