Hybrid Image Steganography Method with Random Embedding of Encrypted Message

Shanza Tariq[1], Ijaz Ali Shoukat[1], Umer Iqbal[1], Muhammad Rehan Faheem[2]

[1]Riphah College of Computing, Riphah International University Faisalabad Campus Pakistan

[2]Department of Computer Science, The Islamia University of Bahawalpur, Pakistan

Email: umeriqbal@riphahfsd.edu.pk

(*Received Date: Accepted Date: Issue Date:*)

ABSTRACT

The main challenge for embedding encrypted message in an input image is to get better the security of the confidential information through hybrid-based image steganography method. Moreover, earlier LSB based solutions existed in which either secret information embedded without encryption or embedded un-randomly in an image and existing MSB based information concealing solutions minimizes information capacity and image quality too. Most of existing steganographic systems either based on LSB or MSB but only some hybrid solutions are available in which either the confidential message is not encoded before embedding it into the image and the embedding system is also not random based. The existing well known hybrid based image steganography techniques are not only deficient in performance but also deficient in embedding of encoded data in an image. To overcome these issues, a Hybrid-LSB-MSB based image steganography and multi-operation data encryption method is proposed in this article. Proposed method is not only randomly embeds the confidential information in a cover image but also provided the facility to encode the confidential information before substituting. The Hybrid-LSB-MSB based proposed image steganography method is compared with earlier Hybrid based image steganography method by using Mean Squared Error (MSE) and Peak Signal to Noise Ratio (PSNR) values including payload capacity. Higher PSNR and Lower MSE values signify effective steganography quality. The experimental results show that proposed method retains higher PSNR and lesser MSE values as contrasted to the existing methods thereby effective in steganographic properties.

KEYWORDS: Data encryption, Image Steganography, Data Decryption, LSB, MSB, PSNR, MSE, NK, AD, SC, LMSE, NAE.

1. INTRODUCTION

With the improvement of the internet technology, cybercrimes are the most severe threats in transferring the secret data over insecure network. Attempts are made to decrease the number of cybercrime is to discover innovative systems for securing information [1]. Secure transmission of secret information is being fundamental for all sorts of systems to keep it from undesirable exposure and alterations during transmission [1]. For the best security of the secret data, combine use of steganography and cryptography is very useful [1] [2]. The most important goal of the image steganography can be planned as robustness, capacity and imperceptibility. Steganography is a scheme in which confidential data is concealed in any cover media and cryptography is used to convert secret data into meaningless form [3] [4]. Every of them have a drawback to provide data security alone. The downside of the cryptography is that figure content looks trivial, so attackers can sever the correspondence or make increasingly cautious keeps an eye on the data from the sender to the recipient [5]. The disadvantage of the Steganography is that when the event of disguised data is uncovered or even supposed, the information is gotten identified. By joining these two strategies we can take care of the above both issues. As far as we could possibly know, in the writing of advanced steganography, the picture is the very famous mean owing to having a high recurrence of excess information and ready to hide the mystery information inside mutually with imperceptible impacts [6][7].

By and large, programmers identify about LSBs and consumed it for the extraction of the mystery message so the utilization of MSB in this methodology makes it significantly extra secure [8]. The foremost improvement of image steganography is that when the private information is stored along the suitable method, the existence of the private information is tough to be aware of and it permits the opportunity of inserting excess private information [9].

The main disadvantage of the traditional LSB based steganography technique is that it is easily cracked by unauthorized users [37].

The only use of traditional MSB based steganography techniques is minimize the secret data hiding capacity and also affects the quality of

image. That's why a hybrid steganographic approach has been anticipated in this research which combines the LSB and MSB based methods to overcome both discrepancies of LSB and MSB based methods.

Researchers have been introduced some LSB based methods in [4] [5] [10] [11] [12] [13] [14] [15] [16] [17] [18] [19] [20] but the LSB based image steganography strategies have not acquired much security on the grounds that the small changes in a picture effectively recognized and this turns out to be progressively basic if the message was implanted in that picture without encryption that is the significant disadvantage of this strategy [21].

The key negative aspect of the LSB technique is that if the attacker extracts the full LSB bits, he can acquire the entire data as the data is concealed in the LSB bits [20].

Furthermore, in [6] [22] researchers have been suggested some MSB based methods but MSB based information covering up limited information and picture quality as well [23].

All these techniques have a few inconsistencies, for example, hardly any strategies inserted the mystery information without encryption and some existed strategies consecutively installed the mystery information. Various solutions exists that just use the LSB based substitution technique to substitute the confidential information and some methods just used the MSB based substitution technique for inserting purpose.

Thus to overcome the all discrepancies of the existed methods, this study utilizing the conception of proposed randomized Hybrid-LSB-MSB based substitution technique due to its novelty and Hill cipher with XOR operation to get better the security of the private data than earlier hybrid image steganography method. In addition, the proposed method is dissimilar with entire existing LSB based image steganography methods in terms of randomized Hybrid-LSB-MSB based substitution technique having high security.

The major improvement of this proposed technique is that it provides significant security of the private data than existed hybrid based image steganography method and it permits the users to convey a lot of information without any coverage.

The rest of this paper is planned as follows: the detailed discussion regarding the literature review and the comparison of proposed method with existed method has been discussed in section 2 and the section 3 has been elaborated the design and working flowcharts of proposed method. However, several experimental outcomes have been comprised in section 4, to verify the validity of the proposed technique. To end with section 5 that bring to a close the discussion through future work.

2. RELATED WORK

A variety of image steganography systems have been existed in which some are LSB based, some are MSB based and few are hybrid based solutions but the most important problem with existed methods was the lower security level of the secret data. An algorithm has been suggested in [9], in which a simple LSB inserting approach is make use of to insert the confidential data into the info picture and a confidential key is additionally utilized for more security purpose [9]. However in this proposed technique, confidential information isn't inserted irregularly and utilized a LSB technique rather than a hybrid-LSB-MSB strategy. The mainly significant disadvantage of just utilizing the LSB based implanting strategy is that LSB based image steganography techniques are for the most part used to move the secret information through an uncertain system [36] that is the reason invaders primarily interfere with the LSB's of the information picture to accomplish the private message [24]. What's more, a calculated guide is additionally utilized right now creates the arbitrary numbers to encode the secret information. The calculated guide has numerous disadvantages, for example, lopsided thickness chances misappropriation [25], slight key space and less protection [26] [27].

Researchers have been presented a method [11] that used Codeword, CRC-32 checksum, Gzip, AES, Fisher-Yates Shuffle strategy and abused the picked pixel of the divergent LSB of whole color channels with high time. AES have various negative aspects, for example, require the extra processing power, on the off chance that the data square size is relatively huge, at that point utilizes further assets and when expands the key size then the encoded time also increases [21]. Hybrid substitution technique for LSB and MSB is likewise not utilized in this method that enhances the security of confidential information. This strategy simply utilized the LSB to substitute the confidential information. LSB based image steganography techniques are much of the time utilized to move confidential information over an uncertain system [36] that is the main cause attacker right off the bat invasion the LSB's of the picture that is the significant disadvantage of LSB based image steganography strategies [24]. Since of the utilization of different strategies require a lot of time for preparing to transfer the secret information safely.

In [13], a sequential technique is utilized for steganography rather than irregular based

substituting strategy. LSB based image steganography techniques are regularly utilized to move confidential information over an uncertain system [36] that is very important reason intruders right off bat invasion the LSB's of the picture that is the significant disadvantage of LSB based image steganography strategies [24]. For the purpose of cryptography, Symmetric XOR technique is utilized. Information is substitute un-arbitrarily and with restricted implanted limit. The hybrid strategy for LSB and MSB is moreover not exploit right now that increases the protection of the private information.

Analysts have been presented a novel steganographic algorithm in [15] that utilized advanced mark and cryptography for encryption. With the end goal of the information camouflage LSB based strategy is utilized with Limited inserted limit. LSB based image steganography techniques are much of the time used to move secret information over an uncertain system that is the reason assailants right off the bat assault the LSB's of the picture [36]that is the significant disadvantage of LSB based image steganography strategies [24]. The hybrid system for LSB and MSB is moreover not exploited right now that gives the best security. Secret information is consecutively installed right now of irregularly embedded.

A novel algorithm has been presented in [17] that used 2D Arnold Cat Map for encoded reason and essential LSB technique is utilized to disguise the private information inside the info picture. LSB based image steganography systems are not safe on the basis that these are generally utilized strategies in steganography for sending confidential information [36]that is the reason attackers for the most part assault LSB's of the information picture [24]. Hybrid-LSB-MSB implanted system isn't making use of right now get better the security of confidential message. Confidential information isn't implanted arbitrarily into the cover image that is the reason security level isn't greatly improved. An algorithm has been introduced in [19] that pre-owned Rotor Caesar cipher to encode the confidential information and 2 piece LSB substitution techniques is utilized to insert the scrambled information in an information picture. Right now, LSB-MSB implanted technique isn't utilized that enhance the safety of the private information. The most renowned weakness of merely utilizing the LSB based installed technique is that LSB based image steganography strategies are not safe in light of the fact that these are generally utilized strategies in steganography for moving secret information [36] that is very important cause assailants for the most part invasion the LSB's of information image [24]. Secret information is successively implanted not irregularly into the information picture that is the reason security level is likewise not critical.

In [20] secret information is scrambled by utilizing an encoded strategy name as Vernam figure. Vernam figure has numerous disadvantages, for example, prerequisite, dissemination, and capacity of the limitless quantity of enormous keys for encoding however these huge keys can be handily followed when irregular number arrangement is identified [28]. An epic image steganography technique is utilized to insert the encoded data in an info picture and among imperfect substituting limit. LSB based image steganography strategies are every now and again used to move secret information over an unreliable system that is very important because assailants right off bat invasion the LSB's of the picture [36] that is the significant downside of LSB based image steganography techniques [24]. The hybrid strategy for LSB and MSB is furthermore not exploited right now. Secret data isn't irregularly substituted into the information picture that' why it isn't given the critical security to move the confidential information safely over an unsafe system.

In [6], pixel value indicator strategy is utilized for the covering of the confidential information in MSBs of the cover picture. MSB based image steganography techniques are reduced in excellence and the capacity of payload. Right now, data isn't encrypted before implanted it in a picture that is the reason it has insignificant safety intensity. The hybrid strategy for LSB and MSB is likewise not make use of right now increase the protection intensity to shift the private data safely through an unreliable method.

In [22], a Pixel Value Indicator and MSB substituting is utilized for parting the color picture in Blue, Red and Green channels. MSB based substituted technique limits the capacity of payload and picture excellence that is the significant disadvantage of simply utilizing the MSB to implant the private information. Private information isn't scrambled before implanting it in picture right now not furnishes the much protection and with insufficient implanted limit. The hybrid technique for LSB and MSB is likewise not make use of right now get better the protection of the confidential information.

Researchers have been suggested a hybrid based algorithm in [23]. In this wok, LSB technique joined with MSB were utilized for the camouflage of the secret information yet right now encryption isn't made before inserted the confidential information. Confidential information is substituted consecutively not arbitrarily. The security level is

not significant due to the consecutively embedding of confidential data in a cover image. The PSNR, capacity of the payload and MSE estimations of the proposed technique are additionally not noteworthy.

In this existed work [29], a comparison has been discussed among the plain hybrid and customized hybrid in a color picture. This plain hybrid method transfers the confidential audio data in the fluctuation of Least Significant Bit and Most Significant Bit of the info picture. The inserting altered hybrid relies upon the estimation of confidential audio in the LSB or MSB. In both techniques, confidential information is consecutively substituted and not scrambled before inserted into the cover picture. Audio information is utilized as confidential information rather than the textual informational set. The simple hybrid technique isn't giving huge security on the grounds that the PSNR and MSE esteems are not noteworthy.

In [30] MSB is used for encryption purpose and LSB bits are utilized for embedding the encrypted information in this work. XOR operation was performed among Most Significant Bit of the input picture pixels and bits of secret information, after that the result implanted in the LSB of the unique image. In this system, the audio file is securely transferred from one place to another place instead of textual information and Most Significant Bit of the info picture is utilized to encrypt the confidential information instead of embedding purpose. The confidential information is not inserted randomly into the cover image in this method.

In [24] an efficient algorithm has been presented, in which a differencing on fifth and sixth bits technique is utilized. Right now, MSB of cover image is utilized for substituting the confidential information successively. Yet, MSB based image steganography strategies limits the information capacity and picture excellence. Confidential information is implanted into the information picture without encryption and simply utilized the MSB inserting strategy rather than a hybrid LSB-MSB technique in this system. This technique is likewise very little secure because of the successively embedding procedure of secret information.

In [1], Hill cipher is utilized with Morse code to encode the confidential information before implanted into the information picture. Yet, the key's length and length of the confidential information must be similar at the encoded era that is the primary disadvantage of using this type of hill cipher. A simple LSB strategy is utilized to substitute the confidential information into the info picture instead of a hybrid LSB-MSB technique and confidential information isn't implanted irregularly in this technique, the security level isn't acceptable. The primary disadvantage of simply utilizing the LSB's of the information picture is that for the most part [36], intruders mistreat the LSB's of the cover picture in the light of the information that the LSB based image steganography systems are often utilized to move the secretive information from dispatcher to recipient over an uncertain system [24].

Consequently, the most advantageous image steganography solution demands both parameters such as significant security and payload capacity. Thus, this study proposed an innovative hybrid algorithm named as Hybrid image steganography method with random embedding of encrypted data for arbitrarily concealing the confidential information in a picture to provide the security of the private data over an unsafe network. In this solution, the security of confidential message is get better by encrypting the secretive message and randomly embedding into the cover picture utilizing hybrid LSB-MSB based inserted technique to stay away from middle man assaults. PSNR and MSE estimations of the proposed calculation are contrasted and earlier Hybrid LSB-MSB based image steganography calculation that demonstrates the better of the proposed calculation than an existed calculation.

Table 1. Comparison of Hybrid, MSB and LSB based image steganography methods with proposed method

Existed methods	Is LSB based method?	Is MSB based method?	Is information encoded before concealing?	Is information substituted arbitrarily?	Side-channel attacks are tackled?	Which Data sets?	Is the Hybrid method?
Ref [1]	✓	×	✓	×	×	Textual data	×
Ref [2]	✓	×	✓	✓	×	Textual data	×

Ref [4]	✓	×	✓	✓	×	Textual data	×
Ref [5]	✓	×	×	✓	×	Textual data	×
Ref [6]	×	✓	×	✓	×	Textual data	×
Ref [8]	×	×	×	×	×	Files	✓
Ref [9]	✓	×	✓	×	×	Textual data	×
Ref [11]	✓	×	✓	✓	×	Textual data	×
Ref [12]	✓	×	✓	✓	×	Textual data	×
Ref [13]	✓	×	✓	×	×	Textual data	×
Ref [14]	✓	×	×	✓	×	Textual data	×
Ref [15]	✓	×	✓	×	×	Textual data	×
Ref [16]	✓	×	×	✓	×	Textual data	×
Ref [17]	✓	×	✓	×	×	Textual data	×
Ref [18]	✓	×	✓	✓	×	Textual data	×
Ref [19]	✓	×	✓	×	×	Textual data	×
Ref [20]	✓	×	✓	×	×	Textual data	×
Ref [22]	×	✓	×	✓	×	Textual data	×
Ref [23]	×	×	×	×	×	Textual data	✓
Ref [24]	×	✓	×	×	×	Textual data	×
Ref [29]	×	×	×	×	×	Audio data	✓
Ref [30]	✓	×	✓	×	×	Audio data	×
Ref [31]	✓	×	✓	✓	×	Textual data	×
Proposed method	×	×	✓	✓	✓	Textual data	✓

In Table 1 discussed the comparative analysis of some existing Hybrid-LSB-MSB based, some LSB based and some MSB based image steganography methods. Many discrepancies have still existed in all of these existed methods such as some methods embedded the secret data without encryption, some methods embedded the secret data sequentially and some methods were used just LSB based substitution technique or MSB substitution technique. Some methods also exist that used the hybrid approach of the LSB and MSB substitution technique but embedded the secret data without encryption. And the payload capacity, PSNR and MSE values of these existed methods are also not significant. But the proposed method will overcome all these problems of existed methods. That's why the proposed method is extra secured than earlier hybrid based, LSB based and MSB based image steganography algorithms. Generally, it can be said that the proposed algorithm have

acquired higher PSNR values and less MSE values than existed hybrid based method which depicted that the proposed algorithm has improved the payload and security of steganography system.

3. PROPOSED METHOD

An effective image steganographic algorithm is developed by consuming the concept of Hybrid-LSB-MSB based substitution technique with arbitrary embedding and combined with steganography. This algorithm is developed to resolve the issues in image steganography and also detailed the working methodology to present the technical and logical explanations of the results. The step by step working methodology of the proposed algorithm is detailed in Figure 3.1 for embedding stage.

Moreover, middle men attacks cannot crack the stego image, as a result, it helps the solution to embed and extract the secret data with high payload capacity.

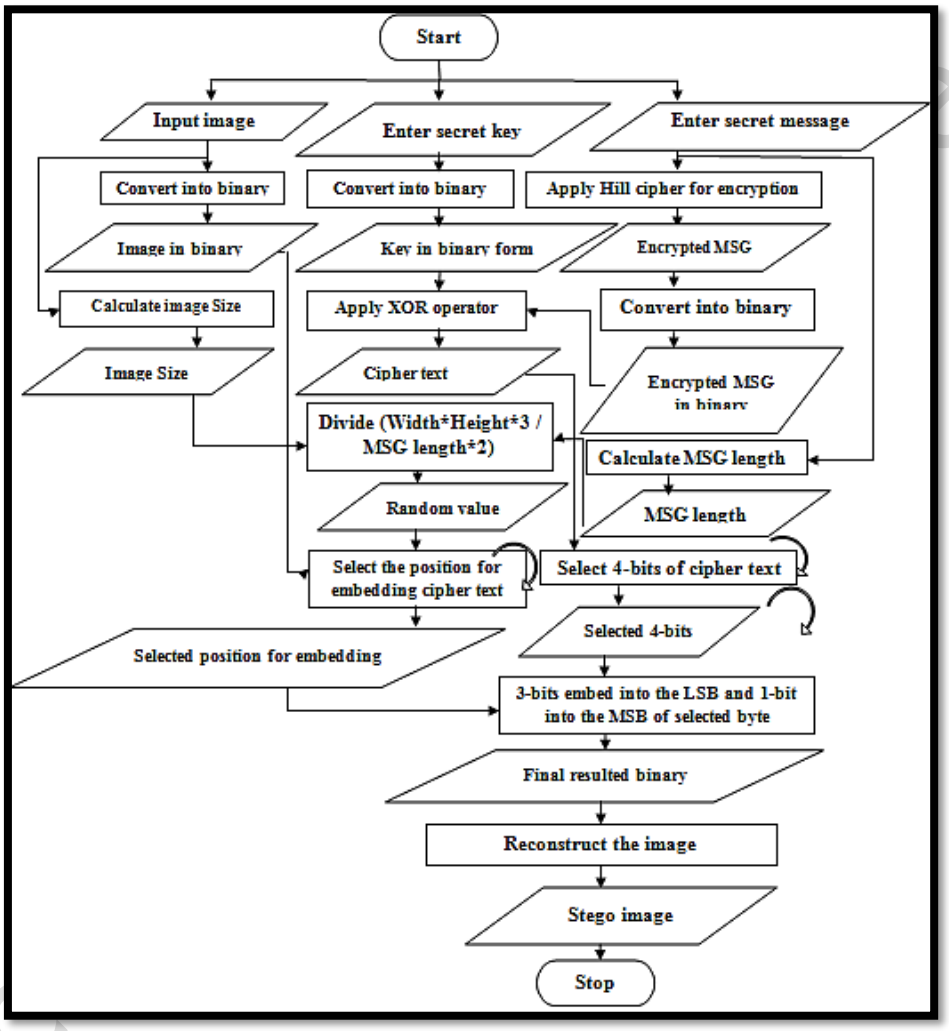


Figure 1: Working Flowchart for Proposed Method: Embedding Side

The overall working flow of proposed hybrid image steganography method of sender side as depict in Figure 1 includes the following steps.

Step1: In very first step, the proposed algorithm takes three inputs which include secret key and secret message to hide in a given input image.

Step2: In the second step, apply the Hill cipher encryption algorithm on the secret message that will increase the security of the secret message and converts this secret message into the encrypted message (cipher text).

Step3: In third step, the proposed algorithm converts the encrypted message and secret key into binary form.

Step4: In the fourth step, apply the Symmetric XOR operator between the binary of the encrypted message and secret key.

Step5: At the fifth step, the proposed algorithm gets a new resulted cipher text in binary form from step4 and store in a separate variable that will be later use for embedding purpose into the input image.

Step6: In the sixth step, get the size of the input image by multiplied the width and height and further multiplied by 3 that value will be later use as a dividend to calculate the random position value.

Step7: At the seventh step, multiply the total length of the secret message by 2 and a new value that will be later use as a divisor to calculate the random position value.

Step8: In the eight step, the proposed algorithm calculate the random position value by divided the achieved dividend value from step6 with the achieved divisor value from step7.

Step9: In the ninth step, finally the proposed algorithm achieve a random position value that will be used to randomly embed the encrypted message into the input image and this random position value store in a saperate variable for later use.

Step10: In tenth step, converts the input image image into binary form.

Step11: In the eleventh step, the proposed algorithm apply the Hybrid-LSB-MSB based method in which 1-MSB is embedded by bit differencing method and 3-LSb's are embedded by simply embedded method in a random position of the input image using random position value that was achieved from step9.

Step12: At the twelvth step, Repeat step11 untill the secret encrypted message is not fully randomly embedded into the image.

Step13: In thirteenth step, the proposed algorithm converts the final resultant binary of the input image into a stego image after embedding process.

Step14: In the last fourteenth step, finally the proposed algorithm achieve a stego image that has secret encrypted data.

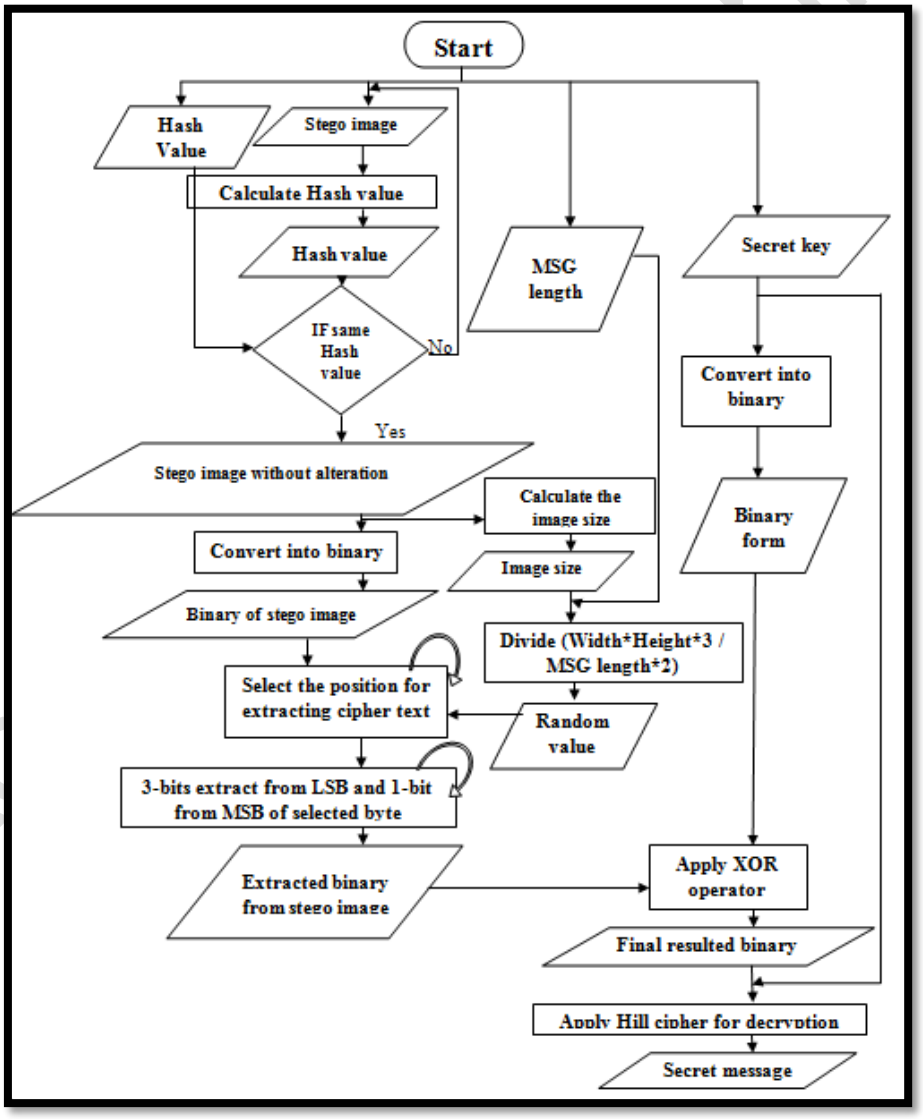


Figure 2: Working Flowchart for Proposed Method: Extraction Side

The overall working flow of proposed hybrid image steganography method of receiver side as depict in Figure 2 includes the following steps.

Step1: In very first step, the proposed algorithm takes four inputs which include stego image, secret key, total length of secret message and hash value of the sending stego image that will check any type of alteration in stego image.

Step2: In the second step, proposed algorithm calculates the hash value of the received stego image and match with the input hash value. If both hash value will same then further steps will be processed otherwise algorithm generate a message of alteration in stego image.

Step3: In the third step, if the both hash value same then the proposed algorithm convert the stego image into binary form.

Step4: In the fourth step, calculate the size of the stego image by multiplied the width and height and further multiplied by 3 that value will be later use as a dividend to calculate the random position value.

Step5: In the fifth step, multiply the total length of the secret message by 2 (achieved from step1) and get a new value that will be later use as a divisor to calculate the random position value.

Step6: At the sixth step, calculate the random position value by divided the achieved dividend value from step4 with the achieved divisor value from step5.

Step7: In the seventh step, finally the proposed algorithm achieve a random position value that will be used to randomly extract the encrypted message from the stego image and this random position value store in a saperate variable for later use.

Step8: In eight step, apply the Hybrid-LSB-MSB based method in which 1-MSB is extracted by bit differencing method and 3-LSb's are extracted by simply extraction method in a random position of the stego image using random position value that was achieved from step7.

Step9: In the ninth step, repeat step8 until secret message is not fully extracted from the binary of the stego image.

Step10: At the tenth step, proposed algorithm achieve the extracted binary from step9.

Step11: In the eleventh step, the proposed algorithm convert the secret key (that achieved from step1) into binary form.

Step12: In twelvth step, apply the symmetric XOR opertor between the extracted binary from step9 and binary of the secret key.

Step13: In thirteenth step, the proposed algorithm get a new resulted encrypted binary from step12 after XOR operator.

Step14: In the fourteenth step, apply Hill cipher on the new resulted encrypted binary that achieved from step13 for decryption purpose.

Step15: In fifteenth step, finally the proposed algorithm get a secret message that was hide into the stego image.

4. RESULT ANALYSIS

This section is concluded the experimental outcomes of proposed algorithm are compared along earlier Hybrid-LSB-MSB based algorithm by considering these statistical parameters such as MSE and PSNR values. Up to this point, for the improved picture quality, MSE worth ought to be lesser and the PSNR worth ought to be higher. The imitation outcomes are demonstrated utilizing dissimilar sizes of normal digital images of 560 × 448, 5040 × 4032, 750 × 1125 and 6750 × 10125 pixels with dissimilar types such as PNG and JPG. The outcomes of PSNR and MSE for dissimilar size of images are presented in Table 2 and Table 3 as well as graphically shown in Fig. 5 and Fig. 6. Regarding entire other metric esteems such as Normalized Cross-Correlation (NK), Average Difference (AD), Structural Content (SC), Laplacian Mean Square Error (LMSE) and Normalized Absolute Error (NAE) shows that the proposed algorithm has performed significant than others.

4.1. Normalized Cross-Correlation

The NK means the Normalized Cross-Correlation. It is also the performance investigation parameter. The common utilized NK formula (1) is specified as beneath [5].

$$\text{NK} = \sum_{j=1}^{M} \sum_{k=1}^{N} Xj,k.X'j,k \sum_{j=1}^{M} \sum_{k=1}^{N} X_{j,k^2} \quad (1)$$

4.2. Mean Squared Error

The MSE is the very significant and well-known performance investigation parameter that calculating the growing squared mistakes among the cover picture and info picture. The common utilized MSE condition (2) is specified as beneath [23].

$$\text{MSE} = \frac{\sum M,N[I1(M,N) - I2(M,N)]^2}{M*N} \quad (2)$$

The amount of columns and rows of the cover pictures are such as N and M corresponding [23].

4.3. Average Difference

The AD stands for the Average Difference. AD is also the most popular performance investigation

parameter. The familiar utilized AD formula (3) is specified as under [5].

$$AD = \sum_{j=1}^{M} \sum_{k=1}^{N} (Xj,k - X'j,k)/MN \quad (3)$$

4.3. Structural Content

The full form of SC is Structural content. It is also the quality analysis parameter. The general utilized SC formula (4) is given below [5].

$$SC = \sum_{j=1}^{M} \sum_{k=1}^{N} X^2 j,k / \sum_{j=1}^{M} \sum_{k=1}^{N} X'^2 j,k \quad (4)$$

4.4. Laplacian Mean Square Error

The LMSE stands for the Laplacian Mean Square Error. It is also the performance investigation parameter. The common utilized LMSE formula (5) is specified as beneath [5].

$$LMSE = \sum_{j=1}^{M} \sum_{k=1}^{N} [O(X_{j,k}) - O(X'_{j,k})] / \sum_{j=1}^{M} \sum_{k=1}^{N} [O(X_{j,k})]^2$$

$$O(X_{j,k}) = X_{j+1,k} + X_{j-1,k} + X_{j,k+1} + X_{j,k-1} - 4X_{j,k} \quad (5)$$

4.5. Normalized Absolute Error

The full form of NAE is Normalized Absolute Error. NAE is also very famous performance investigation parameter. The general utilized NAE formula (6) is given below [5].

$$NAE = \sum_{j=1}^{M} \sum_{k=1}^{N} \left| X_{j,k} - X'_{j,k} \right| / \sum_{j=1}^{M} \sum_{k=1}^{N} |X_{j,k}| \quad (6)$$

4.6. Peak Signal to Noise Ratio

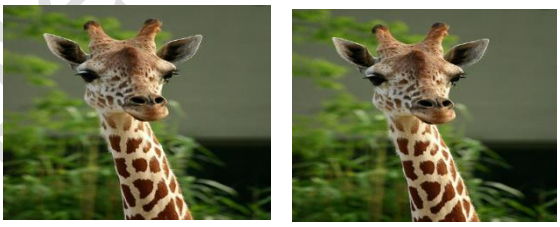
PSNR is utilized to calculate the statistical dissimilarities amid the cover picture and the info picture and for this computation, MSE is also utilized. The PSNR condition (7) is specified as underneath and the value of R is 255 [23]

$$PSNR = 10 \log 10 \frac{R^2}{MSE} \quad (7)$$

Input image Stego image

Figure 3: Cover picture and stego picture of Rose

Fig 3 shows that the data sets of Rose image of JPG type along dissimilar dimensions that utilized to contrast the proposed method with existing method. It has been clearly seen that the stego images with secret data is looking same like input images. Nobody can notice that the stego images has secret message and securely transport the private message from sender to receiver.



Input image Stego image

Figure 4: Cover image and stego image of Giraffe

Fig 4 is represented the data sets of giraffe color image with different dimension that used to get the results. The stego picture has 31,160 bytes of mystery information but look same like input image. In this figure, it has been easily seen that the stego image with secret data is looking same like input images. Attackers cannot notice that the stego image has confidential message and securely transfer this secret message.

Table 2. Comparison of Proposed and Existing Method for PSNR Results of different Images

Sn	Image	Dimensions	Payload capacity (Text)	PSNR	
				Proposed method	Earlier method [23]
1	(a) Rose.jpg	560 × 448 pixels	31,160	40.7595791	18.664 dB

			bytes	**dB**	
	(b) Rose.jpg	**5040 × 4032 pixels**	**31,160 bytes**	**60.6778423 dB**	**37.642 dB**
	(a) Giraffe.png	**750 × 1125 pixels**	**31,160 bytes**	**45.0900912 dB**	**23.809 dB**
2					
	(b) Giraffe.png	**6750 × 10125 pixels**	**31,160 bytes**	**65.2513488 dB**	**42.894 dB**

The contrast of the PSNR esteems of the proposed algorithm among the previous method is represented in Table 2. Dissimilar data sets are utilized in Table 2 for the evaluation of the PSNR values and JPG type pictures of rose among dissimilar dimensions such as 5040 × 4032 pixels, 560 × 448 pixels, are utilized to check the proposed method. PNG type pictures of giraffe along contradictory dimensions such as 6750 × 10125 pixels, 750 × 1125 pixels are utilized to investigate the proposed method. Table 2 shows that the proposed algorithm acquires better PSNR vales than the existing technique due to its novel hybrid based substitution method. The proposed hybrid based method enhances the payload and security of the confidential information to firmly move than earlier method.

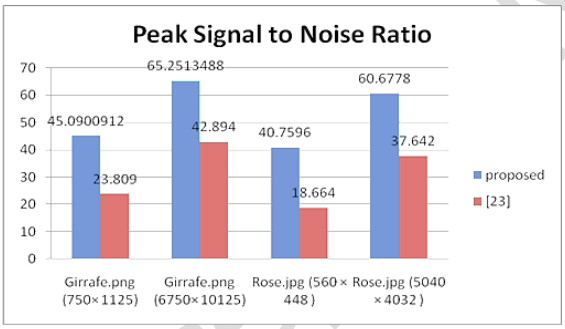


Figure 5: PSNR values comparison for Proposed and Existing method [23] for different images

Fig 5 illustrated that the proposed algorithm has acquired high PSNR esteems on entire images as compared to earlier Hybrid-LSB-MSB inserting technique. In the event of PSNR, this worth is contrarily relative to MSE esteem [38].

In the event that the MSE worth will be lower than the PSNR worth. The simulation results of PSNR with JPG type Rose color pictures (5040 × 4032 pixels) (560 × 448 pixels) and PNG type Giraffe color pictures (750 × 1125 pixels) (6750 × 10125 pixels) as data sets are used that shows the improved results of proposed algorithm than earlier Hybrid algorithm. Proposed algorithm gains the 40.7595791dB PSNR but earlier Hybrid algorithm has 18.664 dB PSNR value with JPG type Rose color image (560 × 448 pixels).

Earlier Hybrid algorithm has 37.642dB PSNR but proposed algorithm achieve 60.6778423dB PSNR value with JPG type Rose color image (5040 × 4032 pixels) and with the PNG type Giraffe color image (750 × 1125 pixels), existed hybrid algorithm has 23.809dB but proposed algorithm gains 45.0900912dB PSNR value. Proposed algorithm acquire 65.2513488dB PSNR but earlier Hybrid algorithm has 42.894dB PSNR values with PNG type Giraffe color images (6750 × 10125 pixels).

Table 3. Comparison of Proposed and Existing Method for MSE Results of different Images

Sn	**Image**	**Dimensions**	**Payload capacity (Text)**	**Mean Square Error**	
				Proposed method	**Earlier method [23]**
1	(a) Rose.jpg	560 × 448 pixels	31,160 bytes	5.5020182 dB	884.537 dB

	(b) Rose.jpg	5040 × 4032 pixels	31,160 bytes	0.0705823 dB	11.192 dB
2	(a) Giraffe.png	750 × 1125 pixels	31,160 bytes	2.0298821 dB	270.532 dB
	(b) Giraffe.png	6750 × 10125 pixels	31,160 bytes	0.0246232 dB	3.339 dB

In Table 3, MSE esteems comparison of the hybrid based proposed method along the existing hybrid based method. To compare the MSE esteems, dissimilar data sets are utilized in Table 3. First of all utilize the JPG type pictures of rose including contradictory dimensions such as 5040 × 4032 pixels, 560 × 448 pixels to analysis the performance of the proposed algorithm. Secondly, utilize the PNG type pictures of giraffe including contradictory dimensions such as 6750 × 10125 pixels, 750 × 1125 pixels to check the proposed algorithm. Proposed algorithm has lower MSE esteems than existing method due to its unique method of data substitution that improves the payload and picture quality of proposed algorithm.

Fig 6 illustrates that proposed method has obtained lowest MSE values on all images as compared to earlier Hybrid-LSB-MSB based system. In the event of PSNR, this worth is conversely corresponding to Mean Square Error value [38]. If MSE values will be lesser than the PSNR value will be high. The experimental outcomes of Mean Squared Error (MSE) with JPG type Rose color images (5040 × 4032 pixels) (560 × 448 pixels) and PNG type Giraffe color pictures (750 × 1125 pixels) (6750 × 10125 pixels) as data sets are used that shows the better results of the proposed algorithm than earlier hybrid algorithm. Earlier Hybrid-LSB-MSB based algorithm has 884.537dB MSE value with the JPG type Rose color image (560 × 448 pixels) but the proposed Hybrid algorithm gains 5.5020182dB. The MSE value of earlier hybrid algorithm is 11.192 dB but the proposed algorithm achieves 0.0705823dB value with the JPG type Rose color image (5040 × 4032 pixels). Proposed algorithm acquire 2.0298821dB MSE value but the earlier Hybrid algorithm has 270.532dB with the PNG type Giraffe color image (750 × 1125 pixels). Earlier Hybrid algorithm has the 3.339dB MSE value but the proposed algorithm gains 0.0246232dB with the PNG type Giraffe color image (6750 × 10125 pixels). The motive at the back of the improved performance of this proposed method is that, it has been utilized dissimilar operations to encrypt the confidential information and multi-operations are used in Hybrid-LSB-MSB based embedding technique to arbitrarily hide the encoded data in a cover picture. Furthermore, the simplicity and easiness of the implementation of this algorithm is more attractive than other existed hybrid solutions to generate improved results.

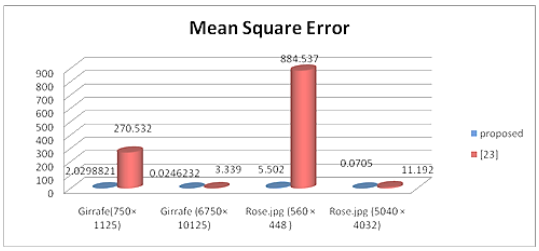


Figure 6. MSE values comparison of Proposed and Existing method [23] for different images

Table 4. RESULTS OF HYBRID-LSB-MSB BASED METHOD ON DIFFERENT IMAGES

Sn	Image	Dimensions	Payload capacity (Text)	NK	AD	SC	LMSE	NAE
1	Rose.jpg	560 × 448 pixels	31,160 bytes	47055.3593416	0.0451810	1.0008246	16.3265306	0.0024633
2	Rose.jpg	5040 × 4032 pixels	31,160 bytes	47146.8420391	0.0016234	1.0000322	145.000000	0.0000364
3	Giraffe.png	750 × 1125 pixels	31,160 bytes	19942.5689639	0.0115322	0.9999910	61.111111	0.0016497
4	Giraffe.pn		31,160	20025.562143	0.000095	1.000001	190.00000	0.000019

	g	6750 × 10125 pixels	bytes	7	4		0	1

In this Table 4, the extra performance analysis parameters such as NK, AD, SC, LMSE and NAE are shown. These all parameters are evaluated to show the significant security of the proposed Hybrid-LSB-MSB based method using different datasets of different dimensions.

5. CONCLUSION

The major objective of proposed algorithm was security with Hill Cipher encryption method and XOR encryption operations to encrypt the confidential information and with multi substitution methods to randomly hide the encrypted data as well as its improvement in PSNR values and lesser the MSE values than the previous image steganography algorithms. Investigational evaluation reflects that the proposed algorithm is safer in substituting of secret encrypted message in different sized images rather to the existed solutions. Moreover, proposed algorithm retains extra feature of randomly embedding encrypted data on the basis of arbitrary values. Furthermore, the utilize of Hybrid-LSB-MSB based implanted algorithm gain the high PSNR esteems (Fig 5) and lower MSE esteems (Fig 6) represents that the proposed algorithm is extensively efficient in security. Therefore, the Experimental results have demonstrated that the steganography algorithm not only acquires improved PSNR and MSE values, but also has good payload capacity.

REFERENCES

[1] C. T. Jian, C. C. Wen, J. Ritchie, C. V., H. Maulana and E. Rahman, "A New Image Encryption Technique Combining Hill Cipher Method , Morse Code and LSB Algorithm," 2018.

[2] H. A. Atee, R. Ahmad, and N. M. Noor, "Cryptography and Image Steganography Using Dynamic Encryption on LSB and Color Image Based Data Hiding," Foundation of Technical Education, Baghdad, Iraq, 23(7), 1450–1460, 2015.

[3] S. Prasad, and A. K. Pal, "Logistic Map-Based Image Steganography Scheme Using Combined LSB and PVD for Security Enhancement," Springer, Singapore, 2019.

[4] K. Muhammad, J. Ahmad, N. U. Rehman, Z. Jan, and M. Sajjad, "color image steganography using stego key-directed adaptive LSB substitution method," Multimedia Tools and Applications, CISSKA-LSB, 2016.

[5] S. K.. Ranade, "A Secure Steganographic Method Using Modified LSB (LSB) Substitution," 6(8), 1268–1273, 2017.

[6] S. Ahmed, "Data Hiding Using Green Channel as Pixel Value Indicator Data Hiding Using Green Channel as Pixel Value Indicator," Nov, 2018.

[7] P. Agrawal and A. Upadhyay, "A Survey of Different Steganography Technique using Cryptographic Algorithm," 7(2), 40–43, 2018.

[8] Y. Y. Wai and E. E. Myat, "Comparison of LSB, MSB and New Hybrid (NHB) of Steganography in Digital Image," 5(4), 16–19, 2018.

[9] M. Ulker and B. Arslan, "A Novel Secure Model : Image Steganography with Logistic Map and Secret Key,"

[10] I. J. Of, "A New Combined Method with High Security for Digital Images Steganography Based on Imperialist Competitive Algorithm," international journal of research in computer applications and robotics, 6(1), 1–12, 2018.

[11] M. C. E. M. Kasapbas, "New LSB-based colour image steganography method to enhance the efficiency in payload capacity, security and integrity check," 2018.

[12] K. Muhammad, J. Ahmad, S. Rho and S. W. Baik, "Image steganography for authenticity of visual contents in social networks,"2017.

[13] M. Saritha, Using MATLAB, 584–587. 2016.

[14] R. Tavares and F. Madeiro, "A LSB Steganography Method with Low Expected Number of Modifications per Pixel,"

[15] X. Zhou, W. Gong, W. Fu and L. Jin, "An Improved Method for LSB Based Color Image steganography Combined with Cryptography," IEEE/ACIS 15th, International Conference on Computer and Information Science (ICIS), 1–4, 2016.

[16] A. Nilizadeh, "A Novel Steganography Method Based on Matrix Pattern and LSB Algorithms in RGB Images," 154–159, 2016.

[17] R. Bhardwaj and D. Khanna, "Enhanced the security of image steganography through image encryption," Dec, 2015.

[18] D. Debnath, S. Deb and N. Kar, "An Advanced Image Encryption Standard Providing Dual Security : encryption using

Hill Cipher & RGB image steganography," 2015.

[19] A. Raj, "An Approach of Cryptography and Steganography using Rotor cipher for secure Transmission," 0–3, 2015.

[20] K. Joshi and R. Yadav, "A New LSB-S Image Steganography Method Blend with Cryptography for Secret Communication," 86–90, 2015.

[21] J. Thakur and N. Kumar, "DES, AES and Blowfish : Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis, "1(2), 6–12, 2011.

[22] A. Sharma, M. Poriye and V. Kumar, "A Review of Image Steganography Techniques : Development Trends to Enhance Performance," ISSN No. 0976-5697, 8(5), 2017.

[23] S. O. Akinola and, A. A. Olatidoye, "ON THE IMAGE QUALITY AND ENCODING TIMES OF LSB , MSB AND COMBINED LSB-MSB STEGANOGRAPHY ALGORITHMS USING DIGITAL," 7(4), 79–91, 2015.

[24] A. U. Islam, F. Khalid, M. Shah, Z. Khan, T. Mahmood and A. Khan, "An Improved Image Steganography Technique based on MSB using Bit Differencing," Mar, 2018.

[25] Y. Wang, Z. Liu and J. Ma, "A pseudorandom number generator based on piecewise logistic map," Nonlinear Dynamics, 83(4), pp. 2373–2391, 2016.

[26] S. Mazloom and A. M. Eftekhari-moghadam, "Color image encryption based on Coupled Nonlinear Chaotic Map," Chaos, Solitons and Fractals, 42(3), 1745–1754, 2009.

[27] H. Gao, Y. Zhang, S. Liang and D. Li, "A new chaotic algorithm for image encryption," 29, pp. 393–399, 2006.

[28] N. K. Sreelaja and G. V. Pai, "Swarm intelligence based key generation for text encryption in cellular networks," In 2008 3rd International Conference on Communication Systems Software and Middleware and Workshops (COMSWARE'08), pp. 622-629, IEEE, Jan, 2008.

[29] N. N. Tun, "Comparison of Simple Hybrid and Modified Hybrid of Audio in Image Steganography," 7(7), pp. 620–622, 2018.

[30] R. R. Mkamis, "HYBRID APPROACH FOR SPEAKER VOICE STEGANOGRAPHY USING MSB AND LSB," Emb : C × M × K, 9(I), pp. 1–13, 2017.

[31] R. S. Phadte, Cryptography, (Iccmc), pp. 230–235, (2017).

[32] Available Online at www.jgrcs.info IMAGE STEGANOGRAPHY USING LSBWITH, 3(3), pp. 53–55, 2012.

[33] M. Islam, M. Shah, Z. Khan, T. Mahmood and M. J. Khan, "A New Symmetric Key Encryption Algorithm using Images as Secret Keys," Dec, 2015.

[34] J. R. T and P. G. Scholar, "Secure Transmission of Data by Splitting Image," 362–368, 2015.

[35] I. Aqeel and M. Raheel, "Digital Image Steganography by Using a Hash Based LSB (3-2-3) Technique," Vol. 1, Springer, Singapore, 2019.

[36] C. Lee and J. Shen, "A High Payload Edge Detection-Based Image Steganography Robust to RS-Attack by Using LSB Substitution and Pixel Value Differencing," Vol. 2, Springer, International Publishing, 2019.

[37] S. Roy and M. Islam, "A Hybrid Secured Approach Combining LSB Steganography and AES Using Mosaic Images for Ensuring Data Security," SN Computer Science, 3(2), pp. 1-12, 2022.

[38] F. Anwar, E. H. Rachmawanto and C. A. Sari, "StegoCrypt Scheme using LSB-AES Base64," In 2019 International Conference on Information and Communications Technology (ICOIACT), pp. 85-90, IEEE, Jul, 2019.

[39] L. Serpa-Andrade, R. Garcia-Velez, E. Pinos-Velez and C. Flores-Urgilez, "Analysis of the application of steganography applied in the field of cybersecurity," International Conference on Applied Human Factors and Ergonomics, Springer, pp. 366–371, 2021.

[40] K. Tiwari and SJ. Gangurde, "LSB steganography using pixel locator sequence with AES," 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC), pp. 302–307, 2021.

[41] Y. Moussa and W. Alexan, "Message security through AES and LSB embedding in edge detected pixels of 3D images," 2nd Novel Intelligent and Leading Emerging Sciences Conference (NILES), pp. 224–229, 2020.

[42] S. Kaur, S. Bansal and R. K. Bansal, "Image steganography for securing secret data using hybrid hiding model," Multimedia Tools and Applications, 80(5), pp. 7749-7769, 2021.