Dual Layered Data Security Via Filter-based Modified 1-LSB Image Steganography and AES

[1]Sharad S. Hegade, [2]Dr. S. R. Pande

[1]Research Scholar, [2]Professor
Department of Computer Science
SSESA's Science College, Nagpur, India

***Abstract*- Nowadays, digital communication plays a vital role in human daily routine. Hence, we need to take care of communication as there exist hurdles. The growth rate of digital communication has increased exponentially and novel challenges rapidly change. So we need to protect and provide a secure platform for communication. There exist two different ways cryptography and steganography which will protect data. In cryptography, digital communication is converted into non-understandable cipher text, whereas data is hidden in the cover media in steganography. In our proposed system, we have implemented double-layer security using AES and filter-based modified 1-LSB steganography. In steganography, the candidate color channel of a pixel is selected for embedding using the proposed filtering algorithm. AES cryptography is applied to secret data before the steganography process. The proposed methodology is robust and secure as it generates high PSNR and low MSE.**

***Keywords*- Data security, Cryptography, Steganography, Filter-based method.**

I. INTRODUCTION

Through the internet, a huge amount of information is accessed by human beings every day. As the Internet is a public entity, anyone can access it. Nowadays speed of accessing data over the internet increasing rapidly and exponentially. So overflow of data and information is present on an insecure communication channel. Therefore, data and information need to be protected from unauthorized entities. Cryptography and steganography are such means that secure data and information[1]. In cryptography, meaningful secret messages get scrambled into non-understandable cipher text which is seen by the naked eye[2][3]. Whereas, steganography covers data behind the cover media which is unseen to humans with an open eye[2][3]. Cryptography and steganography break when the secret key is known and the existence of steganography is identified in cover media respectively[2][3]. Cryptography and steganography come with considerable advantages and limitations. To overcome limitations and utilize the advantages of both of them blended approach of a crypto-steganographic system was implemented[4].

Cryptography is the way of converting plain text into cipher text systematically and scientifically. It can be implemented with or without a secret key. Hence, cryptography is divided into Symmetric key cryptography, Asymmetric key cryptography, and Hash function cryptography. In symmetric key cryptography, to encrypt and decrypt the message same secret key is used[5][6]. Whereas in Asymmetric key cryptography, a public key is used for encryption, and a private key is used for decrypting the message[5][6]. It is useful to implement confidentiality, integrity, source authentication, and key management[6][7].

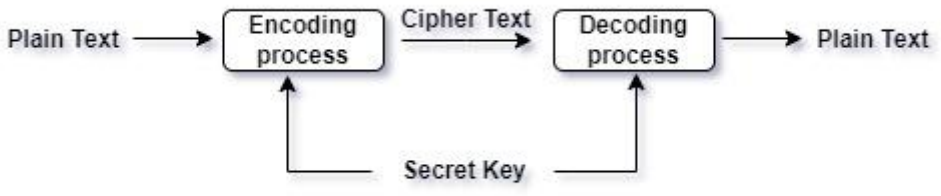


Figure 1: Cryptographic Model

Steganography is a technique in which secret data is covered in cover files such as images, audio, text, video, etc[5][8]. The existence of a secret message is not known to others except actual communicators. Steganography fails when the existence of a hidden message is identified by a third party[9].

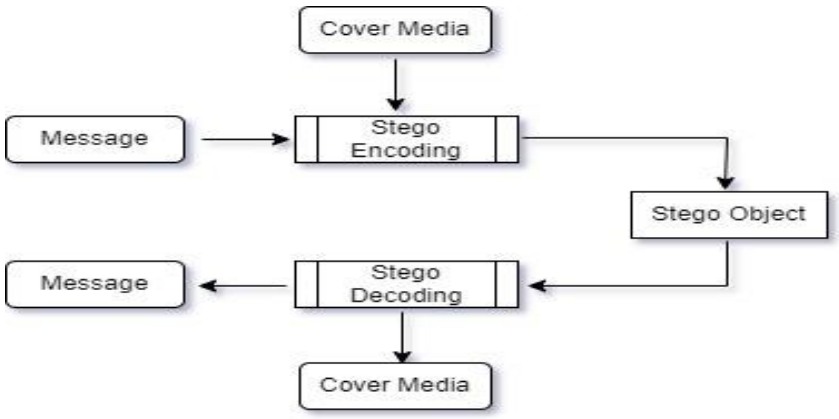


Figure 2: Steganographic Model

In our proposed system, the plain text is converted to cipher text using AES cryptography. The basic internal structure and working of AES cryptography are as below:

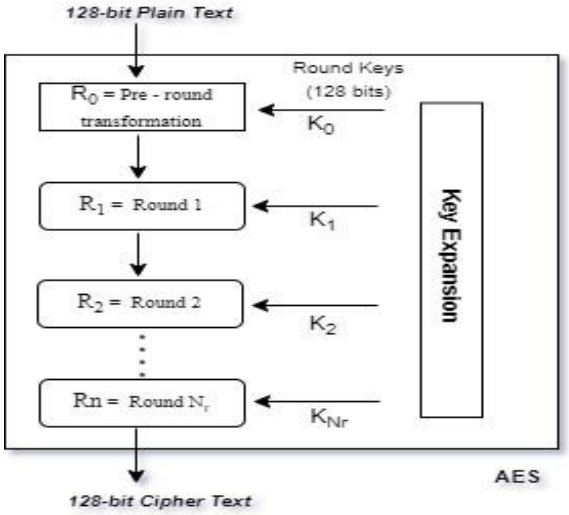


Table	
Key Size	*Number of Rounds*
128	10
192	12
256	14

Relationship between Secret Key Size and Number of Rounds

Figure 3: AES cryptography architecture

II. RELATED WORK

In the field of research, there exists a lot of research work on the crypto-steganography blending approach. This blending approach produces a more robust and secure platform as compared to systems with cryptography and steganography individually.

Authors at [10] implemented PC data security using RSA cryptography and 1,2,3-LSB steganography. In this combined security approach authors claimed that 3-LSB steganography is better than 1,2-LSB steganography.

The research at [11] proposes novel dual-layer security using cryptography and steganography. The cryptography was implemented using the Vernam cipher method and then the resultant cipher text was hidden behind the cover image using LSB with shifting (LSB-S).

In the paper [12], a multi-layer security mobile system was implemented using Hash, cryptography, and steganography. Hashing algorithms present in this system are Message Digest 5 (MD5), Secure Hash Algorithm 1 (SHA-1), SHA-256, SHA-384, and SHA-512. In the proposed first system, the password is digested using the mentioned hash algorithms then it is embedded in a cover image using LSB steganography. Whereas in the other method, the hash-digested password is encrypted using AES cryptography, then the result is hidden behind the cover image using LSB steganography.

In the system [13], using DES cryptography message is enciphered, and then a cipher message hides in a cover image using DCT steganography. This said the system was utilized for protecting PDF, document, excel, or PowerPoint.

The authors at [14] propose a new blending approach to security in which a secret message is enciphered using a QR code encoder, and then quantized bits of QR code embedded into an image using the LSB substitution method.

The Internet banking facility security is implemented at [15]. The sensitive information such as bank card details, location, time, and date is enciphered using AES, and then that data is embedded in an image using F5 steganography.

after receiving of created stego image at the server end, the server calculates the creation time of it. The server denies the transaction in case the difference between the stego image creation time and transaction time exceeds, otherwise validates the transaction. After successful validation, the server compares the current transaction amount with the previous spending average and also compares the current transaction location with previous transaction locations. If there exists a major difference between them, then bank takes care using whether to deny the transaction or verify the user identity using OTP or call method.

In [16], authors implemented double-layer security using AES and a modified LSB with stream builder filtering. AES used to encipher the data before embedding, whereas a modified LSB with stream builder filtering is used to find out locations to embed enciphered data.

The secure environment is implemented with Elliptic Curve Cryptography and LSB steganography [17]. Initially, secret messages were encrypted using Elliptic Curve Cryptography, then obtained cipher text embedded into grayscale images using LSB steganography. Then sender compresses the resultant stego file.

The authors at [18] delivered a crypto-steganographic model of security, in which AES cryptography was used for encryption and Bit matching steganography for data embedding. The proposed system provides an undistorted stego image and a high-capacity payload.

The proposed method at [19] proposes blending model of cryptography and steganography. to cipher the secret data they used 3DES cryptography and data embedding implemented using enhanced LSB steganography. The least dominant color channel of the color image image is used to embed the data.

III. RESEARCH METHODOLOGY

Our proposed blended crypto-steganography approach consists of two sub-sections the Data embedding process and the Data extraction process. In the steganographic process, we have utilized a 24-bit color image as cover media. A pixel is the smallest unit of an image whose length is 24-bit in a color image. The equal-sized Red, Green, and Blue are the three components of each pixel of an image. The filter-based modified LSB steganography is used for covering secret data in the cover image which is depicted below (A). Whereas, a 128-bit AES cryptographic algorithm is applied to a secret message before the steganographic process. The following algorithmic process of (A) Data embedding and (B) Data extraction is described below:

(A) Data embedding Process

A modified 1-LSB image steganography based on a filtering method is used to find out the candidate color channel of pixels of an image. The obtained candidate color channel of a pixel of an image is used for data embedding. Figure 4 and Table 1 describe the flowchart and illustration of the data embedding process respectively. The algorithmic process is depicted below:

(i) Read the cover image and secret message.
(ii) Apply 128-bit AES cryptography on a secret message results in cipher text.
(iii) Set R = 0, G = 0, and B = 0.
(iv) Read a pixel of an image
(v) **Filtering Method**
(a) Perform 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)
(b) Find out the maximum of calculated R’, G’, and B’ at step (v)(a)
(c) If R’ is maximum, perform R = R + 1
If G’ is maximum, perform G = G + 1
If B’ is maximum, perform B = B + 1
(d) Repeat the process from step iv), if all pixels of an image are not visited. Otherwise, switch to step (v)(e)
(e) Then find out the maximum between R, G, and B obtained at step (v)(c). The candidate channel is as follows
R is the maximum → candidate color channel of a pixel is R,
G is the maximum → candidate color channel of a pixel is G,
B is the maximum → candidate color channel of a pixel is B.
(f) Read the cover image again
(g) Read a pixel of an image
(h) Perform 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)
(i) Compare R’, G’, and B’ obtained at step (v)(h) and find out the maximum.
(vi) **Data Embedding**
(a) If R’ is maximum at step (v)(i) and R is the candidate color channel at step (v)(e), then perform R Channel = (Value of R Channel) OR (Bit),

If G' is maximum at step (v)(i) and G is the candidate color channel at step (v)(e), then perform G Channel = (Value of G Channel) OR (Bit),
If B' is maximum at step (v)(i) and B is the candidate color channel at step (v)(e), then perform B Channel = (Value of B Channel) OR (Bit).
Where Bit = Cipher text bit

(b) If not all bits of the secret message are embedded in a cover image then switch to step (v)(g). Otherwise, stop the process.

Table 1: Data Embedding Process Illustration

Pixel No.	**Color Channel**	**Channel value**	**(3) AND ~1**	**Max Value Color Channel of (4)**	**Color Channel as Flags of (5)**	**The final calculated value of each Color Channel of (6)**	**Max Value Color Channel of (7)**	**Message bits**	**Color component of (8) whose value at (4) is greater than others, then perform (value of that component) OR single bit of (9) at a time**
(1)	**(2)**	**(3)**	**(4)**	**(5)**	**(6)**	**(7)**	**(8)**	**(9)**	**(10)**
1	R	01100010	01100010	R	R = 1 (increment)	R = 1 G = 1 B = 2	B	"11"	01100010
	G	00000000	00000000		G = 0				00000000
	B	00011001	00011000		B = 0				00011000
2	R	01010101	01010100	B	R = 1				01010100
	G	00110111	00110110		G = 0				00110110
	B	01011001	01011000		B = 1 (increment)				01011001
3	R	01000011	01000010	B	R = 1				01000010
	G	00101000	00101000		G = 0				00101000
	B	01001011	01001010		B = 2 (increment)				01001011
4	R	10110011	10110010	G	R = 1				10110010
	G	11001001	11001000		G = 1 (increment)				11001000
	B	11000111	11000110		B = 2				11000110

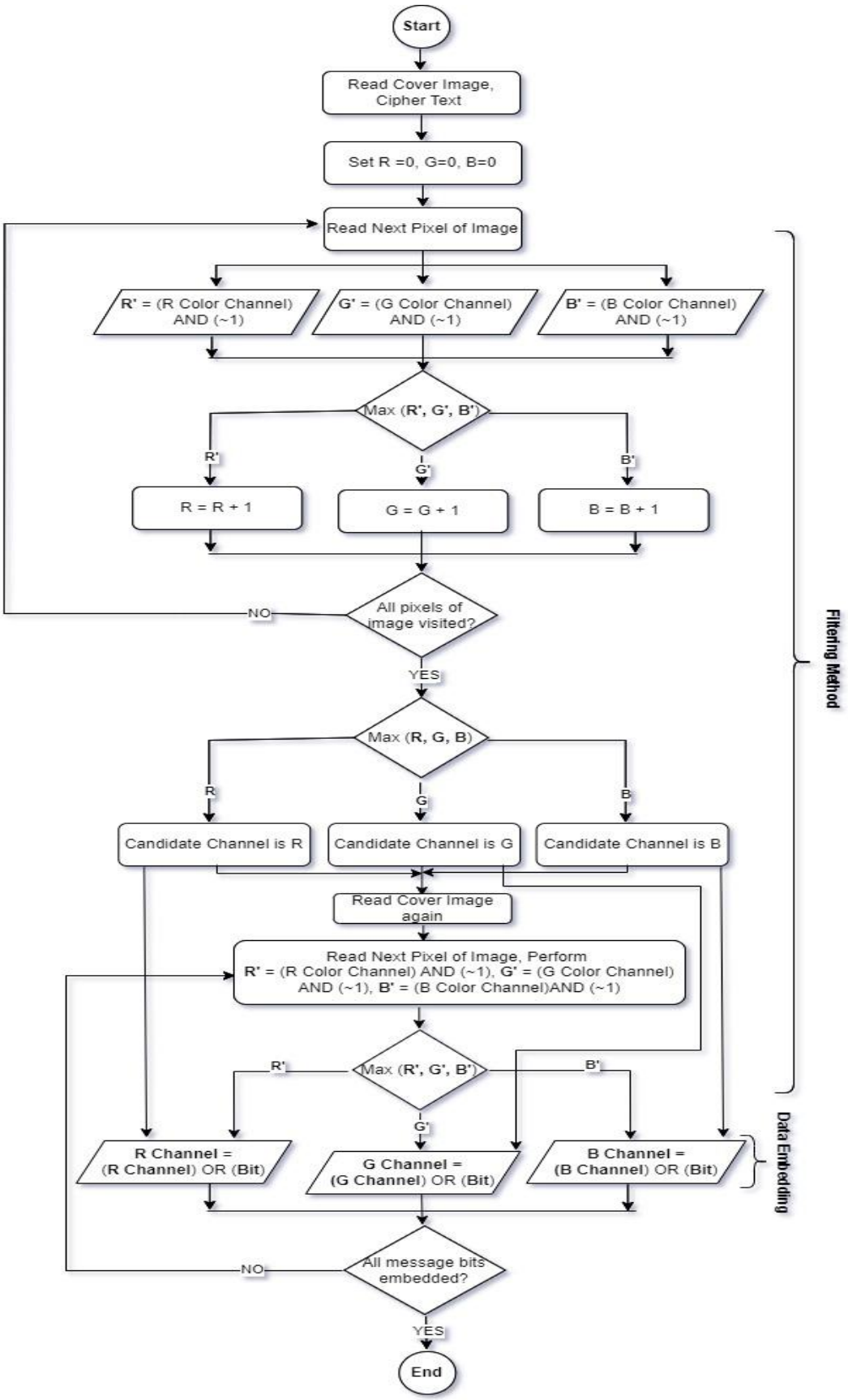


Figure 4: Data Embedding Process Flowchart

(B) Data extraction

The sender sends multi-layer secured data to the recipient. Figure 5 and Table 2 describe the flowchart and illustration of the data extraction process respectively. At the recipient end, the received stego image is converted into its original form by below mentioned algorithmic steps:

(i) Read the stego image.
(ii) Set R = 0, G = 0, and B = 0.
(iii) Read a pixel of the stego image
(iv) **Reverse Filtering Method**
(a) Perform 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)
(b) Find out the maximum of calculated R', G', and B' at step (iv)(a)
(c) If R' is maximum, perform R = R + 1
If G' is maximum, perform G = G + 1
If B' is maximum, perform B = B + 1
(d) Repeat the process from step iii), if all pixels of an image are not visited. Otherwise, switch to step (iv)(e)
(e) Then find out the maximum between R, G, and B obtained at step (iv)(c). The candidate channel is as follows
R is the maximum → candidate color channel of a pixel is R,
G is the maximum → candidate color channel of a pixel is G,
B is the maximum → candidate color channel of a pixel is B.
(f) Read the stego image again
(g) Read a pixel of an image
(h) Perform 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)
(i) Compare R', G', and B' obtained at step (iv)(h) and find out the maximum.
(v) **Data Extraction**
(a) If R' is maximum at step (iv)(i) and R is the candidate color channel at step (iv)(e), then perform Bit = (Value of R Channel) AND (1),
If G' is maximum at step (iv)(i) and G is the candidate color channel at step (iv)(e), then perform Bit = (Value of G Channel) AND (1),
If B' is maximum at step (iv)(i) and B is the candidate color channel at step (iv)(e), then perform Bit = (Value of B Channel) AND (1).
Where Bit = Extracted Bit
(b) If not all bits of the secret message are extracted from the stego image then switch to step (iv)(g). Otherwise, stop the process.

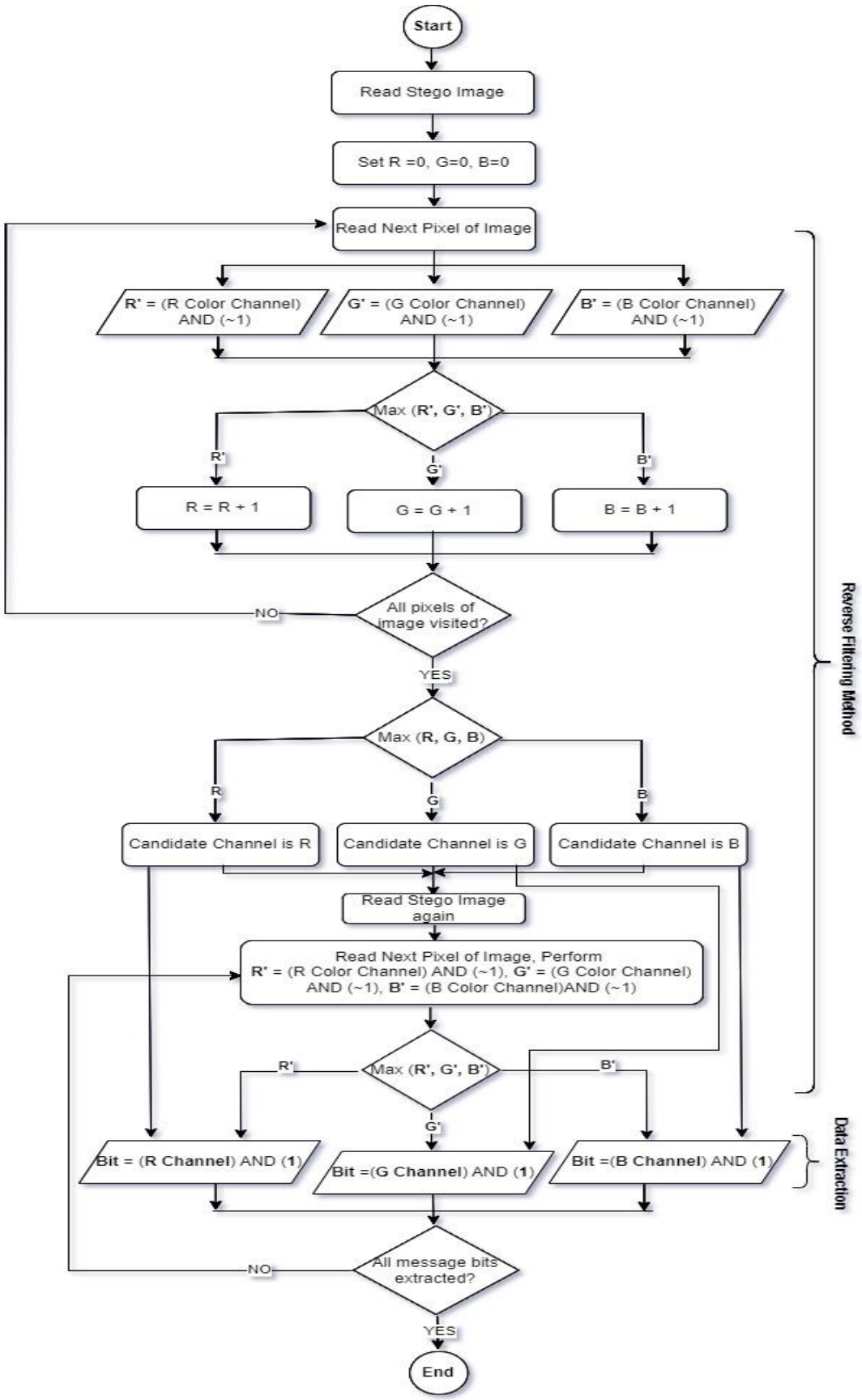


Figure 5: Data Extraction Process Flowchart

Table 2: Data Extraction Process Illustration

Pixel No.	Modified Color Channel	Modified Channel value	(3) AND ~1	Table 2: Color Channel of (8)	Data Extraction: Value of color channel (8) of each pixel at (4)	Extracted Message Bit using (6)

					is greater than others then perform ((value of that color channel at (3)) AND 1)	
(1)	**(2)**	**(3)**	**(4)**	**(5)**	**(6)**	**(7)**
1	R	01100010	01100010		01100010	
	G	00000000	00000000		00000000	
	B	00011000	00011000		00011000	
2	R	01010100	01010100		01010100	
	G	00110110	00110110		00110110	
	B	01011001	01011000	B	01011001	**"11"**
3	R	01000010	01000010		01000010	
	G	00101000	00101000		00101000	
	B	01001011	01001010		01001011	
4	R	10110010	10110010		10110010	
	G	11001000	11001000		11001000	
	B	11000110	11000110		11000110	

IV. EXPERIMENTAL RESULT

In our proposed methodology, we have used a 24-bit color image as a cover image to hide the secret message. The experimental result of our methodology is evaluated based on Peak Signal-to-Noise Ratio, Mean Square Error, and Histogram Analysis.

i. Mean Square Error (MSE)

Mean square error is one of the important evaluation metrics in steganography which is defined as the average square difference between the original values of the cover image and calculated values after data embedding into that cover image. the quality of the stego image is high, when MSE is low. The MSE between two images A(x,y) and B(x,y) is,

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

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

If the value of PSNR is high, then less distortion is present in the obtained stego image. Hence, PSNR is related to the measure of distortion of the image. PSNR is useful for calculating the error size related to the maximum value of a signal. The PSNR formula is

$$\text{PSNR} = 10 \log_{10}\left(\frac{C_{\text{MAX}}^2}{\text{MSE}}\right)$$

$$C_{\text{MAX}}^2 \leq \begin{cases} 1 \text{ in double precision intensity images} \\ 255 \text{ in 8-bit unsigned integer intensity images} \end{cases}$$

The following Table 3 shows the calculated values of PNSR and MSE in our experiment. The PNSR and MSE values are related to the five images mentioned in Figure 6.

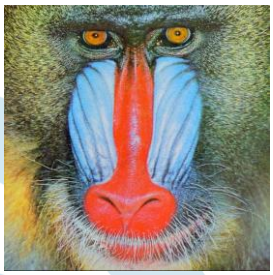
Table 3: PNSR and MSE values of different images

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	71.00	67.98	66.21	64.97	0.0077	0.0156	0.0233	0.0310

512 * 512	Pepper.jpg	Pepper.jpg	70.91	67.91	66.14	64.91	0.0078	0.0158	0.0236	0.0313
512 * 512	Baboon.jpg	Baboon.jpg	70.99	67.97	66.23	64.95	0.0076	0.0155	0.0230	0.0306
512 * 512	Airplane.jpg	Airplane.jpg	70.98	67.99	66.22	64.96	0.0077	0.0155	0.0230	0.0306
512 * 512	Splash.jpg	Splash.jpg	71.03	68.00	66.21	64.96	0.0077	0.0155	0.0233	0.0311


Lenna.jpg


Pepper.jpg


Baboon.jpg


Airplane.jpg

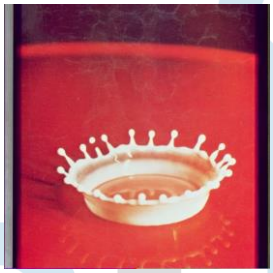
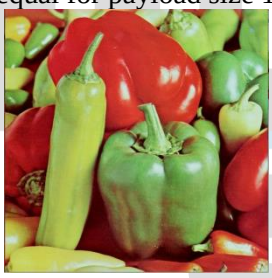

Splash.jpg

Figure 6: Cover images

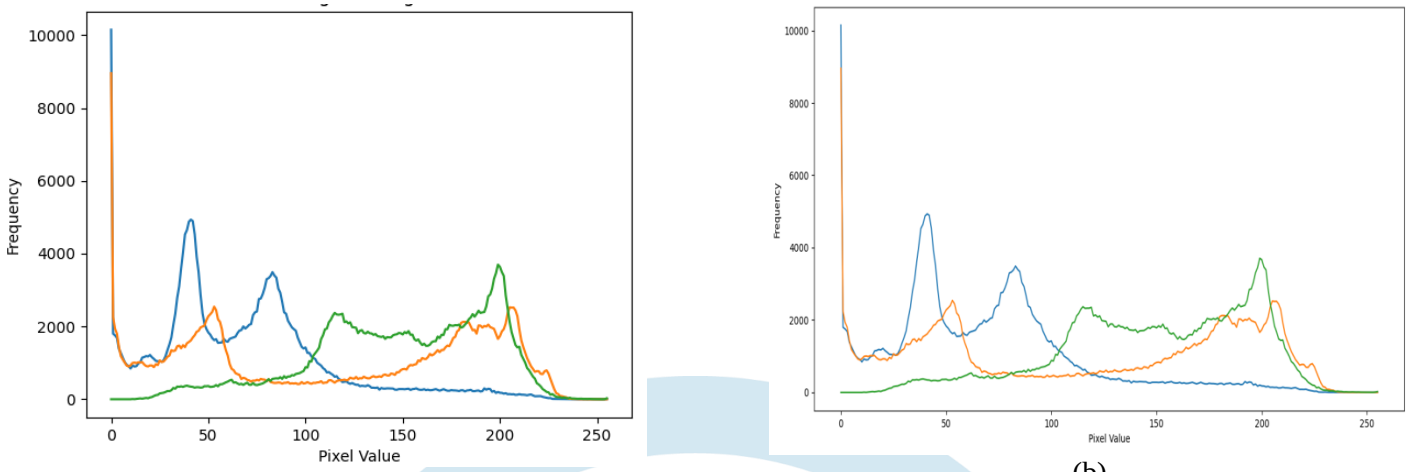
iii. Histogram Analysis

The cover image used in the steganographic approach in our experiment is of 24-bit color image. we have also evaluated our system based on a histogram of both the cover and the stego images. The cover image and obtained stego image are seen as similar to each other in Figure 7. Also in Figure 8, the histogram of the cover image and obtained stego image are quite equal for payload size 1 KB.


(a)


(b)

Figure 7: (a) Cover Image and (b) Stego Image



(a) (b)

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

V. CONCLUSION

The proposed system implements dual-layer security with AES and filter-based 1-LSB steganography. This system is robust and secure as it produces high PSNR, low MSE, and a quite similar histogram of the cover image and obtained stego image. There is a proportional relation between data payload and MSE, whereas data payload and PSNR are inversely proportional.

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] 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.

[3] 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.

[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] 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.

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

[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] 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.

[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] 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.

[13] A. Solichin and E. W. Ramadhan, "Enhancing data security using DES-based cryptography and DCT-based steganography," *Proceeding - 2017 3rd Int. Conf. Sci. Inf. Technol. Theory Appl. IT Educ. Ind. Soc. Big Data Era, ICSITech 2017*, vol. 2018-Janua, no. January, pp. 618–621, 2017, doi: 10.1109/ICSITech.2017.8257187.

[14] S. R. M. Mary and E. K.Rosemary, "Data Security Through Qr Code Encryption And Steganography," *Adv. Comput. An Int. J.*, vol. 7, no. 1/2, pp. 1–7, 2016, doi: 10.5121/acij.2016.7201.

[15] N. Devadiga, H. Kothari, H. Jain, and S. Sankhe, "E-Banking Security using Cryptography, Steganography and Data Mining," *Int. J. Comput. Appl.*, vol. 164, no. 9, pp. 26–30, 2017, doi: 10.5120/ijca2017913746.

[16] and E. J. K. Christy Atika Sari, Eko Hari Rachmawanto, "GOOD PERFORMANCE IMAGES ENCRYPTION

USING SELECTIVE BIT T-DES ON INVERTED LSB STEGANOGRAPHY," *J. a Sci. Inf.*, vol. 2, pp. 91–102, 2019.

[17] J. Bhadra, M. K. Banga, and M. Vinayaka Murthy, "Securing data using elliptic curve cryptography and least significant bit steganography," *Proc. 2017 Int. Conf. Smart Technol. Smart Nation, SmartTechCon 2017*, pp. 1460–1466, 2018, doi: 10.1109/SmartTechCon.2017.8358607.

[18] H. Antonio, P. W. C. Prasad, and A. Alsadoon, "Implementation of cryptography in steganography for enhanced security," *Multimed. Tools Appl.*, vol. 78, no. 23, pp. 32721–32734, 2019, doi: 10.1007/s11042-019-7559-7.

[19] N. Adam, M. Mashaly, and W. Alexan, "A 3DES Double-Layer Based Message Security Scheme," *2nd Int. Conf. Comput. Appl. Inf. Secur. ICCAIS 2019*, pp. 1–5, 2019, doi: 10.1109/CAIS.2019.8769457.