IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

SECURING DATA IN INTERNET OF THINGS USING STEGANOGRAPHY TECHNIQUES

[1]V.Padmavathi, [2]R.Rohith, [3]B.Sriramamohandoss

[1]Assitant Professor, [2,3]Scholar

[1,2,3]Department of IT,

[1,2,3]A.V.C. College of Engineering, Mannampandal, Mayildathurai.

Abstract: Steganography is the method of hiding secret information like text, password, image and audio behind original cover file. In this paper we proposed an image steganography using raspberry pi. In this system, our aim is to hide message behind the image file the message can be a text, image. The embedded system will help to secure the message with in the image file. In Embedded system, the message much secure because albeit even though if the unauthorized person succeeds in being able to hack the image, the person won't ready to read the message. Secret data like image encrypted into cover data by developing the application involved with LSB algorithm on ARM architecture device. Images with embedded data can be used to convey secrets using easy, fast and stand-alone novel algorithms, which when combined together, yields a more complex algorithm. This paper deals with a significant bit XOR encryption with a recursive diagonal transformation as a pre-processing step and is then embedded employing a using a Least Significant Bit (LSB) steganography. An innovative manner in this entire process using raspberry pi. The results were found to be lossless, secure and high image metric values are achieved.

Index Terms **- IoT, Steganography, LSB**

I. INTRODUCTION

The growing possibilities of modem communications need the special means of security especially on network. The network security is becoming more important because the number of data being exchanged on the Internet increases. Therefore, the confidentiality and data integrity are required to guard against unauthorized access. This has resulted in an explosive growth of the sector of data hiding. In addition, the rapid climb of publishing and broadcasting technology also requires an alternative solution in hide information. To overcome this problem, some invisible information are often embedded within the digital media in such how that it couldn't be easily extracted without a specialized technique. Information hiding is an emerging research area, which encompasses applications like copyright protection for digital media, watermarking, fingerprinting, and Stenography. All these applications of information hiding are quite diverse. With rapid advancement in the world of communications; the necessity for having increased data security is of primary importance. Security is often enhanced using cryptography, steganography or a mixture of both. While cryptography makes the secret unreadable to the third person, it doesn't hide the very existence of the secret. Steganography on the opposite hand, hides the exact same but once discovered, the key is exposed. Thus this paper combines both the cryptography and steganography techniques so as to realize added security. A given plaintext is converted into cipher text using the proposed lightweight encryption mechanism which ensures that none of the data (as a byte) is in its original position in the cipher. For embedding the text inside the image, there is a need for a location map. A novel Super-knight's tour Algorithm has been proposed for the same and has also addressed the problems faced by the existing Knight's tour Algorithm. This methodology is thus called Text as Secret (TAS).

II. RELATED WORKS

W. Zhang et.al [1] Lately, a number of image encryption algorithms that are either based on pixel level or bit level encryption have been proposed. However, not only pixel level permutation, but also bit level permutation has its intrinsic drawbacks. This paper proposes a new cryptosystem to address these drawbacks. Different kinds of permutation algorithms are first comprehensively analyzed and compared. Because, from a bit level perspective, an image can be considered as a natural three-dimensional (3D) bit matrix (width, height, and bit length), a new 3D bit matrix permutation is proposed, in which the Chen system is used to develop a random visiting mechanism to the bit level of the plain-image. By combining aspects of the Chen system with a 3D Cat map in the permutation stage, a new mapping rule is developed to map one random position to another random position (that is, double random position permutation) in the 3D matrix rather than using traditional sequential visiting to the plain-image. Simulations are carried out and the results confirm the security and efficiency of our new cryptosystem.

SghaierGuizni et.al [2] In recent years a growing interest in information hiding in multimedia data as the host has

been observed in the research community. This hidden information can be used for many different purposes, including source identification, copyright protection and covert data transmission. In this paper, an optical crypto technique with adaptive steganography (AS) is proposed for audio/video sequence encryption and decryption. The optical crypto technique is based on double random phase encoding algorithm to encrypt and decrypt the intended audio/video sequences. The main purpose of steganography algorithms is to hide as much information within the cover media as possible. Therefore, for steganography algorithms, the tradeoff is between the amount of covert information being embedded, called stego-data, and that the ensurance for its presence to remain undetected. While their purposes may seem different, recent advances allow more and more the use of advanced watermarking techniques to embed large amounts of covert information that is also robust against removal and detection.

D. Xu et.al [3] proposed that Digital image sometimes needs to be stored and processed in an encrypted format to maintain security and privacy, e.g., cloud storage and cloud computing. For the purpose of content notation and/or tampering detection, the cloud servers need to embed some additional information directly in these encrypted images. As an emerging technology, reversible data hiding in the encrypted domain will be useful in cloud computing due to its ability to preserve the confidentiality. In this paper, a novel separable and error-free reversible data hiding scheme in encrypted images is proposed. After analyzing the property of interpolation technology, a stream cipher is utilized to encrypt sample pixels and a specific encryption mode is designed to encrypt interpolation-error of non-sample pixels. Then, the data-hider, who does not know the original image content, may reversibly embed secret data into interpolation-error using a modified version of histogram shifting and difference expansion technique. In order to adapt to different application scenarios, data extraction can be done either in the encrypted domain or in the decrypted domain. In addition, real reversibility is realized, that is, data extraction and image recovery are free of any error. Experimental results demonstrate the feasibility and efficiency of the proposed scheme.

K. Kainth et.al [4] Encryption is process of converting data into a cipher text in so that only solely licensed parties will have access to it. Image encryption is essentially an important aspect of encryption where 2-D pictorial data is encrypted; hence all the encryption process is performed upon it. In this paper some addition to an antecedent image encryption approach based on SCAN patterns is done in such a simple way that it provides security to great extent. In SCAN methodology the carrier image is generated by employing a distinctive code known as four out of eight-code and addition of carrier image to original image that result into the encrypted image. Rather than encrypting an image in its original pattern, this paper provides another approach within which image is split into totally different elements so that it merged in to a pattern which is solely known to authorize parties and then further encryption and decryption process method is completed. Approach outlined during this paper provides security to bigger extent. All the method of encryption and decryption are enforced in MATLAB and an analysis has been created for various image qualities.

M Pooyan et.al [5] presented a novel method for digital audio steganography where encrypted covert data is embedded into the wavelet coefficients of host audio signal. To avoid extraction error we use lifting wavelet transform. For using the maximum capacity of audio signals, we calculate hearing threshold in wavelet domain. Then according to this threshold data bits are embedded in the least significant bits of lifting wavelet coefficients. Inverse lifting wavelet transform is applied to modified coefficients to construct stego signal in time domain. Experimental results show that proposed method has large payload, high audio quality and full recovery.

S. Chakravarthy et.al [6] Now a days, the need for of data-integrity and privacy is higher than ever. From small bank transactions to large-scale classified military information, these factors have been prerequisites. This classified information can be faked deliberately by the sender with the help of a pseudo secret in order to increase the level of security. Cryptography makes this information unreadable and steganography hides the same. This paper brings together the paths of steganography and Rijndael encryption, which is commonly known as the AES. The secret image or text-file is encrypted using AES algorithm and is then camouflaged into the pseudo-secret image using a modified proposed Knight's Tour-inspired chess-based algorithm that enhances data diffusion. Then the pseudo-secret image/text is once again encrypted using the AES algorithm and is masked into the cover image/text using a checkerboard-based location map. Thus lossless, highly secure, nested-layer steganography is achieved with high complexity and high PSNR for various extension types of images as illustrated in the paper.

III. EXISTING SYSTEM

In previous, cryptography and steganography is used for encryption of data and provides data security. Actually term cryptography provides privacy and steganography is the art and science of communicating in an approach which hides the existence of the communication. The steganography hides the message so it cannot be seen; cryptography jumble a message so it cannot be understood. Cryptography systems can be broadly classified in to symmetric-key systems that use a single key that both the sender and the receiver have, and public key systems that use two keys, a public key known to every one and a private key that only the recipient of messages uses.

IV. PROPOSED SYSTEM

In existing system, if the "Unauthorized user" is in a position to access the content of cipher message steganography with fail to beat this drawback only steganography is employed for sending data like image and make it hidden. Up to now data hiding is completed by using Matlab in order that it's only utilized in systems and laptops, now we are implementing this project in raspberry pi kit with Linux operating system this we can use this in mobile phones also. Steganography algorithm is used for embedding the data in to Portable Network Graphics image and the decoded data is vied by using Cloud over the world.

V. IMPLEMENTATION

In this proposed system, we need to give a input image for securing data and that data is in behind the image in a form of encoded data. Then the new image is created automatically and the decoded word is stored in the new image. That decoded image is written in text file. Client request for the data through apache server. Then the apache server retrieve the output data/decoded data and it is viewed in the local server with username and password.Client request for the data through apache server. Then the apache server retrieve the output data/decoded data and it is viewed in cloud at anywhere and anytime.

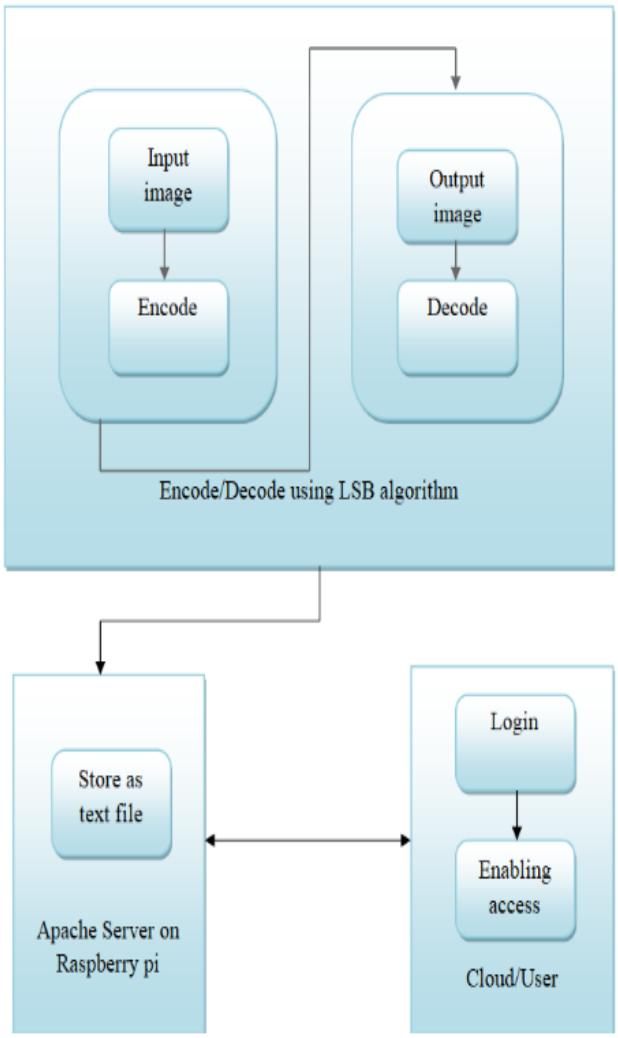

Fig.1: Proposed Architecture

5.1. Encoding

For each character within the data, its ASCII value is taken and converted into 8-bit binary .Three pixels are read at a time having a complete of 3*3=9 RGB values. The first eight RGB values are won't to store one character that's converted into an 8-bit binary. The corresponding RGB value and binary data are compared. If the digit is 1 then the RGB value is converted to odd and, otherwise, even.

The ninth value determines if more pixels should be read or not. If there is more data to be read, i.e. encoded or decoded, then the ninth pixel changes to even. Otherwise, if we want to stop reading pixels further, then make it odd. Repeat this process until all the data is encoded into the image.

5.2. Decoding

Three pixels are read at a time. The first 8 RGB values give us information about the secret data, and the ninth value tells us whether to move forward or not. For the first eight values, if the value is odd, then the binary bit is 1, otherwise it is 0. The bits are concatenated to a string, and with every three pixels, we get a byte of secret data, which means one character. Now, if the ninth value is even then we keep reading pixels three at a time, or otherwise, we stop.

5.3. Server View

Client request for the data through apache server. Then the apache server retrieves the output data/decoded data and it is viewed in the local server with username and password.

5.4. Cloud View

Client request for the data through apache server. Then the apache server retrieves the output data/decoded data and it is viewed in cloud at anywhere and anytime.

VI. ALGORITHM USED

6.1. Least Significant Bit

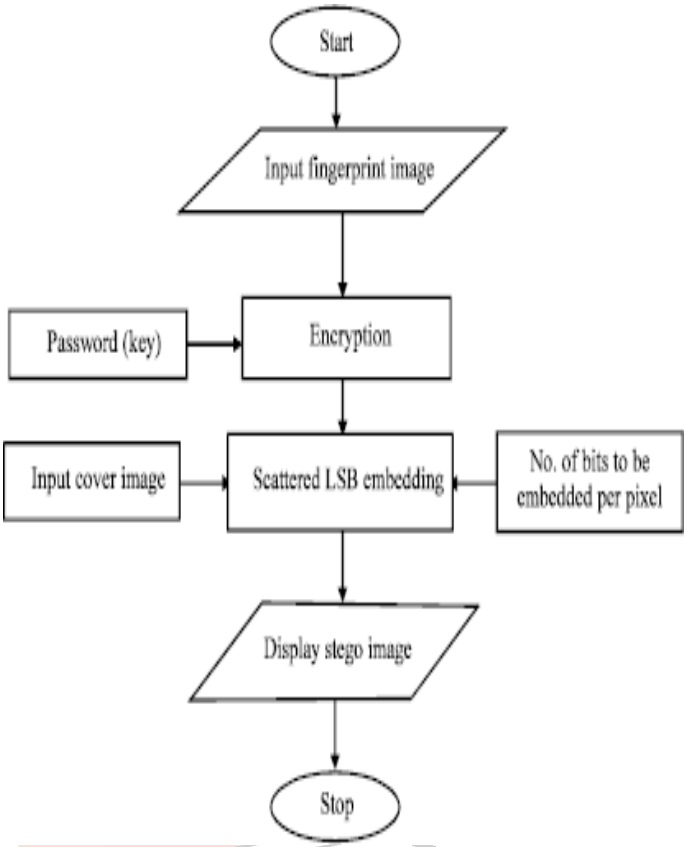

Fig.2: Flow diagram for Least Significant Bit

The Least Significant Bit(LSB) steganography is one such technique in which least significant bit of the image is replaced with data bit. As this method is vulnerable to steganalysis so as to make it more secure we encrypt the raw data before embedding it in the image.In existing system, if the "Unauthorized user" is able to access the content of cipher message steganography will fail, to overcome this drawback only steganography is used for sending data like image and audio and make it hidden. Up to now data hiding is done by using Matlab so that it is only used in systems and laptops, now we are implementing this project in raspberry pi kit with Linux operating system. By this we can use this in mobile phones also. Steganography algorithm is used for embedding the data in to bit map image (.bmp) and joint photographic expert group (.jpg) and audio files like waveform files (.wav).

The algorithm implemented in this project is LSB (least significant bit) algorithm This approach is to replace the data of lower bit in a cover audio data and in a cover image file by a secret data. Secret data like image or audio is encrypted and send in another image or audio, the cover image need to be selected carefully and preferably in gray scale, as the human eye will not detect the difference between different gray values as easy as with different colors. We are using raspberry pi for designing predictive model for image and audio steganography system.

VII. BLOCK DIAGRAM

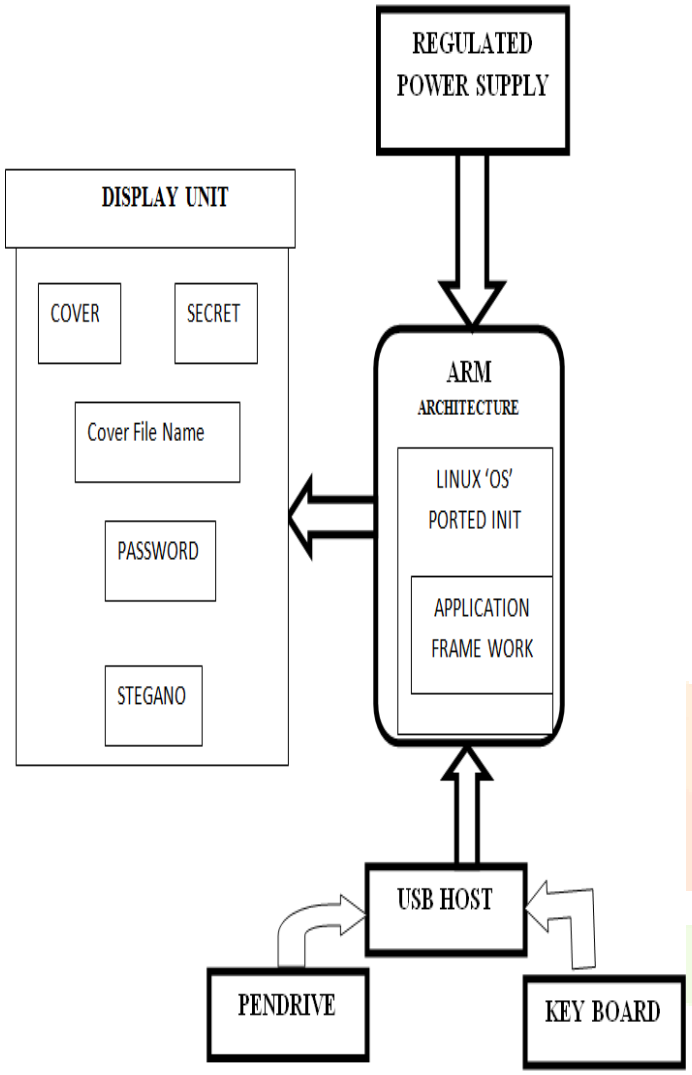

Fig.3: Block Diagram of Steganography Techniques

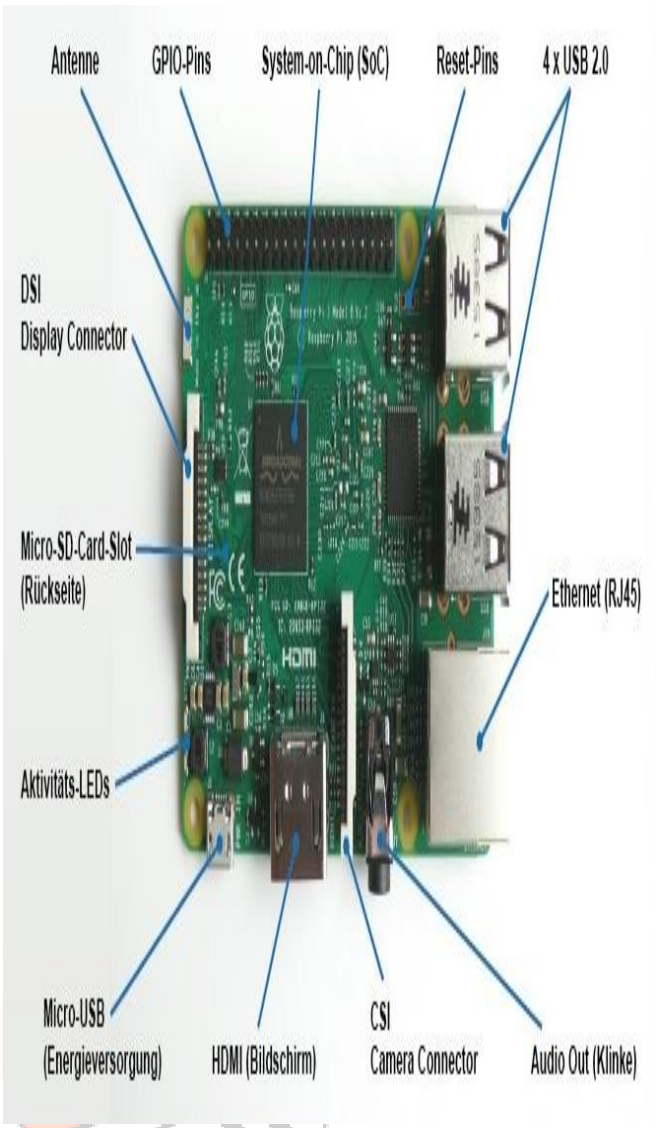

Fig.4: Raspberry Pi 3

VIII. TECHNOLOGY USED

8.1. Raspberry Pi 3B

The Raspberry Pi could also be a series of small single-board computers developed in the UK by the Raspberry Pi Foundation to plug teaching of basic computing in schools and in developing countries. The first model became far more popular than anticipated selling outside its target market place to be used like robotics. It doesn't include peripherals like keyboards and mice. However, some accessories are included in several official and unofficial bundles.

The organization behind the Raspberry Pi consists of two arms. The primary two models were developed by the Raspberry Pi Foundation. After the Pi Model B was released, the inspiration Found about Raspberry Pi Trading, with Eben Upton as CEO, to develop the third model, the B+. Raspberry Pi Trading is responsible for developing the technology while the inspiration is a tutorial charity to plug the teaching of basic computing in schools and in developing countries.

The Raspberry Pi 3's four built-in USB ports provide enough connectivity for a mouse, keyboard, or anything that you simply feel the RPi needs, but if you would like to feature even more you'll still use a USB hub. Keep in mind, it's recommended that you simply use a powered hub so as to not overtax the on-board transformer. Powering the Raspberry Pi 3 is straight forward; just plug any USB power supply into the micro-USB port. There's no power button therefore the Pi will begin else as soon as power is applied, to show it off simply remove power. The four built-in USB ports can even output up to 1.2A enabling to connect more power hungry USB devices (This does require a 2Amp micro USB Power Supply) On top of all that, the low-level peripherals on the Pi make it great for hardware hacking. The 0.1" spaced 40-pin GPIO header on the Pi gives you access to 27 GPIO, UART, I 2C, SPI also as 3.3 and 5V sources. Each pin on the GPIO header is just like its predecessor the Model B+.

8.2. SoC

Built specifically for the new Pi 3, the Broadcom BCM2837 system-on-chip(SoC) includes four high-performance ARM Cortex-A53 processing cores running at 1.2GHz with 32kB Level 1 and 512kB Level 2 cache memory, a VideoCore IV graphics processor, and is linked to a 1GB LPDDR2 memory module on the rear of the board.

IX. RESULTS AND DISCUSION

Now a days, hacking is happened in everywhere and for all purposes. In IoT devices data are easily hacked by hackers so need security to transfer the data. In previous using Cryptography techniques encrypt and decrypt process are used to secure the data .The data is easily hacked by hackers. In this project we used STEGANOGRAPHY technique is used to secure the data inside the image .We used steganography techniques encoding and decoding process in the image to hide the data ,It is used in IOT devices data are securely transfer from user to access. Data receive from IoT devices securely with help of steganography technique. If when hackers hacked the data it will shown only the image. Hackers are not seen the data inside the image. User access the data or see the data in cloud only. User to see the data only in cloud anytime and anywhere No one access the data. In previous steganography techniques is used to hide data in image, text, file to secure the data in IoT. In future, we want to develop this project as a real time application. It is useful to military.

References

[1] W. Zhang, H. Yu, Y. Zhao, and Z. Zhu, "Image encryption based on three-dimensional bit matrix permutation," Signal Processing, vol. 118, pp. 36–50, Jan. 2016.

[2] SghaierGuizni, NidalNaser,"An Audio/Video Crypto Adaptive Optical stegnographyTechnique"IEEE 2012

[3] D. Xu and R. Wang, "Separable and error-free reversible data hiding in encrypted images," Signal Processing, vol. 123, pp. 9–21, Jun. 2016. V. Vijayalakshmi, G. Zayaraz, and V. Nagaraj, "A modulo based LSB steganography method," IEEE, 2006, pp. 1–4.

[4] K. Kainth, D. K. K. Randhawa, and G. Singh, "A potent approach to enhance security extent of an image during image encryption," IEEE, 2016, pp. 1104–1109.

[5] M, Pooyam, A, Delforouzi "LSB based steganography method based on lifting wavelet transform"2007 IEEE International symposium on signal processing and information technology, pp600-603.

[6] S. Chakravarthy, V. Sharon, K. Balasubramanian, and V. Vaithiyanathan, "Art of Misdirection using AES, bi-layer Steganography and novel King-Knight's tour algorithm," in Advances in Signal Processing and Intelligent Recognition Systems, Springer Science + Business Media, 2015, pp. 97–108.

[7] N. Akhtar, P. Johri, and S. Khan, "Enhancing the security and quality of LSB based image Steganography," IEEE, pp. 385–390.

[8] B. Karthikeyan, J. Chakravarthy, and S. Ramasubramanian, "Amalgamation of scanning paths and modified hill cipher for secure steganography," vol. 6, ResearchGate, 2012, pp. 55–61.

[9] C.-K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," Pattern Recognition, vol. 37, no. 3, pp. 469–474, Mar. 2004.

[10] I. Parberry, "An efficient algorithm for the knight's tour problem," Discrete Applied Mathematics, vol. 73, no. 3, pp. 251–260, Mar. 1997.

[11] S. S. Malvika, D. J. D. Abishek, S. Mithula, B. Karthikeyan, and V. Vaithiyanathan, "Tweeting pi: An household computerization system," IEEE, pp. 1306– 1311.

[12] V. Vujović and M. Maksimović, "Raspberry pi as a sensor web node for home automation," Computers & Electrical Engineering, vol. 44, pp. 153–171, May 2015.

[13] S. Chandran and K. Bhattacharyya, "Performance analysis of LSB, DCT, and DWT for digital watermarking application using steganography," IEEE, pp. 1–5.

[14] P. K. Gupta and S. K. Shrivastava, "Improved RSTattacks resilient image watermarking based on joint SVDDCT," IEEE, pp. 46–51.

[15] V. Aslantas, "A singular-value decomposition-based image watermarking using genetic algorithm," AEU - International Journal of Electronics and Communications, vol. 62, no. 5, pp. 386–394, May 2008.

[16] M. Manisha, S. S. Malvika, B. Karthikeyan, V. Vaithiyanathan, and B. Srinivasan, "Devanagari text embedding in a gray image: An offbeat approach," IEEE, pp. 1284–1288