International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Research Article

Smart & Secure Data Communication using Steganography Technique

Yogesh Y. Lamture and Dr. Sudeep D. Thepade

Department of Computer Engineering, Pimpri-Chinchwad College of Engineering, Akurdi, Pune - 44

Received 10 Nov 2020, Accepted 10 Dec 2020, Available online 01 Feb 2021, **Special Issue-8 (Feb 2021)**

Abstract

This paper presents a smart and secure data communication mechanism using image steganography technique. For these two secret messages are embedded into the single-color image. A hybrid combination of special domain and frequency domain techniques used for this purpose. In this proposed method two secret messages (i.e. in the form of image) are embedded by applying DWT on L channel of Kekre's LUV color space model and LSB (Least Significant Bit) technique in Red, Green & Blue channel of RGB color space. By using this process, the extraction of the secret message becomes easy without access of the original cover image. The result & analysis of the proposed technique shows that it can resist various Steganalysis attacks.

Keywords: *Steganography, "Discrete Wavelet Transform" (DWT), "Least Significant Bit" (LSB), Kekre's LUV.*

Introduction

We all are living in the era of digital world and in this digital world everyone is using social media. Everyday lots of data is being share on the social media. Everyone is trying to communicate with each other by sharing some information. So that in this scenario there is concern of security of the shared data. Means user will able to share or communicate with other with higher amount of security so that no third party can steal their private information. There is one technique available called cryptography. It is used for privacy protection. In cryptography technique it converts the original message into some encrypted format named as cipher text. This encrypted text generated by using some key and then this encrypted text along with the key is being share along the communication channel. At the end of the receiver he will convert that cipher text into the original text (i.e. Decryption Process) using the same key used while encryption [1]. In today's modern world cryptography is mostly used for security purpose. But one disadvantage of the cryptography is that it cannot conceal the presence of the confidential message. By seeing the cipher text hacker can easily understand that some confidential communication is going on between two party. Then he will try to decrypt the message by applying various method. So, in order to conceal the presence of the confidential data there is a technique called as steganography. Steganography is nothing but hiding secret message inside any digital media. Digital media can be anything like digital image, video file, audio file etc. The encrypted data consists of symbols and when this type of data or message identified by someone then this will increase the chances of secret communication happens between two or more members. Steganography is somehow resembling to cryptography (i.e. Both these techniques are useful for secret communication). Steganography is an alternate tool for maintaining the privacy and security, rather than converting message of one form to another form hide the message inside any kind of digital media which will help to maintain the privacy. In steganography any kind of message can be easily conceal inside any digital media like video file, audio file, and image file. Steganography could be the first option in area where cryptography is against the law.

To implement steganography two techniques have been used i.e. special domain & frequency domain. In special domain the processing is directly perform on the intensity values contain by the image because of this there might be a chance of losing quality of image. But in frequency domain there is conversion of time domain image into frequency domain image and then finally confidential information can be embed into it. In previous steganography related research work most of the confidential images are in gray scale format instead of an RGB image. Some of them used RGB color image for information hiding purpose. RGB is correlated color space model means any modification in one channel affects the other channel also. So that it is not good idea to use RGB color image for watermarking purpose. This is the reason behind the selection of Kekre's LUV color model in this experiment. The experimentation results prove that our method performs better than the previous work mentioned in the literature and also generate good quality of image after embedding the

data. It can also resist against various Steganalysis attacks.

Related Work

K. Muhammad, in 2016 [2] presented image steganography technique for security of online social network content by using uncorrelated HSV color model. In order to achieve this author used HSV color space model. In this method first the RGB color cover image gets converted into encrypted scrambled image using image scramble algorithm. After this process this encrypted color cover image gets converted into HSV color space which is uncorrelated color space. Then select V channel for hiding the confidential information. In the next phase encrypt secret message by using iterative magic matrix encryption algorithm. Then this encrypted confidential information conceals inside the V channel of HSV color image using adaptive LSB (Least Significant Bit) algorithm along with the embedding key. After embedding process again combine this H, S, V channel and then convert HSV color image into RGB color image. In order to generate the final Stego image again decrypt the RGB color image using image descrambler. Extraction of secret message possible without access of the host image and confidential information. This paper did not test this method against various Steganalysis attacks. This method generates Stego image with good visual quality. In 2019, Chitra Biswas [5] presents mixed cryptography method, encryption of confidential message is done using symmetric key and for security purpose this symmetric key is also encrypted. One more plus point of the mixed cryptography technique is creation of digital signature by encoding the hash value of confidential message. The use of digital signature is at receiver side for the integrity check. Then finally all encoded message, encoded symmetric key and encoded digest are combine together to generate final confidential message. For increasing the privacy and security this final confidential message generated which is mention above is secured by using Steganography technique i.e. LSB ("Least Significant Bit"). The above mention mixed cryptography (i.e. combination of cryptography and Steganography) gives better protection for communication. Integrity checking of the confidential message is plus point of this paper. In 2017, Sunil Yadav [4] proposed method of image steganography using "2 DWT-FFT-SVD" on "YCbCr" color image. RGB is correlated color image i.e. if one of the channels of RGB gets modified then this will affect on the remaining channels also. In this paper YCbCr color space model used to steganography purpose. In this method apply "DWT" apply on both the host image and payload message in image format this will divide the image into four distinct sub bands i.e. "LLx1, LHx1, HLx1, HHx1" and "LLy1, LHy1, HLy1, HHy1". Then select "LHx1" and "LHy1" for next processing step perform FFT on "LHx1" as well as "LHy1" of this sub bands. After this process SVD (Singular Value Decomposition) algorithm applied on FFT coefficients. For embedding purpose change the singular values of S and then finally combine all the RGB plane for generating the Stego image. The disadvantage of this method is for extraction process it requires both original cover image and payload image. In 2018, Mohammed Hashim [3] presents a paper which describe the various performance metrics for image steganography technique combine with analysis of LSB based on variety of image forms. This paper describes various evaluation measures for image steganographynewly created HH sub band i.e. "Q-LL" with the help of following formula [9].

$$WQLLn = QLLn + WRn * k \quad (2)$$

Where QLLn is the quantized LL sub band. WRn denotes secret image that is to be embedded. WQLLn denotes Stego image generated after embedding of the first secret image and k represents a constant parameter that denotes the concentration level of the secret image. The peak value of k will enlarge the concentration level of hidden secret image, this would result in easy recognition of Stego image. After hiding the secret image, apply "Inverse DWT" on the four sub bands, i.e. "LL", "LH", "HL", "WQLL" this will generate new L` component. Then convert L`, U, V color image back to RGB color image by using following formula [like Payload capacity measurement, Security measurement, Regular

Singular Image histogram, confusion matrix and "Receiver operatingcharacteristics" (ROC). Along with this there some image quality measurements (IQM) like "Mean Squared Error" (MSE), "Root Mean Square Error" (RMSE), "Signal-to-Noise Ratio" (SNR), "Peak Signal to Noise Ratio" (PSNR), "Image Quality Index" (Q Index), "Structural Similarity Index" (SSIM), "Image Fidelity" (IF) & "Normalized Cross Correlation" (NCC).

Proposed Methodology

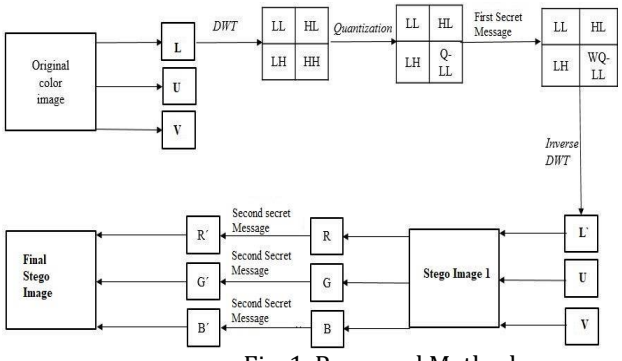


Fig. 1. Proposed Method

A) Embedding Process:

I) Embedding First Secret Message:

In the first step convert original RGB image to Kekre's LUV color model. The formula used for conversion of RGB into Kekre's LUV is mention below.[10]

$L = Red + Green + Blue$

$U = -2 * Red + Green + Blue$
$V = -Green + Blue$

After Kekre's LUV conversion, select L channel for further embedding process perform DWT [4] transformation technique to divide the L channel in Low-Low (LL), Low-High (LH) High-Low (HL) and High-High (HH). This Low-Low sub band represents the output of low pass filter and other remaining bands stores detail information regarding the quality of image and that are invisible to human eye.
Then by applying quantization process on LL sub band that will generate quantized "LL" sub band denoted as "Q-LL". Then simply replace HH sub band with "Q-LL". This procedure required because "Q-LL" (i.e. Compressed Low-Low sub band) is difficult to modify under any kind of malicious attack. This feature allows user to blindly extract the hidden message. The first secret image is hide into this newly created HH sub band i.e. "Q-LL" with the help of following formula [9].
WQLLn = QLLn + WRn * k (2)
Where QLLn is the quantized LL sub band. WRn denotes secret image that is to be embedded. WQLLn denotes Stego image generated after embedding of the first secret image and k represents a constant parameter that denotes the concentration level of the secret image. The peak value of k will enlarge the concentration level of hidden secret image, this would result in easy recognition of Stego image. After hiding the secret image, apply "Inverse DWT" on the four sub bands, i.e. "LL", "LH", "HL", "WQLL" this will generate new L` component. Then convert L`, U, V color image back to RGB color image by using following formula [10].

$$\text{Red} = \frac{L}{3} - \frac{U}{3}$$
$$\text{Green} = \frac{L}{3} + \frac{U}{6} - \frac{V}{2} \quad (3)$$
$$\text{Blue} = \frac{L}{3} + \frac{U}{6} + \frac{V}{2}$$

I) *Embedding Second Secret Message:*

After embedding of the first confidential image will generate Stego image and this image is in RGB color format. In order to increase the data payload, embed one more secret image inside this RGB color image. For that extract each channel i.e. Red, Green & Blue from RGB color image. Convert image pixel into binary 8-bit format the right most bits are called as LSB [3] and left most bits are called as MSB. The LSB bits contains less amount of information if we modify those bits it will not make any difference in the intensity values of image. MSB bits important information regarding the image quality if we try to modify the MSB bits of the image then resulted image will be having some amount of distortion in the quality of image. So that in order to hide or embed the second secret message LSB bits are useful. Extract pixels from each channel of the cover image i.e. Red, Green & Blue and convert those pixels into binary format. Same for secret image and replace LSB data of cover image by MSB data of secret image. After completion of hiding operation of all complete confidential image combine all three channels to generate Stego image. This Stego image having good visual quality.

B) *Extraction Process:*

In this proposed method removal confidential image is done without access to original host image. For extraction of the first secretimage convert RGB image into Kekre's LUV color image. Then perform one level "DWT" decomposition on L channel of LUV color space model. It will generate LL, LH, HL, HH sub bands. Then apply quantization process on the LL band it will generate Q-LL band. Then by using the following formula extract the hidden secret image [9].

$$WR_n = \frac{(HH_n - QLL_n)}{k} \quad (4)$$

"QLLn" indicates pixels value in "Q-LL", "HHn" represents pixels value of HH sub- band, "WRn" represent extraction bit of confidential image, and k denotes concentration level of Secret image and this value is same for all secret image hiding process. In order to extract the second hidden secret image, extract red, green & blue plane from RGB color image, and extract Least Significant Bits (LSB) from each of the plane. With this we can extract second secret image.

Results & Discussion

For the experimentation purpose dataset of 20 RGB color images have been used. These images are downloaded from the internet source. The dimension for the host image is 512 x 512. Below are the set of 20 images used as cover image for steganography method. Inside this image secret image has to be embed.

Fig.2. Cover Image Dataset

II) Mean Square Error (MSE):

This metric is calculated with in original host image and confidential image as well as original confidential image and extracted confidential image [7].

Below are the two secret images that are used for information hiding. The dimension for the one secret image is 256 x 256 and the dimension for another image is 131 x 142.

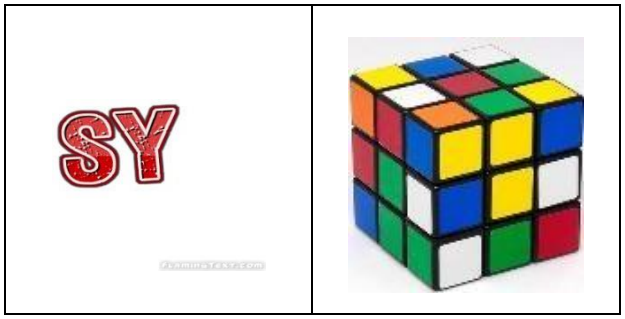


Fig.3. Secret Images

A) Result of Imperceptibility:

For this experiment, three "Image Quality Assessment" (IQA) metrics
[7] (i.e. "Peak Signal-To-Noise Ratio" (PSNR), "Mean Square Error" (MSE) and "Structural Similarity Index" (SSIM)) have been used for measurement of visual quality performance of the dual steganography mechanism.

I) Peak Signal-to-Noise Ratio (PSNR):

The PSNR is represents in decibels format (DB). Value of the PSNR measurement indicates perceptible quality of Stego image. This indicates that the value of PSNR is in direct proportion with the perceptible quality of image. Value greater that 35 DB indicates better visual quality of the image. Value less than 35 DB is having relatively less quality of image. The formula for PSNR is written below [7].

$$PSNR = 10 * \log 10 \left(\frac{Max^2}{MSE}\right) \quad (5)$$

II) Mean Square Error (MSE):

This metric is calculated with in original host image and confidential image as well as original confidential image and extracted confidential image [7].

$$MSE = \frac{1}{M*N} \sum_{i=1}^{M} \sum_{j=1}^{N} (p_{ij} - q_{ij})^2 \quad (6)$$

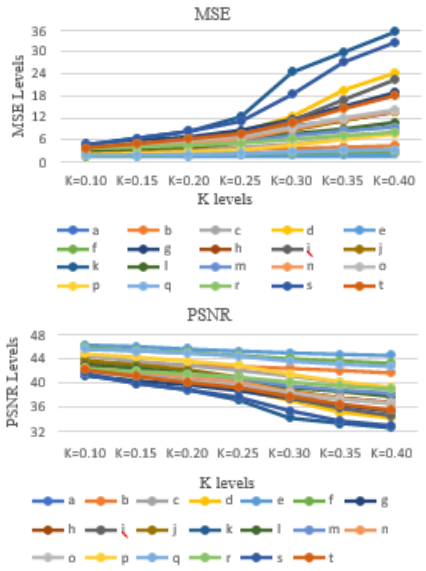
M and N indicates rows and columns of the input images respectively. represents host image and Stego image pixel at ith row and jth column respectively. Lower value of MSE indicates similar the two images. Ideally value of MSE should be zero.

Structural Similarity Index (SSIM):

It is the measure of change in structural information between host image and Stego image. It offers better estimation of perceived image distortion. The SSIM value denotes the similarity between the two set of images. SSIM with zero value represents that two images are identical [7].

$$SSIM(s,p) = \frac{(2\mu_s\mu_p + D_1)(2\sigma_{sp} + D_2)}{(\mu_s^2 + \mu_p^2 + D_1)(\sigma_s^2 + \sigma_p^2 + D_2)} \quad (7)$$

μs, μp= Mean intensities of cover and Stego pixel.
σs, σp= Mean intensities of cover and Stego image block
In this experiment k represented as strength of Stego image (i.e. Concentration level). The peak value of k indicates the concentration level of hidden confidential image. This will result in easy perceive of confidential image. So that imperceptibility testing is necessary. For that various performance metrics have been used like PSNR, MSE and SSIM. We perform the above method on different 20 images with varying value of k from 0.10 to 0.40. The details of result are shown in Fig.3, Fig.4, and Fig.5. Fig.3. indicates the result of "MSE" for k values ranging from 0.10 to 0.40. This graph concludes that as we increase the value of k the error values gets increased. From the below Fig.3 initially value of k is 0.10 and value of error approx. to 2 as the k increases then this error value becomes 35 approx. Fig.4. represents the result of "PSNR" metric. This graph shows that as we increased the value of k from 0.10 to 0.40 then automatically there is gradual decrease in the PSNR value. That indicates the visual quality of Stego image. For k=0.40 the PSNR value is approximately 47 DB or 48 DB and this value gets reduced up to 32 DB if value of k becomes
0.40. Fig.5. represents the result of SSIM measure. SSIM gives result that how much two images are identical to each other. The value of SSIM always measured in the range of 0 to 1. 0 indicates both images are not identical and 1 indicate both images are identical to each other. From the below graph initially when k is 0.10 the value of SSIM will be equal to 1 and as we increase the value of k up to 0.40 value of SSIM reduced up to 0.87.



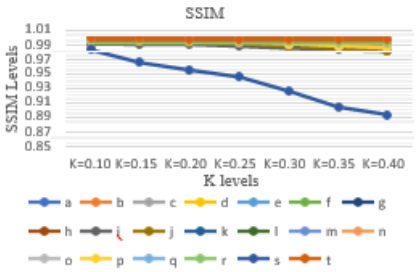


Fig.4.Performance Result Against Value of k

Table I. PSNR values against Stego attacks

Attack Name	Parameters	PSNR	
		Kekre's LUV	YCbCr
Salt & Paper Noise	0.01	47.8768	38.19
	0.02	45.7858	35.6851
	0.04	43.4356	33.0321
	0.08	40.85	29.9426
Gaussian Noise	0.1	45.1428	34.2763
	0.3	45.2537	31.5607
	0.5	44.6942	28.08
Darken	50	48.766	35.8329
	80	46.5363	31.3664
Cropping	10%	39.5918	21.99
	30%	40.4463	22.1349
Brighten	50	51.2906	38.2822
	80	48.247	33.4255
Blur	5	43.5057	33.3717
	6	43.5057	31.7167
	8	43.1306	30.2688
Twist	50	41.069	24.1882

Table II. Structural Similarity Index values against Stego attack

Attack Name	Parameters	Structural Similarity	
		Kekre's LUV	YCbCr
Salt & Paper Noise	0.01	0.9987	0.968
	0.02	0.9974	0.9345
	0.04	0.9939	0.8745
	0.08	0.9843	0.7678
Gaussian Noise	0.1	0.9964	0.9125
	0.3	0.9972	0.8885
	0.5	0.9977	0.8295
Darken	50	0.9988	0.9589
	80	0.9983	0.9072
Cropping	10%	0.9681	0.6311
	30%	0.9755	0.6497
Brighten	50	0.9993	0.9781
	80	0.9989	0.9426
Blur	5	0.9945	0.8729
	6	0.9945	0.837
	8	0.9936	0.8038

Table III. Correlation Coefficient values against Stego attack

Attack Name	Parameters	Correlation Coefficient	
		Kekre's LUV	YCbCr
Salt & Paper Noise	0.01	0.9997	0.998
	0.02	0.9996	0.9966
	0.04	0.9994	0.9941
	0.08	0.9982	0.9882
Gaussian Noise	0.1	0.9995	0.9952
	0.3	0.9995	0.9906
	0.5	0.9995	0.9784
Darken	50	0.9997	0.9952
	80	0.9996	0.9878
Cropping	10%	0.9983	0.9163
	30%	0.9986	0.919
Brighten	50	0.9998	0.9972
	80	0.9997	0.9925
Blur	5	0.9993	0.9915
	6	0.9993	0.988
	8	0.9993	0.9836
Twist	50	0.9988	0.9459

Table I, II, III are representing the performance result of existing and proposed method against various Steganalysis attacks in terms of PSNR, Structural Similarity Index and Correlation Coefficient. Image steganography technique using Kekre's LUV and YCbCr method is tested against attacks like Salt & Paper noise, Gaussian noise, brighten attack, Darken attack, Blur attack, Crop attack, and twist attack. From the above table values we can see that Kekre's LUV i.e. proposed method is perform well than existing method

Conclusion

In this paper we presented smart and secure data communication using image steganography technique. In this method we embed two secret messages in the form of image inside a single-color image. The first secret image embedded in L channel of kekre's Luv color image using DWT method and second secret image embedded inside RGB color image using LSB method. For measuring the performance of the above method, we use three image quality measurements like PSNR, MSE and SSIM. This proposed method tested against 20 different images. Also, this proposed method tested against various Steganalysis attacks like blur attack, salt & paper attack, Gaussian attack, JPEG attack, brighten attack, Darken Attack, Crop attack and twist attack. Experimental results show that the proposed method gives better performance than the existing method. Against various attacks also kekre's Luv gives best output than the YCbCr method. In future scope we will try to embed multiple RGB color images inside a single-color image

References

[1] Digital Watermarking and Steganography, 2nd Edition, Publication: Morgan Kaufmann.

[2] Khan Muhammada, Muhammad Sajjad b, Irfan Mehmoodc, Seungmin Rhod, Sung Wook Baik a, "Image steganography using uncorrelated color space and its application for security of visual contents in online socialnetworks", 16 June 2016. www.elsevier.com/locate/fgcs.

[3] Mohammed Hashim, Mohd Shafry Rahim, Fadil Johi, Mustafa Taha, Hassan Hamad," Performance evaluation measurement ofimage steganography technique with analysis of LSB based on variation image formats.", International Journal of Engineering & Technology,2018

[4] Sunil Kumar Yadav, Manish Dixit, "An Improved Image Steganography based on 2-DWT-FFT-SVD on YCBCR Color Space", International Conference on Trends in Electronics and Informatics, ICEI 2017.
[5] Chitra Biswas, Udayan Das Gupta, Md. Mokammel Haque, "An Efficient Algorithm for Confidentiality, Integrity and Authentication Using Hybrid Cryptography and Steganography", 2019 International Conference on Electrical, Computer and Communication Engineering (ECCE), 7-9 February 2019.
[6] Sabyasachi Kamila, Ratnakirti Roy, Suvamoy Changer, "A DWT based Steganography Scheme with Image Block Partitioning", 2015 2nd International Conference on Signal Processing and Integrated Networks (SPIN).
[7] Sahar A. El_Rahman, "A comparative analysis of image steganography based on DCT algorithm and steganography tool to hide nuclear reactors confidential information.", Computers and Electrical Engineering,2016.
[8] Shrikan Mudnur," Hiding the secret image using two over images for embedding the robustness of the Stego image using Haar DWT and LSB techniques. ", 2018.
[9] Xiao-Long Liu, Chia-Chen Lin*, Member, IEEE, and Shyan-Ming Yua "Blind dual watermarking for color images' authentication and copyright protection", DOI 10.1109/TCSVT.2016.2633878, IEEE.
[10] Dr.H. B. Kekre, Sudeep D. Thepade, "Improving 'Color to Gray and Back' using Kekre 's LUV Color Space", 2009 IEEE International Advance Computing Conference (IACC 2009) Patiala, India, 6-7 March 2009.