JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Double Layered Data Security Via AES and Modified LSB Image Steganography Using A Filtering Algorithm

[1*]Sharad S. Hegade, [2]Dr. S. R. Pande
[1]Research Scholar, [2]Professor
[1, 2]Department of Computer Science, SSESA's Science College, Nagpur, India

Abstract: In digital space, data plays a vital role, so considered an asset. Hence, the sender and recipient must be more cautious during communication. Moreover, data is stolen and altered over the internet during its transmission. During the transmission of data over the internet needs to provide security is essential. Therefore, to provide additional security during data transmission, there are cryptography and steganography methods. In cryptography, the information is scrambled using a secret key, but an intruder can able to identify its existence by seeing it. On the other side, steganography hides the existence of a secret message in the cover work which is not seen by the naked eye easily. This paper introduces a new idea for implementing a blending model of data security using cryptography and steganography. In modified LSB image steganography using a filtering method, the 24-bit color image is used as the cover image. In this image steganography, not all three color channels of each pixel of an image are used for data hiding. That means in the proposed filtering algorithm, a single color channel out of three of every pixel of an image is selected as the candidate color channel for data embedding and also the candidate color channel for each pixel is dependent on the filtering algorithm. For implementing an additional layer of security, before embedding AES encryption is applied to the secret message. The proposed experiment is evaluated by calculating the PSNR, and MSE of the stego image, and using Histogram analysis. The said method produces high PSNR and low MSE.

Keywords- Data security, Cryptography, Steganography, Filtering method.

I. INTRODUCTION

Day by day digital world touches every corner of human life. Its growth rate follows the exponential phenomena of expansion. Therefore, huge amounts of data are transmitted over the internet. Communication is one of the important sections of it. In human life, communication between human beings is an important corner of society. Hence, digital communication needs to be secure from intruders. Cryptography and steganography are two means of implementing data security[1]. Cryptography converts plain text into cipher text using a private key, but its existence is seen by everyone[2][3]. On the other side, steganography hides the writing into cover work which is unseen to the attackers[2], [3]. Individually both of us provide advantages with their limitations. Hence, a combined approach of cryptography and steganography into one system provides a more robust solution as compared to individuals[4].

Cryptography is a scientific way to secure digital communication over insecure public channels. It broadly connects with confidentiality, integrity, source authentication, and key management[5][6]. Cryptographic system is categorized into Symmetric key, Asymmetric key, and Hash function. In symmetric key cryptography, the same secret key is used for both encryption and decryption. Whereas, public and private keys are used for encoding and decoding respectively in asymmetric key cryptography. In hash function cryptography, no key is used and it calculates a fixed-length hash value on the input message.

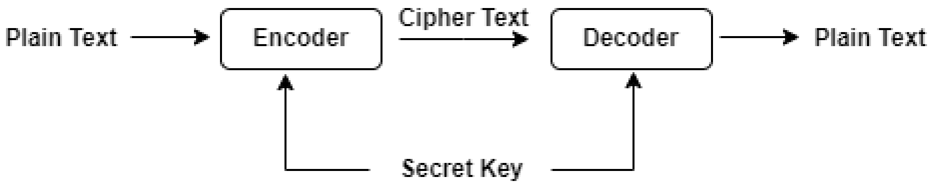


Figure 1: Basic Cryptography Model

In steganography, a secret message hides in cover work. The cover work may be an image, video, audio, text, etc[7][8]. The existence of a secret message is unknown except sender and recipient. If existence is understood by an intruder, then steganography fails[9].

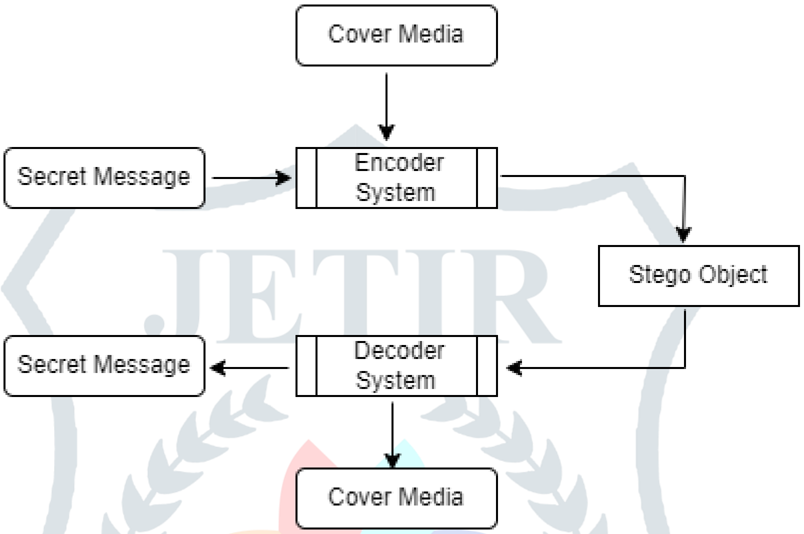
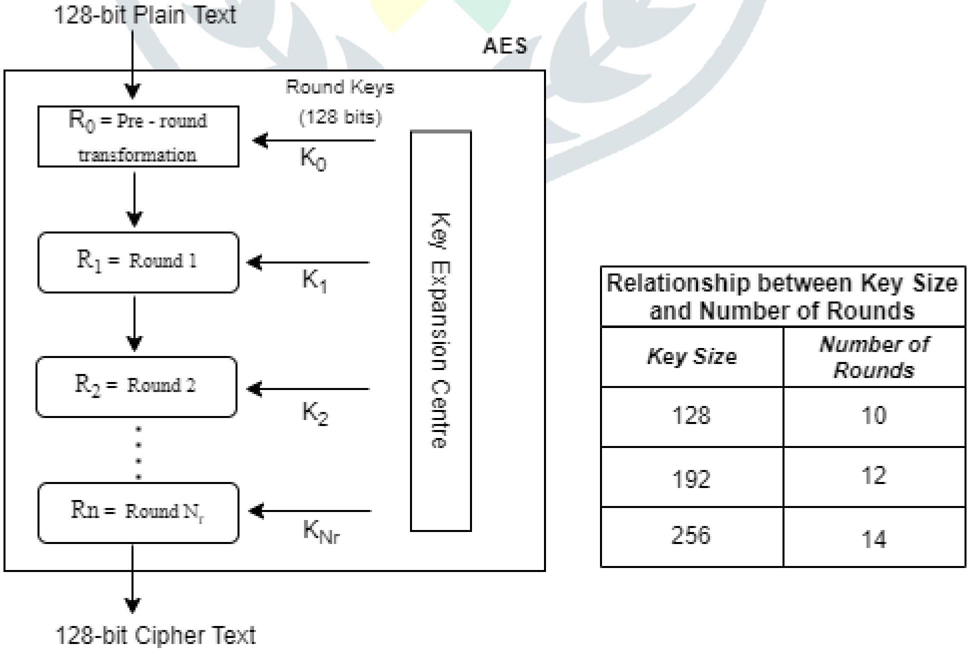


Figure 2: Basic Steganography Model

In our proposed method, 24-bit color image, Modified LSB image steganography using filtering method and AES cryptography is used. The following Figure 3 illustrates the architecture of 128-bit AES cryptography.



Relationship between Key Size and Number of Rounds	
Key Size	*Number of Rounds*
128	10
192	12
256	14

Figure 3: Architecture of AES Encryption

II. RELATED WORK

In the field of data security, implementing a robust and secure system combining the approach of cryptography and steganography is used. There is a lot of work related to implementing cryptography and steganography into one system available.

The paper [10] introduced a novel steganography technique in which a 24-bit color image is used. They counted the number of 1's and 0's of the Red color component of the pixel, then computed the absolute difference between them. Finally, the obtained result is divided by 2, and that number of bits is embedded into the remaining Green and Blue color components of that pixel.

Authors at [11] proposed a blended system of cryptography and steganography. In which, a secret message is encrypted using the Vernam cipher algorithm and then cipher text is hidden into an image using LSB with Shifting (LSB-S).

The methodology at [12] implemented digital image watermarking using ANN and LSB. They first hide the image into another image using LSB, and then the ANN method is used to display secret information.

Research at [13] developed a novel method in which plain text is encrypted using AES and then proposed a filtering method that filters the entire image to find out the candidate pixel. Finally, the ciphered message is added to an image using a user-defined password and LSB steganography.

At [14], the authors proposed a modified LSB with a stream builder filtering to find out locations to hide the secret data. To implement a more secure environment, before embedding secret messages get ciphered using AES.

An efficient filtering-based approach of modified LSB image steganography using status bit and AES implemented at [15]. This technique performs steganographic operations on a Bitmap image. The two-layered security is implemented in such a way secret data is converted into cipher text using AES and then modified LSB steganography with a filtering method that uses MSB bit for filtering.

Authors at [16] implemented encryption using RSA and LSB video steganography via 1,2,3 – LSB. They also concluded that 3-LSB is much better as compared to 1,2–LSB.

In the proposed method [17], authors designed two different security mechanisms for mobile systems. In the first module, the hash digest of the password is calculated using hash algorithms such as Message Digest 5 (MD5), Secure Hash Algorithm 1 (SHA-1), SHA-256, SHA-384, and SHA-512. Then digest is embedded into a cover image using LSB steganography. In the second method, they calculated password digest by using Message Digest 5 (MD5), Secure Hash Algorithm 1 (SHA-1), SHA-256, SHA-384, and SHA-512, then obtained digest encrypted using AES before hiding data into an image using LSB steganography. Through this, they have implemented confidentiality and integrity.

The multi-layer security model at [18] implements a secret message enciphering using XOR or OTP-based cryptography which uses a secret key as a randomly generated key and a user input key respectively. LWT was applied on the cover image to obtain the LH sub-band for hiding cipher text. Additional security is implemented via scrambling the stego image and finally, visual cryptography is applied to it.

III. RESEARCH METHODOLOGY

Dual-layer data security is implemented using cryptography and steganography. The general layout of our proposed model is depicted in **Figure 4**. Initially, the secret message was enciphered using a 128-bit AES encryption. The process of 128-bit AES encryption is depicted in **Figure 3.** The second layer of security is implemented using modified LSB image steganography. The cover image used in steganography is a 24-bit color image consisting of equal-sized Red, Green, and Blue color channel components.

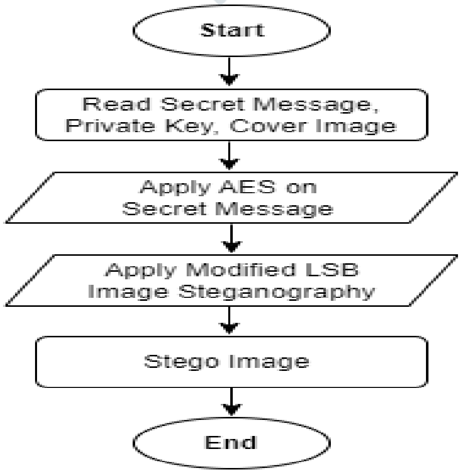

Start
Read Secret Message, Private Key, Cover Image
Apply AES on Secret Message
Apply Modified LSB Image Steganography
Stego Image
End

Figure 4: State diagram of the Proposed System

Data Embedding Process

Before embedding secret data, it gets converted into scrambled cipher text. In our proposed algorithm, to implement invisible data hiding non-secret 24-bit color image file is used. During data embedding all the pixels of an image are used sequentially, but not all color channels of that pixel. Any one color channel of each pixel selected for embedding is based on the proposed filtering method. Figure 5 indicates the flow of the filtering method and data-hiding process, whereas, Table 2 discusses both of them with examples. The following algorithm describes the working of the proposed color channel component of the pixel of image filtering method and data embedding:

```
i.   Input 24-bit color image and cipher text equivalent of plain text.
ii.  If (cipher text = = NULL), stop the process. Otherwise, visit to next step.
iii. proposed filtering method:
     a) read the next pixel of an image.
     b) Calculate R = (Value of R color channel) AND (~1), G = (Value of G color channel) AND (~1), and
        B = (Value of B color channel) AND (~1).
     c) Find the total count of all ON bits of 2’s complement of calculated R, G, and B separately and also find
        out the maximum of them (R-Max / G-Max / B-Max).
iv.  Data embedding process:
     Bit = read next cipher bit.
     a) If R-Max, then embeds as R = (R) OR ((Bit) XOR (2nd LSB of R)). Visit to step ii.
     b) If G-Max, then embeds as G = (G) OR ((Bit) XOR (3rd LSB of G)). Visit to step ii.
     c) If B-Max, then embeds as B = (B) OR ((Bit) XOR (4th LSB of B)). Visit to step ii.
```

Data Extraction Process

At the recipient's end, the data extraction process is followed. In Figure 6, the execution flow of reverse data filtering and data extraction process are depicted. Table 3 explains both of them using the examples. The algorithm for the said mechanism is as follows:

```
i.   Read the stego image.
ii.  proposed reverse filtering method:
     a) read the next pixel of the stego image.
     b) Calculate R = (Value of R color channel) AND (~1), G = (Value of G color channel) AND (~1), and
        B = (Value of B color channel) AND (~1).
     c) Find the total count of all ON bits of 2’s complement of calculated R, G, and B separately and also find
        out the maximum of them (R-Max / G-Max / B-Max).
iii. Data extraction process:
     a) If R-Max, then extracts as Bit = ((Value of R color channel) AND (1)) XOR (2nd LSB of R).
     b) If G-Max, then extracts as Bit = ((Value of G color channel) AND (1)) XOR (3rd LSB of G).
     c) If B-Max, then extracts as Bit = ((Value of B color channel) AND (1)) XOR (4th LSB of B).
iv.  If all hidden bits are extracted, then stop the process. Otherwise, visit to step ii.
```

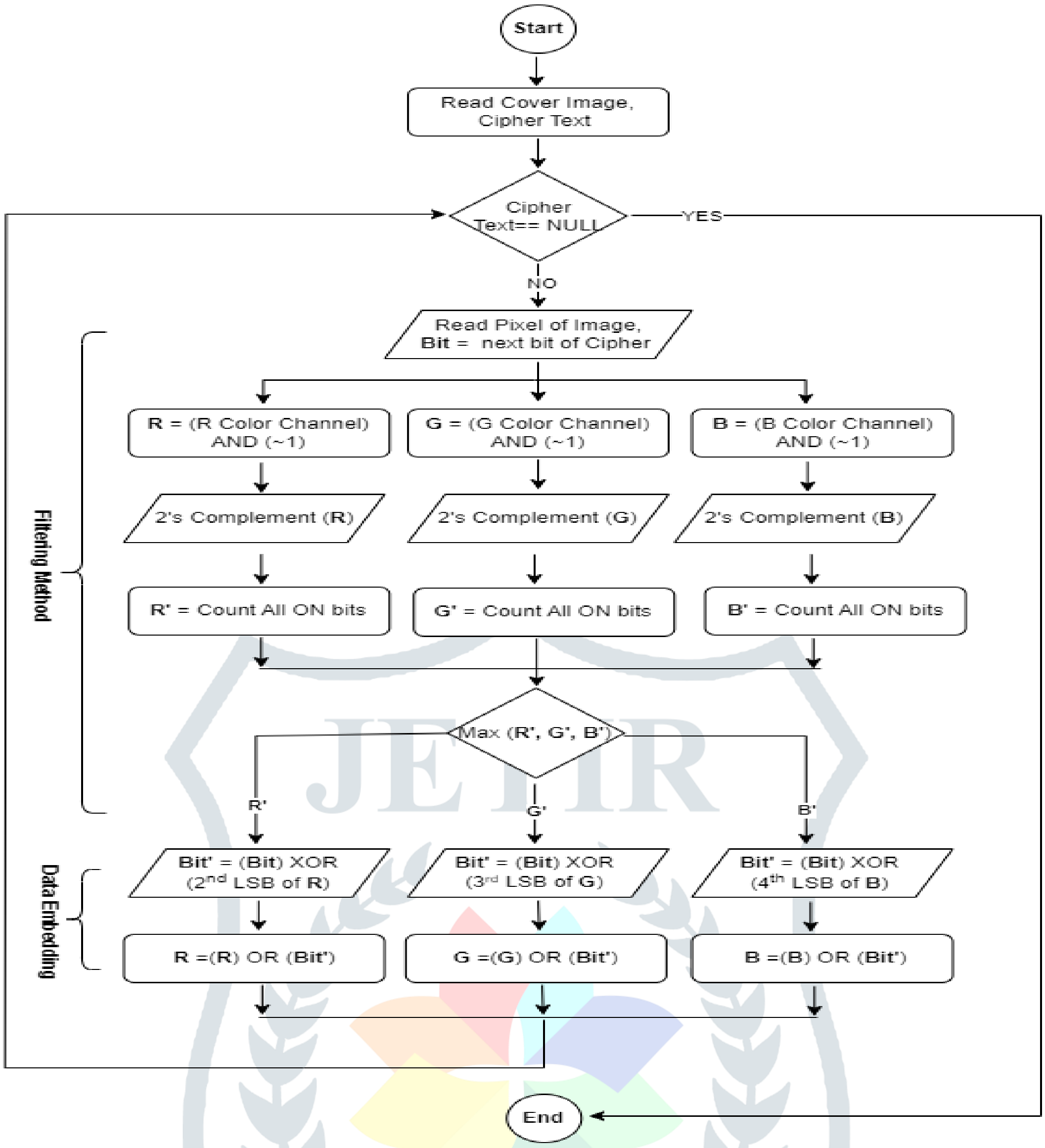

Start
Read Cover Image, Cipher Text
Cipher Text== NULL
YES
NO
Read Pixel of Image, Bit = next bit of Cipher
R = (R Color Channel) AND (~1)
G = (G Color Channel) AND (~1)
B = (B Color Channel) AND (~1)
2's Complement (R)
2's Complement (G)
2's Complement (B)
R' = Count All ON bits
G' = Count All ON bits
B' = Count All ON bits
Max (R', G', B')
R'
G'
B'
Bit' = (Bit) XOR (2nd LSB of R)
Bit' = (Bit) XOR (3rd LSB of G)
Bit' = (Bit) XOR (4th LSB of B)
R =(R) OR (Bit')
G =(G) OR (Bit')
B =(B) OR (Bit')
Filtering Method
Data Embedding
End

Figure 5: Filtering method and Data embedding flowchart

Table 2: Filtering method and Data embedding

Pixel No.	**Color Channel**	**Channel value**	**(3)AND ~1**	**2's Complement of (4)**	**ON bit Count of (5)**	**Color component of (2) related to Max of (6)**	**Data Bit**	**Using pixel color component of (7): (8) XOR (2nd / 3rd / 4th LSB of (4) of R / G/ B resp.)**	**Based on (7): (4) OR (9)**
(1)	**(2)**	**(3)**	**(4)**	**(5)**	**(6)**	**(7)**	**(8)**	**(9)**	**(10)**
1	R	11001010	11001010	00110110	4	G	0	0	11001010
	G	01100010	01100010	10011110	5				0110001**0**
	B	01011111	01011110	10100010	3				01011110
2	R	11001001	11001000	00111000	3	B	0	1	11001000
	G	01100001	01100000	10100000	2				01100000
	B	01011110	01011110	10100010	3				0101111**1**
3	R	11010000	11010000	00110000	2	B	1	1	11010000
	G	01101000	01101000	10011000	3				01101000
	B	01100101	01100100	10011100	4				0110010**1**
4	R	11001101	11001100	00110100	3	B	0	1	11001100
	G	01100101	01100100	10011100	4				01100100
	B	01100010	01100010	10011110	5				0110001**1**

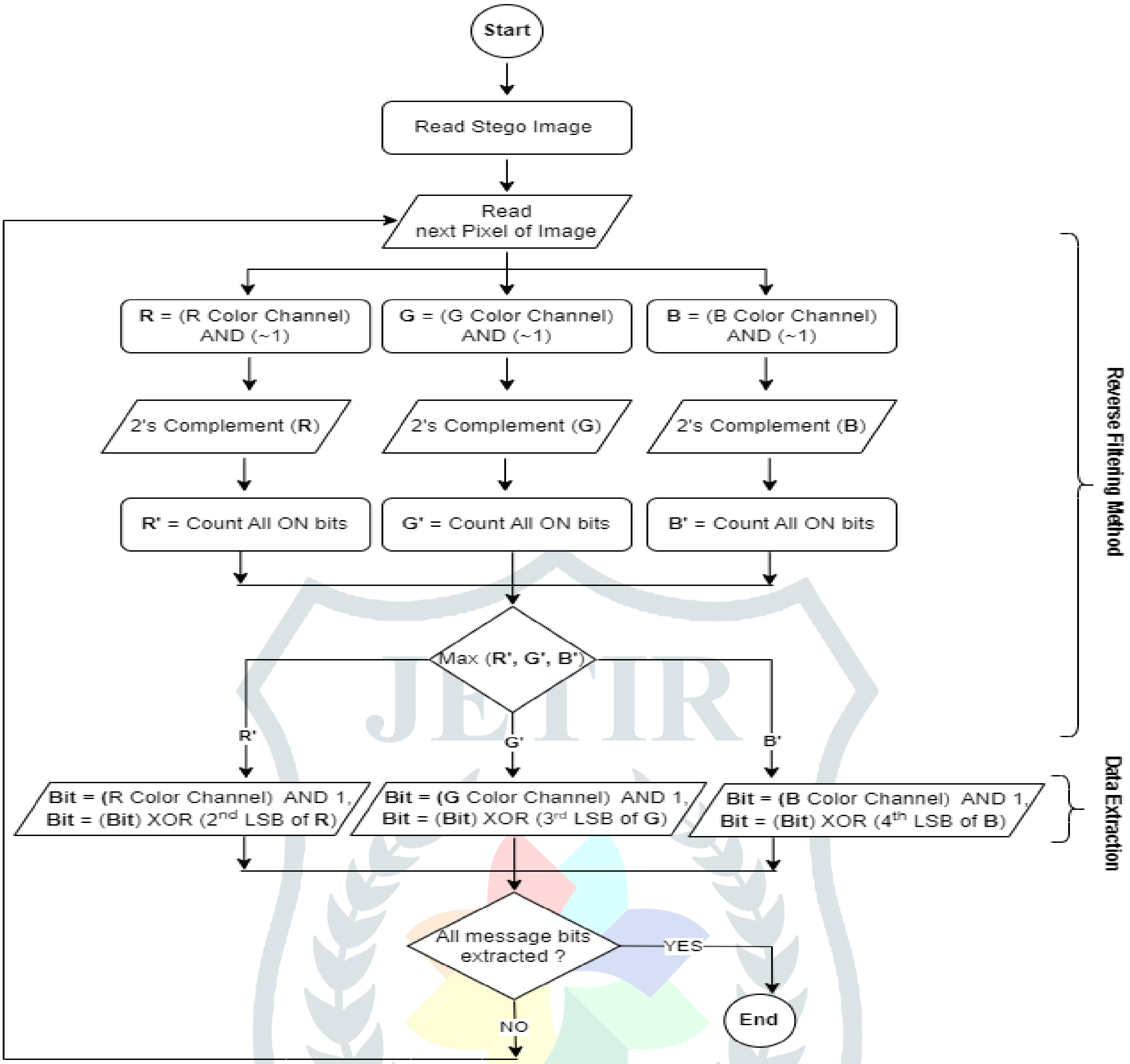

Start
Read Stego Image
Read next Pixel of Image
R = (R Color Channel) AND (~1)
G = (G Color Channel) AND (~1)
B = (B Color Channel) AND (~1)
2's Complement (R)
2's Complement (G)
2's Complement (B)
R' = Count All ON bits
G' = Count All ON bits
B' = Count All ON bits
Max (R', G', B')
R'
G'
B'
Bit = (R Color Channel) AND 1, Bit = (Bit) XOR (2nd LSB of R)
Bit = (G Color Channel) AND 1, Bit = (Bit) XOR (3rd LSB of G)
Bit = (B Color Channel) AND 1, Bit = (Bit) XOR (4th LSB of B)
All message bits extracted ?
YES
NO
End
Reverse Filtering Method
Data Extraction

Figure 6: Reverse Filtering method and Data extraction flowchart

Table 3: Reverse filtering method and Data extraction

Pixel No.	Modified Color Channel	Channel value	(3) AND ~1	2's Complement of (4)	ON bits Count of (5)	Color component of (2) related to Max of (5)	Value of color component of (7) using (3) AND 1	Extracted Message Bit: (8) XOR (2^{nd} / 3^{rd} / 4^{th} LSB of (4) of R / G/ B resp.) related to (7)
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(10)
1	R	11001010	11001010	00110110	4	G	0	0
	G	01100010	01100010	10011110	5			
	B	01011111	01011110	10100010	3			
2	R	11001001	11001000	00111000	3	B	1	0
	G	01100001	01100000	10100000	2			
	B	01011111	01011110	10100010	3			
3	R	11010000	11010000	00110000	2	B	1	1
	G	01101000	01101000	10011000	3			
	B	01100101	01100100	10011100	4			
4	R	11001100	11001100	00110100	3	G	1	0
	G	01100101	01100100	10011100	4			
	B	01100001	01100000	10100000	2			

IV. EXPERIMENTAL RESULT

In our experiment, we have used a 24-bit color image. So we have analysed five 24-bit color images, all having 512 * 512 dimensions. Our experimental result consists of evaluation metrics Peak Signal-to-Noise Ratio, Mean Square Error, and Histogram Analysis.

i. Mean Square Error (MSE)

It is one of the important evaluation metrics of image. It is defined as the average square difference between the original values of the image and values that are calculated after embedding message bits into the same image object. If MSE is less, then the quality of an image is high. The MSE between A(x,y) and B(x,y) images is,

$$MSE = \sum_{i=1}^{x} \sum_{j=1}^{y} \frac{(|A_{ij} - B_{ij}|{}^\wedge 2)}{x \times y}$$

ii. Peak Signal-to-Noise ratio (PSNR)

It is also an important measurement metric for images. PSNR measures image distortion. PSNR calculates the error size related to the signal maximum value. The high PSNR value indicates, less distortion present in the stego image. That means there is no such considerable difference between the original image and the stego image. The formulae of PSNR is

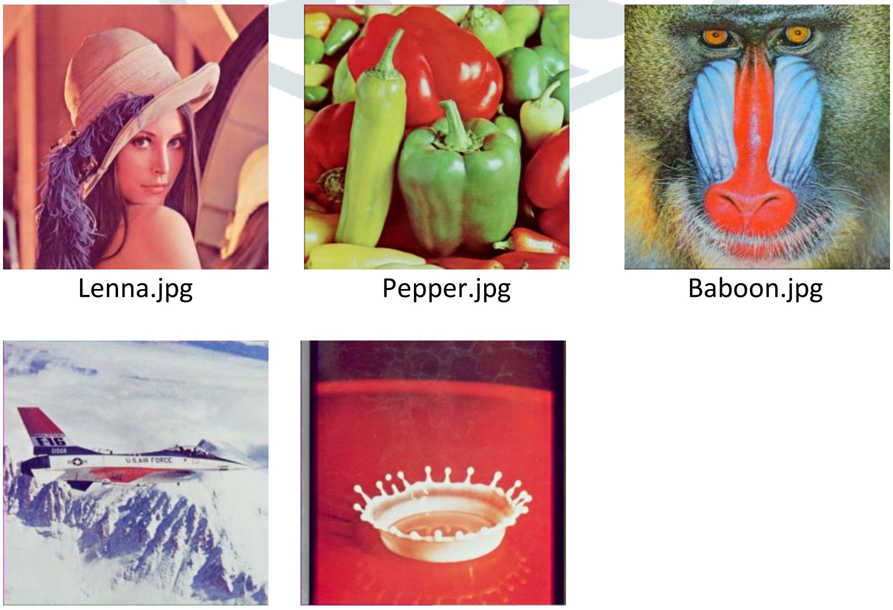
$$\mathrm{PSNR} = 10 \log_{10}\left(\frac{\mathrm{C}_{\mathrm{MAX}}^{2}}{\mathrm{MSE}}\right)$$

$$\mathrm{C}_{\mathrm{MAX}}^{2} \leq \left\{ \begin{array}{l} 1 \; \textit{in double precision intensity images} \\ 255 \; \textit{in 8-bit unsigned integer intensity images} \end{array} \right.$$

We have calculated values of PNSR and MSE during the experiment. Table 1 shows the PNSR and MSE values of all five images mentioned in Figure 7.

Table 1: PNSR and MSE values of different images

Dimension	Original image	Stego image	PSNR (in dB) for payload				MSE for payload			
			1 Kb	2 Kb	3 Kb	4 Kb	1 Kb	2 Kb	3 Kb	4 Kb
512 * 512	Lenna.jpg	Lenna.jpg	70.92	67.90	66.16	64.92	0.0075	0.0153	0.0230	0.0309
512 * 512	Pepper.jpg	Pepper.jpg	71.00	67.97	66.21	64.94	0.0078	0.0155	0.0231	0.0312
512 * 512	Baboon.jpg	Baboon.jpg	71.03	67.95	66.21	64.93	0.0077	0.0158	0.0235	0.0313
512 * 512	Airplane.jpg	Airplane.jpg	71.00	67.92	66.18	64.94	0.0075	0.0154	0.0231	0.0308
512 * 512	Splash.jpg	Splash.jpg	71.04	68.00	66.23	64.97	0.0075	0.0153	0.0229	0.0306



Lenna.jpg

Pepper.jpg

Baboon.jpg

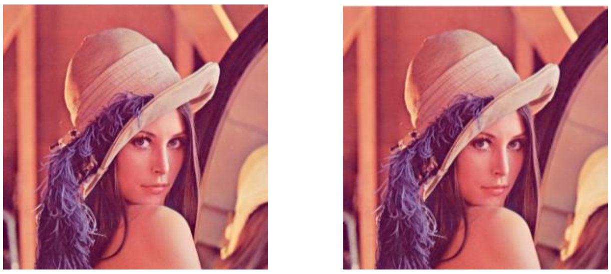
Airplane.jpg

Splash.jpg

Figure 7: Cover images

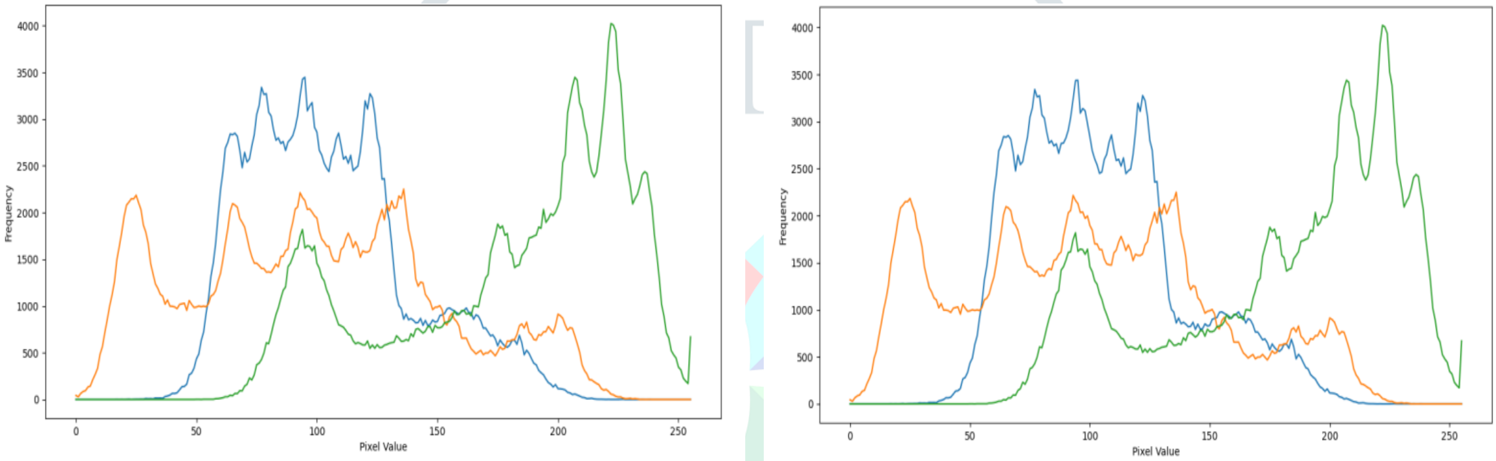
iii. Histogram Analysis

The proposed model was also evaluated based on Histogram analysis. We have given input as a 24-bit color image and also obtained its stego image. The obtained stego image is approximately similar to the original cover image which is shown in Figure 8. From Figure 9, there is quite a match between the histogram of the stego image and that of the cover image where the payload size is 1 Kb.



(a) (b)

Figure 8: (a) Cover Image and (b) Stego Image



(a) (b)

Figure 9: Histogram of Figure 8 of (a) Cover Image and (b) Stego Image

V. CONCLUSION

To strengthen the steganography process, we have designed a novel filtering-based modified LSB steganography method where one color channel out of three color channels of pixels is selected for embedding. Also, single-color channels of pixel filtered based on the proposed filtering technique. The main focus of this paper is not to embed large data in cover media, but to implement a robust and secure environment. Another level of security is implemented using AES. The proposed method provides a secure platform cause it produces high PSNR and low MSE.

VI. REFERENCES

[1] M. H. Rajyaguru, "CRYSTOGRAPHY-Combination of Cryptography and Steganography With Rapidly Changing Keys," *Int. J. Emerg. Technol. Adv. Eng.*, vol. 2, no. 10, pp. 329–332, 2012.

[2] M. Khalid, K. Arora, and N. Pal, "A Crypto-Steganography: A Survey," *Int. J. Adv. Comput. Sci. Appl.*, vol. 5, no. 7, pp. 149–155, 2014, doi: 10.14569/ijacsa.2014.050722.

[3] P. R. E. R. N. Benkar, "A Comparative Study of Steganography & Cryptography," *Int. J. Sci. Res.*, vol. 4, no. 7, pp. 670–672, 2015, [Online]. Available: https://www.ijsr.net/archive/v4i7/SUB156327.pdf.

[4] S. Almuhammadi and A. Al-Shaaby, "A Survey on Recent Approaches Combining Cryptography and Steganography," no. March, pp. 63–74, 2017, doi: 10.5121/csit.2017.70306.

[5] B. Kaliski, "A Survey of Encryption Standards," *IEEE Micro*, pp. 1–67, 1998, doi: 10.1007/978-3-642-58877-8_1.

[6] V. M. Wajgade, "Stegocrypto - A Review Of Steganography Techniques Using Cryptography," *Int. J. Comput. Sci. Eng. Technol.*, vol. 4, no. 04, pp. 423–426, 2013.

[7] M. Warkentin, M. B. Schmidt, and E. Bekkering, "Steganography and steganalysis," *Intellect. Prop. Prot. Multimed. Inf. Technol.*, no. January, pp. 374–380, 2007, doi: 10.4018/978-1-59904-762-1.ch019.

[8] G. C. Kessler and C. Hosmer, "An Overview of Steganography," *Adv. Comput.*, vol. 83, pp. 51–107, 2011, doi: 10.1016/B978-0-12-385510-7.00002-3.

[9] N. F. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen," *Computer (Long. Beach. Calif).*, vol. 31, no. 2, pp. 26–34, 1998, doi: 10.1109/MC.1998.4655281.

[10] S. K. Ghosal, "A New Pair Wise Bit Based Data Hiding Approach on 24 Bit Color Image using Steganographic Technique."

[11] K. Joshi and R. Yadav, "A new LSB-S image steganography method blend with Cryptography for secret communication," *Proc. 2015 3rd Int. Conf. Image Inf. Process. ICIIP 2015*, pp. 86–90, 2016, doi: 10.1109/ICIIP.2015.7414745.

[12] F. Deeba, S. Kun, F. A. Dharejo, and H. Memon, "Digital image watermarking based on ANN and least significant bit," *Inf. Secur. J.*, vol. 29, no. 1, pp. 30–39, 2020, doi: 10.1080/19393555.2020.1717684.

[13] M. R. Islam, T. R. Tanni, S. Parvin, M. J. Sultana, and A. Siddiqa, "A modified LSB image steganography method using filtering algorithm and stream of password," *Inf. Secur. J.*, vol. 30, no. 6, pp. 359–370, 2021, doi: 10.1080/19393555.2020.1854902.

[14] S. Sultana *et al.*, "A Modified Filtering Approach of LSB Image Steganography Using Stream Builder along with AES Encryption," *Recent Trends Inf. Technol. its Appl.*, vol. 1, no. 2, pp. 1–10, 2018.

[15] M. R. Islam, A. Siddiqa, M. P. Uddin, A. K. Mandal, and M. D. Hossain, "An efficient filtering based approach improving LSB image steganography using status bit along with AES cryptography," *2014 Int. Conf. Informatics, Electron. Vision, ICIEV 2014*, 2014, doi: 10.1109/ICIEV.2014.6850714.

[16] N. A. Al-Juaid, A. A. Gutub, and E. A. Khan, "Enhancing PC Data Security via Combining RSA Cryptography and Video Based Steganography," *J. Inf. Secur. Cybercrimes Res.*, 2018, doi: 10.26735/16587790.2018.006.

[17] M. Alotaibi, D. Al-hendi, B. Alroithy, M. AlGhamdi, and A. Gutub, "Secure Mobile Computing Authentication Utilizing Hash, Cryptography and Steganography Combination," *J. Inf. Secur. Cybercrimes Res.*, vol. 2, no. 1, 2019, doi: 10.26735/16587790.2019.001.

[18] and Y. C. Chaitra Rangaswamaiah, Yu Bai, "Multilevel Data Concealing Technique Using Steganography and Visual Cryptography," vol. 70, pp. 739–758, 2020, doi: 10.1007/978-3-030-12385-7.