Advances in Parallel Computing Technologies and Applications
D.J. Hemanth et al. (Eds.)

doi:10.3233/APC210147

A Novel Dual Encryption Algorithm to Enhance the Security in Image Transmission Using LSB 3-2-2 Technique

Anitha R [a,1], Ashok Kumar P M [a] and Ravi Kumar T [a]
[a] *Assoiciate Professor, Department of Computer Science and Engineering,Koneru Lakshmaiah Education Foundation, Vaddeswaram*

Abstract. Nowaday's providing the security for image is essential for correspondence.Steganography and cryptography are a technical method for the transfer of information to eliminate burglary and stealing of information.. Cryptography steganography hides the occurrence of a mystery message. We need more Secured and confidential images to transfer. Steganography procedure on RGB genuine nature utilizing LSB 3-3-2 technique.On the RED & GREEN line, on the LSB Three-Three-two is a procedure, while on the blue channel, it is just 2 LSB. Messages are not exactly RED and GREEN on BLUE platforms.Double encryption techniques are used, such as Caesar cipher & Vigenere cipher, to preserve the nature of the stegno photos and to increase message safety.Use of steganographic strategies are insufficient to give security to informingit is imperative to join the strategy of cryptography.A combination of Caesar Encryption and Vigenere applies to message until they are inserted in LSB Three-Three-Two methods to provide extra protection. At this pointwe are providing the Caesar code and Vigenere image estimating to enhance security. The target of this is to upgrade the secrecy & security of the image steganography. It will be more efficient becauseusing the two fold layer of security.

Keywords. Stegonography, Caesar, LSB, Vigenere Encryption.

1. Introduction

Today assortment of innovation is progressed, and everybody can without much of a stretch use innovation to help with performing activities. Nonetheless, as the innovation propels, the wrongdoing is additionally expanding the secure data issues, by unapproved parties. Cryptography is connected strategy where these methods are utilized to give information security and secure correspondence [1]. Cryptography gives highlights, for example, secrecy, realness and trustworthiness of information. For instance, classification is accomplished through encryption calculation which blends the private data so it gets muddled to anybody aside from the collector [2–4]. As predetermined by cryptography estimation, for example, RSA can be utilized to change the information into an indistinguishable arrangement. Steganography can't be distinguished by untrustworthy

[1] Anitha R, Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram.
E-mail: anitharaju15@gmai.com

gatherings. Steganography requires in any event two properties, to be specific: compartments or spread and messages. steganography is recognized as the grouping of media for instance image, sound, and video; in any case, pictures are used to shroud data. Additionally, the progressions in highly developed images are characteristically unnoticeable to independently. Along these lines, joining the cryptography with steganography is the best arrangement in making sure about a message [5, 6]. Here we use some sample images for steganography. There are primarily two type of images. The first is Rastor Images and a series of pixels or individual blocks are created in order to create a frame. JPEG, GIF, and PNG are both raster extensions to images. Any image you find online is a sort of raster image. Pixels are based to a certain degree on their resolution, and where they are stretched to take place, images are distorted or vague. We cannot however resize raster images without losing their resolution in order to maintain the pixel quality.The file extension for Roster images are PEG (or JPG) ,PNG GIF – Graphics [7]. The second category of images consists of Vector images that are additionally stretching and shaped to a certain degree by relative formulas. EPS, AI and PDF are the best way to construct graphics that still need to be resized [8].The same as a vector was shaped like logo and brand graphics and we should still have a very relevant dossier.The PDF - Portable Document Format, EPS - Encapsulated Postscript,AI - Adobe Illustrator is the extension for these styles of images. Documentation Stegnograpy [9, 10] is come into messages in the digital images in the technique of LS Bit. Message estimate with LSB technique is finished by supplanting and every portion of spread picture with computerized message bit. The Caesar imageis the mostly refer to calculations in the crypto as the most seasoned and easiest, so it is whatever but difficult to utilize [11, 12]. The Caesar image moves in a similar action with a cap of just 26 keys, so the amount of health is small for all characters in plaintext. In this loop, the level is very low. You must have an alternative equation for this function.Vigenere Cipher is a kind of polyalphabet substitution, but Caesar has safer locks. Essentially, Vigenere Cipher is like Caesar Cipher, it is important to transfer all the features of this message in Caesar Cipher, with all the features in Vigenere Cipher, so that the key and one byte are changed to bits in a message, the first three message sections are rooted in three pieces [13].The blue shading has only two messages embedded, since it is more sensitive and can change the data from the spreadsheet more extensively.

2. State of Art

Steganography implements techniques to mask clustered data, e.g. photographs, text, sound or advanced video, with the aspiration of not suspected the proximity of these puzzle data.In electronic steganography there are two main ways that they encrypt and disengage. All plaintexts, chips, pictures and other serious data may be communications. Encoding is the road to embedding a message into a remarkable image called the spreading image in order to construct stego media.By embedding them to the bottom portion of the pixel LSB is a fundamental and simple steganographic technique. Usually a 1 part message is inserted on of pixel pixel image with the grayscale image embedding of message. There are LSB 3-3-2 processes in the shading image. This technique is mainly designed to attain the dominant quality of the painting, LSB frame, where eight parts of a riddle are considered to be embedded spreads.As a result, in the 3RLSB pixel bits the three fundamental components of the confidential correspondence are hidden and the next 3

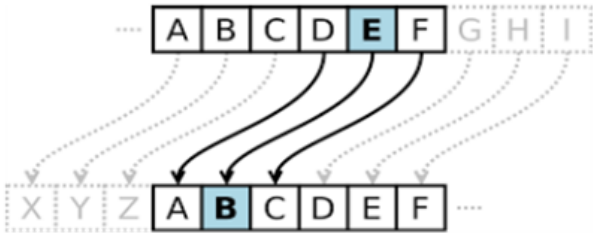

Figure 1. Caeser Cipher

pieces in the LSB Green pixels are enclosed in two BLSB pixels. Given the response of the human eye to blue, the bit is less bluish.

Caesar's cryptographic scheme guarantees that the message is obtained by replacing any letter of a particular plaintext with an additional letter in the plaintext's three letters. Science has the potential to write the encryption process equation using the figure of the Caesar with respect to the decoding process using the equation.

$$Ct(pt+n)Mod26 \tag{1}$$

$$pt = (Ct-n)Mod26 \tag{2}$$

Here C= Cipher text and P=Plain text and n= number of interval For example a plaintext encryption: STEGANO, n = 3 is ciphertext: VWHJDQR

Vigenere Cipher Technique mainly is for scrambling text with figure lines dependent on catchphrases. At first, the encryption sequence of this calculation can utilize the tabularecta where each column in the table expresses the cipher text as in the Caesar image [14]. The far left part of the tabularecta speaks to the key, and the top line to the plaintext. The essence of tabula recta shows that the chip text starts with the plaintext. Example: Essential Ciphertext: XQVLRVTM. CIPHER Key:

The integer can be generated by means of a hexadecimal 0x... In decimal prose, for instance, 0x1f represents 16+15=31. Hexadecimal entries may also be made. Bitor is inclusive logical or (bit-to-bit). Bitor input (0x12,0x38) or bitor output: 58

Figure 2. Bitand Bitor example

3. Proposed Work

Image steganography exploits the impediments of the natural eye. This exploration then uses a true nature image of RGB as a propagated picture to inject a hidden message using a 3-3-2 LSB approach related to both techniques. There are two standard structures in the projected methodology, for instance the embeddings strategy and the extraction technique .An image Stegonagraphy mode has four main processes encryption, embedding, decryption and extracting. In this paper from encryption process two encryption methods are used with new Algorithm.

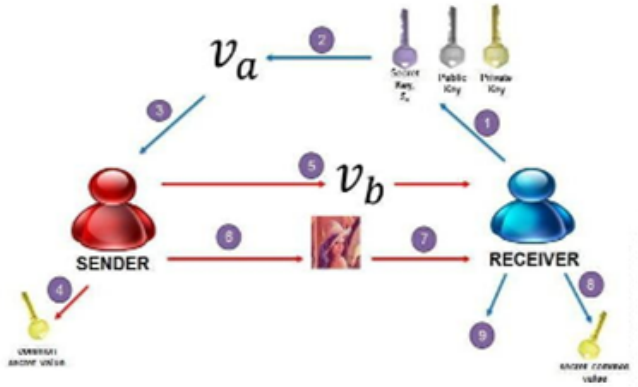

Figure 3. Secure Image Stegonagraphy model

3.1. Novel Dual Encryption Algorithm

"ABE encryption technique is not the only technique in PBE, there is IDE (Identity-Based Encryption) and Fuzzy-IDE as well" [15]. However this RGB as cover image and text messages is already available in this pre-owned 24-piece [7]. In this Algorithm initial RGB color image is taking as input and converted into binary format and in the second step Encryption formula is applied on the test message which we would like to send by applying the formula .Once it is done then apply vignere cipher for the tex obtained .Finally the converted binary image will come as output .In that image we can Keep secret image in LSB to RGB pixels . The subtleties of the installation process are:

1. Transformed RGB colour image to binary form
2. Formula for Encrtyption is applied for the text read from message

$$C_t(P_{t+n})Mod26 \tag{3}$$

3. Apply vigenere Cipher for text you obtained after applying Caesar Cipher

$$C_t(P_{t+n})Mod26 \tag{4}$$

4. Finally convert the binary form to Cover Page
5. Insert per 8-bit LSB secrecy message into the RGB pixel screen.

Table 1. Bitand on Red Color with 248

Sample Pixel Cover Red	0	0	0	0	0	0	0	0
Bits (248)	1	1	1	1	1	0	0	0
Results	0	0	0	0	0	0	0	0

THREE RED bits, THREE GREEN pixel bits, TWO BLUE pixel bits await all the embedded mystery message pieces. Do as in the red, green and blue channels with whole pixels. After that, render a message Bitand cycle with an estimated RED channel of 128, 64, 32, 16, 8 and 4 and Bit with a Blue Channel of 2 and 2.If the bitand results match the bits of each pixel so execute the red and green pixel calculation bitor with bits of 4, 2 and 1 and parts of 2 and 1 for blue pixel.

Table 2. Bitand on red with 128

Bitwise AND									
Message	1	1	1	0	0	1	1	0	Bitand
Bit (128)	1	0	0	0	0	0	0	0	
Results	1	0	0	0	0	0	0	0	

Table 3. Bitor on red with 4

Bitwise OR If result Bitand message and bit 128 = 128									
	128	**64**	**32**	**16**	**8**	**4**	**2**	**1**	
Red pixel	0	0	0	0	0	0	0	0	Bitor
Bit (4)	0	0	0	0	0	1	0	0	
Results	0	0	0	0	0	1	0	0	

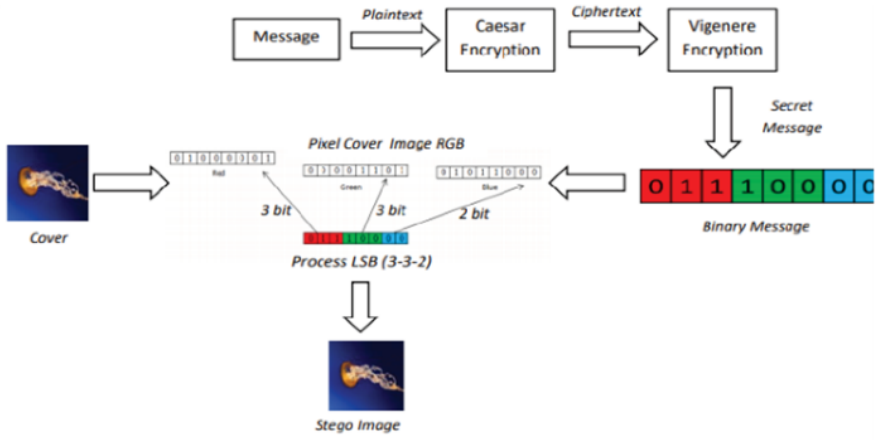

Figure 4. Embedded Process

4. Result and Analysis

At this stage 5 primary photographs from windows are used as an expansion photo of the specific dimension 1920x1200 using 8x8, 32x32, 64x64, 128x128 and 256x256 pixels of a resize ability.Embedded messages are maxed, half and 10 percent for the sums of characters. In case of photo sized m*n, at this stage maximum weight m*n bytes, the payload was acquired by multiplication of pixel size, illumining that the message RGB stuck 8 bit in 1 pixel.

Figure 5. 256X256 sample images of normal and Stego

The first picture and the stego are not separated from each other. The assessment of the MSE and PSNR figures was then determined to determine the picture quality. The MSE calculation is calculated in order to measure the PSNR as the average square error which calculates the contrast from the assessment value to the actual value of the loss of image quality or quantity. The MSE appreciation will first be calculated by PSNR. PSNR constitutes an opportunity for the calculation of commotion between the bulk of the big sign and the amount.The spread picture is entailto as a sign, and commotion is spoken to as a blunder. PSNR figures are smaller than 30 dB, anywhere bending is apparent because of inclusion. Efficiency is usually poor. However the high quality of stego pictures is at or above 40dB.

The Mean Square Error(MSE): The medium squared error calculation has to be predicted or calculated along with a It is stated that the data function is indicator or estimator.

$$MSE = \frac{1}{MN} \sum_{x=1}^{M} \sum_{x=1}^{N} (Sxy - Cxy)^2 \tag{5}$$

M and N shall be the sizes of the pictures, X and Y shall be the co-ordinate value of the pixel and S shall be stego and C shall be the cover graphic. Peak Signal to Noise Ratio:PSNR Since numerous signs have a wide powerful range, (proportion betweenvalues of an alterable amount) the PSNR is usually expressed in decibel scale.Systematically to recognize whether a specific calculation creates better outcomes [16].The parameter under investigation is the peak-signal-to-noise proportion.On the off chance that we can show that a calculation or set of calculations can upgrade a corrupted realized picture to all the more intently take after the first, at that point we can all the more precisely reason that it is a superior calculation.

Table 4. Comparison of Various Values of Various images

Resolution in pixel	Payload (bytes)	PSNR	MSE	bpp
8x8	64	30.9063	18.875	2.67
	32	40.4402	4.84896	1.33
	6	60.8156	0.703125	0.25
32x32	1024	31.1942	27.028	2.67
	512	35.8452	24.1683	1.33
	102	50.1794	4.09635	0.265
64x64	4096	34.5066	11.2694	2.67
	2048	39.5936	8.33138	1.33
	409	49.2905	6.02865	0.27
128x128	16384	37.9212	6.71733	2.67
	8192	43.5932	4.02779	1.33
	1638	55.2288	1.84395	0.27
256x256	65536	39.1224	5.7837	2.67
	32768	46.4125	2.79809	1.33
	6553	61.3623	0.642695	0.27

$$PSNR = 20log10\left(\frac{C^2max}{MES}\right) \tag{6}$$

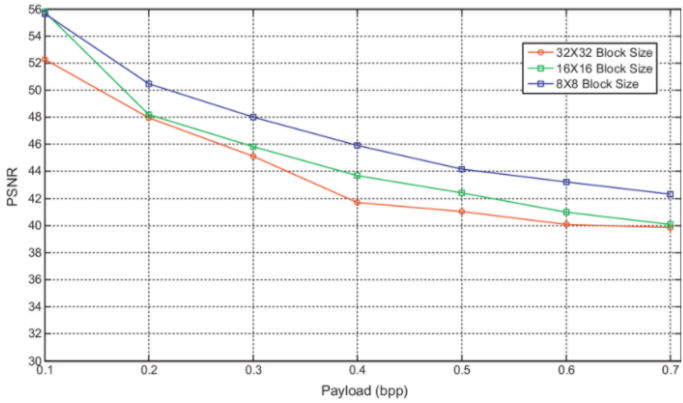

Figure 6. PSNR vs. payload for block size 8 × 8 to 32 × 32 for the input image (LEENA)

Indeed the geometry of a stego picture can decrease, if additional weight message is embedded in a spread image. With this evaluation, the most remarkable weight message is understandable, which the large image will now persevere on the indistinguishable border. After the figure is taken, the contrast calculation from MSE to PSNR is calculated from one image to the next in compliance with the image scale and message attribute measurements. The PSNR norm evaluation, which has been proven to be over 40dB, seems to mean a higher performance strategy. To test the nature of the extraction, (CER) is utilized as an estimating instrument. Message extraction must be done consummately; in any case, the proposedsteganographic technique will be futile. The Figure 7 the his-

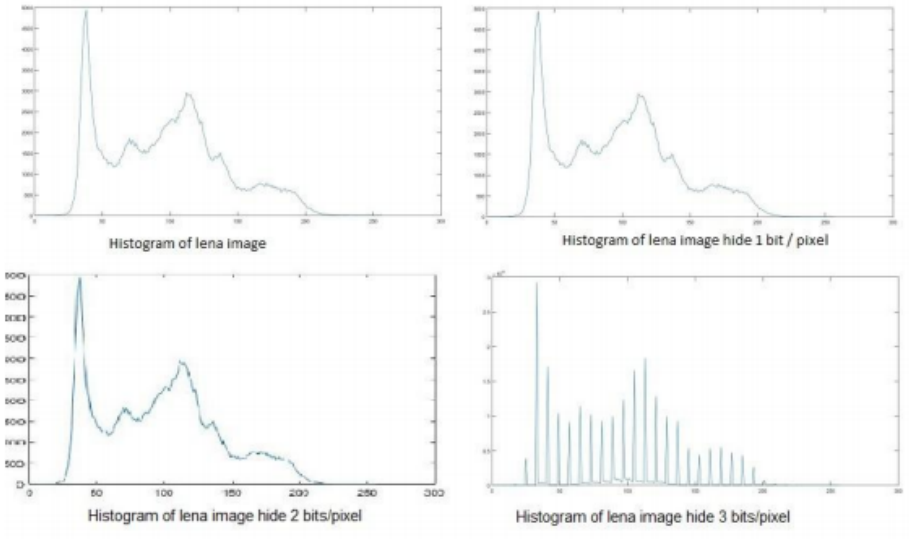

Figure 7. Histograms of Original and Stego images

togram of the original image and images after embedding data within cover image for one ,two and three bit per pixel.

5. Conclusion

Taking into Account this model is strong and is separating information without knowing the design of the proposed procedure is troublesome. Regardless of whether, the interloper gathers the LSB from the spread picture; he despite everything couldn't peruse the mystery message since it is as ciphertext. From the test result, it has confirmed that the proposed model will generate a decent quality picture subsequent to embeddings the high limit of mystery message with the PSNR estimation of 71.9 dB. At the point when the inserting limit of the mystery message expands, it will bring about slight decay of PSNR esteem.

References

[1] Anand J, Sivachandar K, Yaseen MM. Contour-based Target Detection in Real-time Videos. International Journal of Computer Trends and Technology. 2013;4(8);2615-18.
[2] Gayathri P, Umar S, Sridevi G, Bashwanth N, Srikanth R. Hybrid cryptography for random-key generation based on ECC algorithm. International Journal of Electrical and Computer Engineering. 2017 Jun 1;7(3):1293-8.
[3] Murali K, Madhumati GL, Khan H. Stochastic key generation mechanism in cryptography applications through partial reconfiguration. Journal of Advanced Research in Dynamical and Control Systems. 2017;9(12):1566-86.
[4] Tumati G, Rajesh Y, Manogna T, Ram Kumar J. A new encryption algorithm using symmetric key cryptography. International Journal of Engineering and Technology(UAE). 2018;7(32):436-8.
[5] Anand J, Flora TA, Philip AS. Finger-vein based biometric security system. International Journal of Research in Engineering and Technology. 2013 Dec;2(12):197-200.

[6] Anitha R, Pandiyaraju V, Muthurajkumar S, Sai Ramesh L, Rakesh R. Secure data sharing in cloud storage using KAC with certificateless encryption. Advances in Natural and Applied Sciences. 2015 Jun 1;9(6):134-9.

[7] Sahu AK, Swain G. A novel n-rightmost bit replacement image steganography technique. 3D Research. 2019 Mar;10(1):1-8.

[8] Sibia EV, Mareena G, Anand J. Content Based Image Retrieval Technique on Texture and Shape Analysis using Wavelet Feature and Clustering Model. International Journal of Enhanced Research in Science Technology & Engineering. 2014;3(8):224-9.

[9] Santoso HA, Rachmawanto EH, Sari CA. An improved message capacity and security using divide and modulus function in spatial domain steganography. In2018 international conference on information and communications technology (ICOIACT) 2018 Mar 6 (pp. 186-190). IEEE.

[10] Pawar SS, Kakde V. Review on steganography for hiding data. International Journal of Computer Science and Mobile Computing. 2014 Apr;3(4):225-9.

[11] Prasad GR, Vivek T, Rohith P, Yashwanth Y. Verilog implementation on cryptography encryption and decryption of 8 bit data using ECC algorithm. Journal of Advanced Research in Dynamical and Control Systems. 2017;9(14):2711-9.

[12] Vyas K, Pal BL. A proposed method in image steganography to improve image quality with LSB technique. International Journal of Advanced Research in Computer and Communication Engineering. 2014 Jan;3(1):5246-51.

[13] Murali Krishna B, Harika P, SasiPriya V, Nikitha K, Bharath M. Homomorphic cryptography. Journal of Advanced Research in Dynamical and Control Systems. 2018;10(4):129-36.

[14] Ramesh C, Rao DV, Murthy KS. Short Note on the Application of Compressive Sensing in Image Restoration. InSmart Intelligent Computing and Applications 2019 (pp. 267-273). Springer, Singapore.

[15] Selvakumar K, SaiRamesh L, Sabena S, Kannayaram G. CLOUD COMPUTING-TMACS: a robust and verifiable threshold multi-authority access control system in public cloud storage. In Smart Intelligent Computing and Applications 2019 (pp. 365-373). Springer, Singapore.

[16] Prasad GS, Praneetha DL, Srivalli S, Sukesh BV. Information security in cloud by using enhanced triple-DES encryption algorithm. International Journal of Innovative Technology and Exploring Engineering. 2019;8(5):679-82.