International Journal of Science, Strategic Management and Technology
Volume **02** Issue **05** May-**2026** | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases

OPEN ACCESS

Implementation of Image Steganography on 32-Bit RISC Processor

Author Details:

Prof. Upendra Patil [1], **Er.Praveen Veer** [2] **Er.Vinod Yadav** [3]

[1] Department of Electronics and Telecommunication / HOC College of Engineering / University of Mumbai, Rasayani Dist-Raigad,INDIA
[2] Department of Electronics / Premlila Vithaldas Polytechnic / SNDT Women's University, Mumbai, INDIA
[3] Department of Electronics / Premlila Vithaldas Polytechnic / SNDT Women's University, Mumbai, INDIA
Corresponding Author Email: Praveen.veer@pvp.sndt.ac.in

https://doi.org/10.55041/ijsmt.v2i5.377

Cite this Article: Veer, E. & Yadav, E. (2026). Implementation of Image Steganography on 32-Bit RISC Processor. International Journal of Science, Strategic Management and Technology, *02*(05). https://doi.org/10.55041/ijsmt.v2i5.377

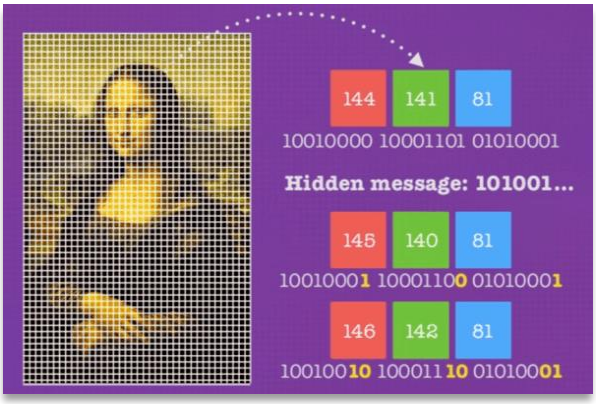
Abstract—
Modern digitization has resulted in versatility to eradicate the divergence among the types of information travel flanked by the users. It presents a pliable approach for the erratic block size selection in an impulsive mode to spice up the extent of sophistication within the stego algorithm. The plan of this work includes the elimination of key exchange for encoding and improving the safety to a large level without compromising the image quality and embedding capacity. The embedded hardware for stego implementations uses a picture carrier that creates soaring demand on memory, the extremely inhibited resource of embedded devices. The efficiency of the algorithm is to take care of image quality. Different applications are there for various requirements of the steganography technique used. This project hides the key message within the first image. The project allows users to decide on the bits for replacement rather than LSB replacement from the image. The sender selects the duvet image with the key text or computer file and hides it into the image with the bit replacement choice; it helps to come up with the secure stego image. The stego image is distributed to the destination with the assistance of a non-public communication network and on the opposite side, the receiver downloads the stego image and using the software retrieves the key text hidden within the stego image.

Keywords—Image steganography, cryptography, LSB method, pixel, Information hiding

I. INTRODUCTION

Steganography may be a Greek word meaning covered writing. The word steganos means covered and graphical means writing. Thus, steganography is that the art of hiding data but also hiding the fact of the transmission of confidential data. Steganography hides the key data in another move into such the simplest way that only the recipient knows the existence of the message [4]. Today the public transmit the info within the variety of text, images, video, and audio over the medium. to soundly transmit confidential data, multimedia objects like audio, video, and pictures are used as cover sources to cover the info [1]. Steganography is defined as invisible communication. Steganography deals with the ways of hiding the existence of the communicated data in such how that it remains confidential. It maintains the secrecy between two communicating parties. In image steganography, secrecy is achieved by embedding data into the duvet image and generating a stego-image. There are differing types of steganography techniques and everyone has its strengths and weaknesses.

This paper reviews the various security and data hiding techniques that are accustomed implement steganography like LSB, ISB, MLSB, etc. In today's world, communication may be a necessity in every growing area [5]. Everyone wants the security of their communicating data. In our everyday life, we use many secure paths just like the internet or telephone for transferring and sharing information, but it's not safe at a specific level. To share the data during a secret manner, there are two techniques that might be used. These mechanisms are cryptography and steganography.



Private information sharing among the people within the current digital world through a selected number of electronic gadgets is rising daily [8]. Steganography may be a type of security technique, the science and art of hiding the existence of a message between a sender and therefore the intended recipient. Steganography is employed to cover secret messages in various kinds of files, including digital images, audio, and video. It includes text, audio, still images, video, etc., the employment of a singular key that encrypts the info embedded in each block has been considered to enhance the protection. In image steganography, a message is embedded into a picture by altering the values of some pixels, which are chosen by an encryption algorithm. to stay the image quality at A level comparable LSB matching, the error reduction has been through with an SWD debugger that greatly improves the error and maintains the imperceptibility of the stego images [3]. Steganography may be very difficult to detect because the image itself looks the identical because the original [8]. This makes steganography an effective tool for phishing emails to spread malicious files instead of attaching them as a file.

Types of Steganography: -

i) Text Steganography: - It consists of hiding information inside the text files. during this method, the key data is hidden behind every letter of each word of a text message. There are different numbers of methods are available for hiding data in an exceedingly document. Some methods are:

a) Format Based Method.
b) Random and Statistical Method.
c) Linguistics Method.

Text steganography are often achieved by altering the text by formatting, or by altering certain characteristics of textual elements (e.g., characters). the most goal is to style coding methods to develop alterations that are reliably decodable. These criteria, reliable decoding, and minimum visible change are somewhat conflicting; herein lies the challenge in designing document marking techniques. The three coding techniques that propose illustrate different approaches. The techniques are used either separately or jointly. These are following:

a). Line-Shift Coding: This is a method for altering a document by vertically shifting the locations of text lines to encode the document uniquely.

b). Word-Shift Coding: This is a method for altering a document by horizontally shifting the locations of words within text lines to encode the document uniquely.

c). Feature Coding: This is a coding method which is applied either to a format file or to a bitmap image of a document.

ii) Image Steganography: - Hiding the information by taking the quilt object as a picture is noted as image steganography. In images, steganography pixels are accustomed hide the information. In digital steganography, images are widely accustomed cover sources because there are variety of bits present in an exceedingly digital representation of a picture.

iii) Audio Steganography: - In audio steganography, the key message is embedded into a digitized audio signal which ends up in slightly altering a binary sequence of the corresponding audio file. There are too many methods are available for audio steganography. It involves hiding data in audio files. This method hides the info in WAV and MP3 sound files. There are different methods of audio steganography:

a) Low Bit Encoding.
b) Phase Coding.
c) Spread Spectrum.

iv)Video Steganography: - it's a method of hiding any quite files or data in digital video format. during this case, video is employed as a carrier for hiding the information. Generally, discrete cosine transforms (DCT) alter the values which are wont to hide the information in each of the pictures within the video, which is unnoticeable by the human eye. H.264, Mp4, MPEG, and AVI are the formats employed by video steganography. all told these methods, the essential principle of steganography is that a original image is to be embedded in another secrete message.

II. LITERATURE REVIEW

Bearing this fact in mind, embedding techniques using LSB substitution methods has become accepted in steganography (Amirtharajan and Rayappan, 2013; Chan and Cheng, 2004; Cheddad et al., 2010) [1][4][5]. Variable number of data bits encoding on the LSB positions of a cover pixel as dictated by the bits in the MSB positions of the same pixels are also in practice. The other form of LSB technique called LSB matching finds the best matching portion of the cover to embed the data [4]. Although, the matching technique helps in maintaining excellent image quality by minimizing the distortions, it slows down the space of the algorithm on producing the stego image. Inclusion of randomization during the selection of cover pixel sequence for data embedding has been a means to improve security [6]. Bytes of pixels are sufficient to carry one message byte. Rest of the bits in the pixels remains the same. Steganography is the art and science of communicating in a way which hides the existence of the communication [9].

Steganography plays an important role in information security. It is the art of invisible communication by hiding information inside other information. The term steganography is derived from Greek word and means covered writing. A Steganography system consists of three elements: cover image (which hides the secret message), the secret message and the stegno image (which is the cover object with message embedded inside it) [7]. A digital image is described using a 2-D matrix of the intestines at each grid point. Typically, gray image uses 8 bits, whereas colored image utilizes 24 bits to describe the color model, such as RGB model. The Steganography system which uses an image as the cover, there are several techniques to hide information inside cover-image. The spatial domain techniques manipulate the cover-image pixel bit values to embedded the secret information. The secret bits are directly embedded to the cover image pixel bytes [2]. The spatial domain techniques are simple and easy to implement. The Least Significant Bit (LSB) is one of the main techniques in spatial domain image Steganography. The concept of LSB technique is simple. Therefore, an altered image with slight variations in its colors will be indistinguishable from the original by a human being. In conventional LSB technique, which requires 8 bytes of pixels to store 1byte of secret data.

III. METHODOLOGY

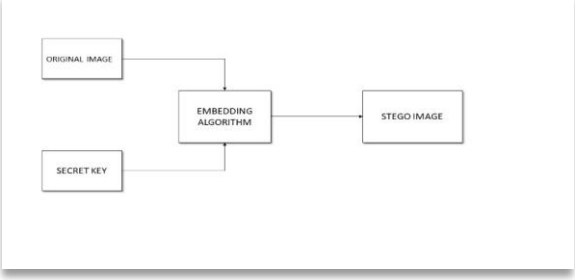


Figure 1 Block Diagram

In figure 1, The algorithm focuses on colored images that can be fit in to the existing on chip SRAM of 32 KB in the embedded processor CORTEX M4 (STM32F407VET6) chosen for hardware implementation. The algorithm was developed in STM32 Cube IDE using the Embedded-C language. The embedded code was compiled with STM32 compiler of STM32 Cube IDE.

Least Significant Bit (LSB): - The Least Significant Bit (LSB) method is the easiest way to embed secret information. In the receiver, only purpose is to extract secret information bits from the corresponding locations. To increase the detection of difficulty of secret data, a pseudo random sequence can be used to control the location, in which the secret binary information is going to be embedding. The LSB method is simple and easy to implement, embeds and extracts information fast, and has a high hiding capacity.

Below is the example of replacing bit in image to text.

Pixel :(00100111 11101001 11001000)

(00100111 11001000 11101001)

(11001000 00100111 11101001)

Char : A

Decimal: 65

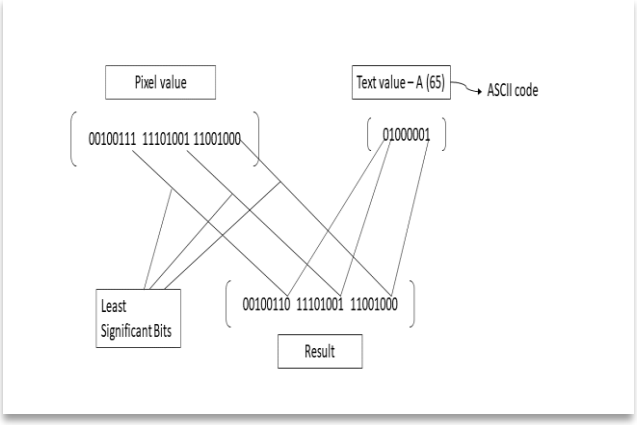
Bit : 01000001

International Journal of Science, Strategic Management and Technology
Volume **02** Issue **05** May-**2026** | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases

Result :(00100110 11101001 11001000)

(00100110 11001000 11101000)

(11001000 00100111 11101001)



LSB is the most popular Steganography technique. Many carrier messages which can be used in the recent technologies, such as Image, text video and many others. LSB uses the image as carrier message because the image file is the most popular because it easy to send during the communication between the sender and receiver. It uses the RGB model of colour image as carrier message. The RGB image has 24 bits values per pixel (00000000, 00000000 and 00000000) for black and (11111111, 1111111 and 11111111) for white pixels. It hides the secret message in the RGB image based on it its binary coding. Above example about pixel values and shows the secret character replacing in pixel using LSB method.

LSB method is used to hide the secret messages by using algorithm. LSB makes the changes in the image resolution quite clear. From the above example it is clear we are hiding two least significant bits directly. But they occur a problem when we hide these two least significant bits in the image, the resolution of the image becomes blur. So that there becomes a difference between original image and encoded image. The quality of the image does not remain same after hiding these bits. This is the main problem of LSB technique. The basic idea of propose method is that choose one pixel of the image randomly, select this pixel as the centre of the image and divide the image into three red, green and blue parts separately according this centre pixel. Now hide two by two bits of the secret message in each part of the pixel by searching about the identical, if the identical found satisfied then set the image with new values if the identical does not find, hide in the two least significant bits and set the image with new values. Now save the location of the hiding bits in binary table. This modification will give the same image quality as original image.

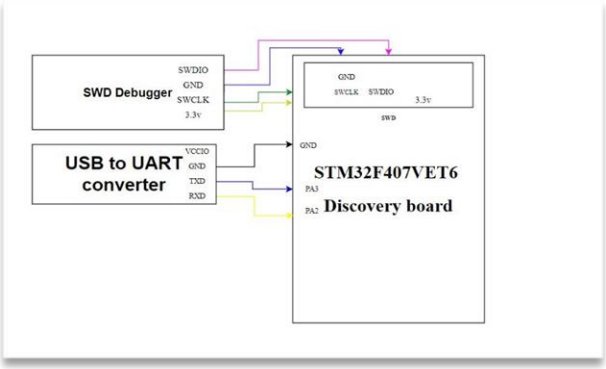


Figure 2 Hardware Connection

In Figure 2, STM32F407VET6 board is connected with UART to USB converter and SWD. Converter shows transmit and receive the algorithm in microcontroller. Debugger is confirm the Algorithm is read and write the data in microcontroller. Also debugger is connected with Computer/laptop for power up the microcontroller board.

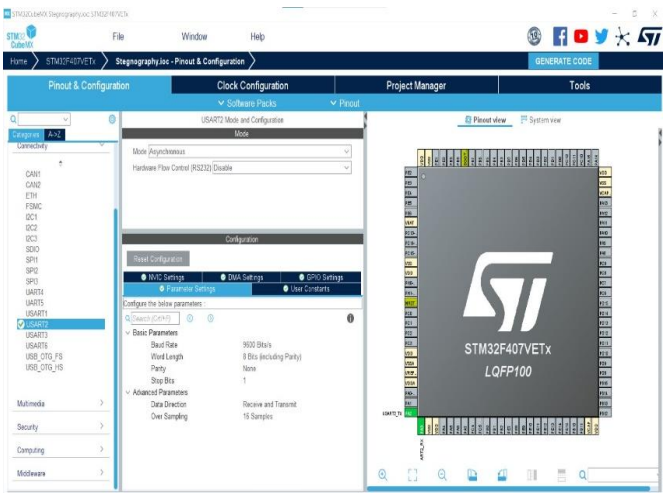


Figure 3 STM 32 Cube MX

Figure 3, shows the pinout diagram of microcontroller using STM32 cube MX. Here we give the input as a transmitter and receiver for USB to UART converter using pin PA2 & PA3.

Below are steps for pinout configuration:

1. Select pin PA2 & PA3.

2. Go to connectivity section and select UART 2 and 3, for activate the pin.

3. After activate the pins select Asynchronous mode.

4. Then check other parameters.

International Journal of Science, Strategic Management and Technology
Volume **02** Issue **05** May-**2026** | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases

5. Now fix he clock Configuration.

6. After all the setting click on “Generate code”.

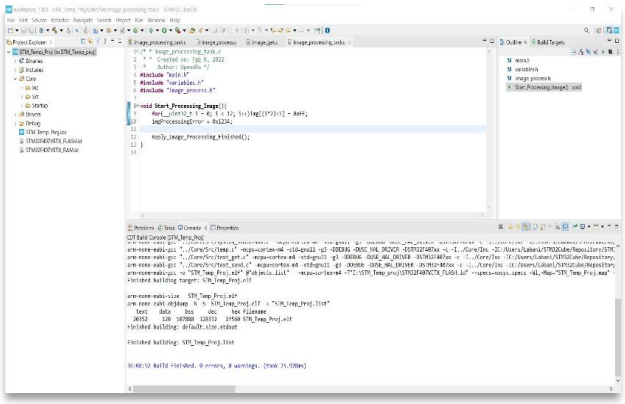


Figure 4 STM32 Cube IDE

In Figure 4, you can see the algorithm which can transmit and receive using Converter to microcontroller. Before starting the Cube IDE first we have to configure the pinout which is shown in above figure. After the last steps of generating code you will see the Cube IDE window. In that you can generate the code. Then click on clean project and build project. If error is found solve the errors. After success of algorithm check on Cube Programmer is the algorithm is successfully read and write on Microcontroller which is shown in below figure.

Figure 5 STM32 Cube Programmer

Below are the steps After opening the GUI:

1. In that first connect the board using converter and click on “Reset Button” at board. Now Board is ready to process.

2. Then click on “Open Image”. It will show the left side of upper box.

3. Then Send and Read the Text in right side of GUI.

4. After this click on “Read image”. Image will be read and it’s shown in left side of Bottom Box.

5. Next click on “Process image button”. Now “Image processing is finished” This command you will see in Right side of Bottom Box.

6. Now again click on “Read image”. Now this is the show the processed image (Text is hidden in image).

7. Now get the snapshot of different visuals.

IV. RESULTS AND DISCUSSION

Below is the Output of Image steganography.

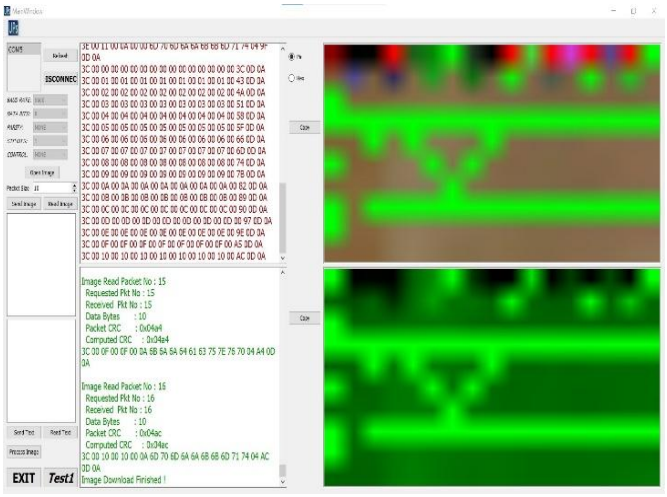


Figure 6 Read and Write Image

Figure 6 shows the Read and Write the image. Before this connect the com port(converter) in GUI. Then simply click on “Open Image” Button. After open the image click on “Send image” and “Read Image”. When the image is transmitting and reading led will blink from converter, which means the image is reading and writing.

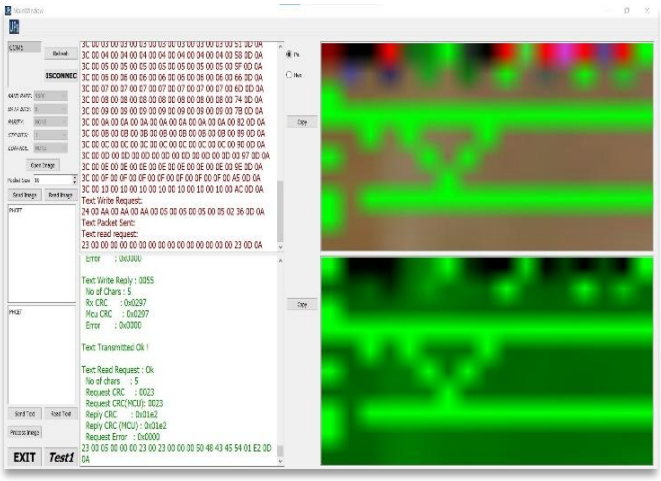


Figure 7 Read and Write Text

International Journal of Science, Strategic Management and Technology
Volume **02** Issue **05** May-**2026** | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases

Figure 7, shows the Read and Write the Text. After read and write the image Write a secrete text and click on "send text" and "Read text". When the text is transmitting and reading led will blink from converter, which means the text is reading and writing.

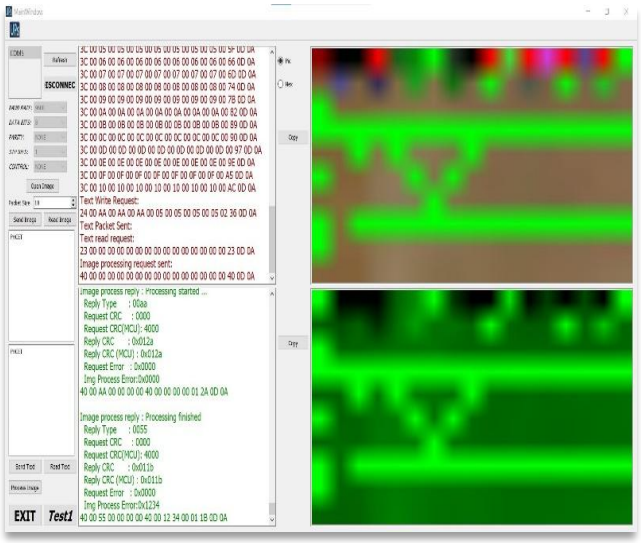


Figure 8: Image Processing

Figure 8, shows the processing image, which means process of hiding text to image. After processing image message will show "Image processing is finished".

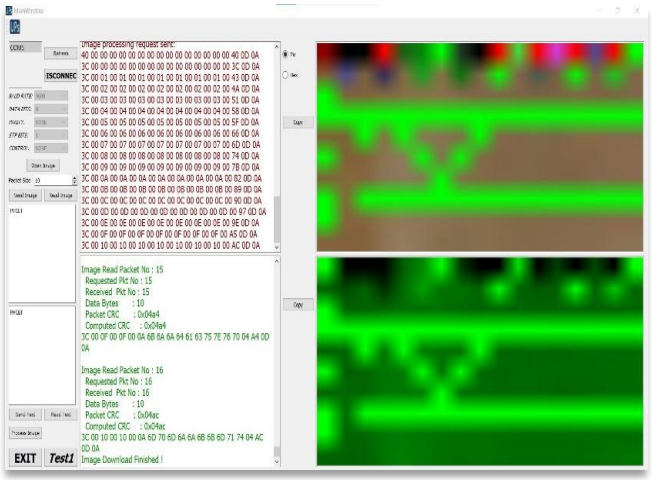


Figure 9: Stenographic Image

Figure 9, shows Steganographic image. In this after finishing image processing simply click on "Read image". The image will show text is hide in image. There is not much change in image using method. The pixels are less bright than original image.

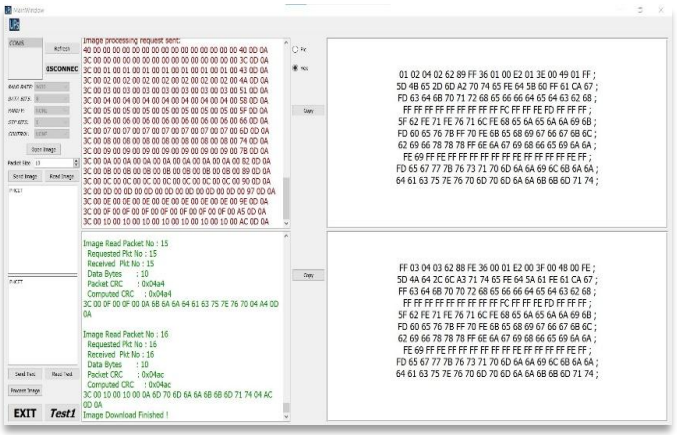


Figure 10: Stenographic Image in Hex form

Figure 10, shows Steganographic image in Hex form. In this Image steganography is shown in Hex form, which means original image shown in hex form and process image also shown in hex form. In original image secrete text is hide which is shown in hex form.

V. CONCLUSION

Steganography though is still a new idea. There is an advancement in the computer field, suggesting advancements in the field of steganography as well. It is likely that there will soon be more efficient and more advanced techniques for Steganalysis. A advancement is the improved sensitivity to small messages. Knowing how difficult it is to detect the presence of a large text file within an image, imagine how difficult it is to detect even one or two sentences embedded in an image! It is like finding a microscopic needle in the ultimate haystack.

Steganography is an efficient way of a secure communication. First encrypt the confidential file and then hide it inside an image of another kind of file before sending to some other.it will decrease the chances of being detected. If a message, is encrypted or hide with a steganographic method, it provides an additional layer of protection and reduces the chance of the hidden message being detected. However, if he only finds a normal image file, he will have no clue. It can be used by government organization to use as the way to send and receive files securely. Steganography is still new concept to the public. The project introduces a tiny part of the art of steganography. Steganography goes well beyond simply hiding text information in an image.

the key findings of your research and their implications for theory, practice, or policy. Highlight the significance

of your contribution and suggest areas for future work. Avoid repeating sentences from the abstract.

REFERENCES

[1] Abomhara, M., O.O. Khalifa, O. Zakaria, A.A. Zaidan, B.B. Zaidan and H.O. Alanazi, 2010. Suitability of using symmetric key to secure multimedia data: An overview. J. Applied Sci.,10: 1656-1661.

[2] Amirtharajan, R. and J.B.B. Rayappan, 2013. Steganography-time to time: A review. Res. J. Inform. Technol., 5: 53-66

[3] Chan, C.K. and L.M. Cheng, 2004. Hiding data in images by simple LSB substitution. Pattern Recognition., 37: 469-474

[4] Cheddad, Abbas, et al." Digital image steganography: Survey and analysis of current methods." Signal processing 90.3 (2010): 727-752.

[5] Mohd, Bassam J. Thaier Hayajneh, and Ahmad Nahar Quttoum." Wavelet-transform steganography: Algorithm and hardware implementation." International Journal of Electronic Security and Digital Forensics 5.3-4 (2013): 241-256.

[6] Zhenghao Shi and Lifeng He," Application of Neural Networks in Medical Image Processing" Second International Symposium on Networking and Network Security (ISNNS 10).

[7] M.Vrhel E. Saber, and H.J. Trussell, "Color image generation and display technologies," IEEE Signal Processing Mag., vol. 22, no. 1, pp. 23–33, Jan. 2005.

[8] K.N. Plataniotis and A.N. Venetsanopoulos, Color Image Processing and Applications. Heidelberg: Springer, 2000.

[9] Huang T. S., Schreiber, W. F., Tretiak, O. J. (1971). Image processing. Proceedings of the IEEE, 59(11), 1586–1609.

[10] J.M. Abrham, C. E. Catchpole, and G. W. Goodrich, "Image processing with a multiaperture, image dissector," SPIE J., vol. 6, 1968, pp. 93-96.

[11] F.C. Billingsley, "Applications of digital image Processing," Appl. Opt., vol. 9, Feb.1970, pp.28

[12] R.N. Bracewell, The Fourier Transform and its Applications. New York; McGraw-Hill, 1965

[13] A. Habibi and P.A. Wine "Image coding by Linear transformations and block quantization," IEEE Trans. Commun. Technnol., vol.COM 19, Feb 19/1, pp.50-62

[14] Xiong, Zixiang, Onur G. Guleryuz, and Michael T. Orchard. "A DCT-based embedded Image coder." IEEE Signal Processing Letters3,11(1996): 289-290.

[15] Eiji Kawaguchi, et al: A Model of Anonymous Covert Mailing System Using Steganographic Scheme, in INFORMATION MODELLING AND KNOWLEDGE BASES XIV, H. Yaakkola et al (Eds), IOS Press, pp.81-85, 2003.