SRI SIDDHARTHA
ACADEMY OF HIGHER EDUCATION
Sri Siddhartha University
(Declared as Deemed to be University u/s 3 of UGC Act,1956)

No. SSAHE/EST/53/2021/2679 Date: 22/01/2021

To,
Team PDS
Inflibnet Centre (An IUC of UGC)
Infocity, Gandhinagar – 382007
Gujarat
E-mail: pds.help@inflibnet.ac.in

Sir,

Sub: Create PDS (Urkund) Acccount & Autorization Letter

I kindly request you to create PDS (Urkund) account of Sri Siddhartha Academy of Higher Education in the name of REGISTRAR with Email id (registrar@sahe.in) and I authorize Dr. Mallika M H, Chief Librarian to access **Urkund Anti Plagiarsm Software** admin account.

USER Admin name	**: Dr. Mallika M H**
Designation	**: Chief Librarian**
Mobile No	**: 9448748679**
Mail ID	**: library@ssit.edu.in**

Kindly do the needful

Thanking you,

Yours sincerely,

(DR.M.Z.KURIAN)
REGISTRAR
Sri Siddhartha Academy of Higher Education
TUMKUR - 572 107, Karnataka.

Unit U5744 - Sri Siddhartha Academy of Higher Education

Change | OrganizationLevels | + Invite to create User Accounts | + Create analysis addresses and send invite to Web inbox | + Whitelisting | Statistics

Properties

Id	U5744	**Contact person**	Dr. Mallika M H
Name	Sri Siddhartha Academy of Higher Education	**Email**	library@ssit.edu.in
		Phonenumber	9448748679
Emailsuffix	.ssahe@analysis.urkund.com	**Language**	English (US)
Organization	O2962 - Inflibnet India Nationwide		
Account	AC29720 - Sri Siddhartha Academy of Higher Education		

Document Cap Dashboard

Documents remaining

Used documents

Receivers

Show 100 entries Search:

Id	Date	Name	Personal Email	Account Email	Org A	Org B	Deleted
R875413	2023-01-03T07:42:00	SSDC	jdsrssdch@gmail.com	jdsrssdch.ssahe@analysis.urkund.com			☐
R862536	2022-11-19T05:12:00	Siddhartha University	chief.coe@sahe.in	chief.coe.ssahe@analysis.urkund.com			☐
R751436	2021-12-06T06:31:00	Dr. Renushree	dr.renushree@gmail.com	dr.renushree.ssahe@analysis.urkund.com			☑

Payment Receipt

TurnitIndia Education Private Limited
Max Towers, 16th Floor, Spaces
Suites #1603-05, 1608, 1610
Sector 16-B, Noida - 201301
Uttar Pradesh, India

Date 02/24/2020

Payment Method Wire Transfer

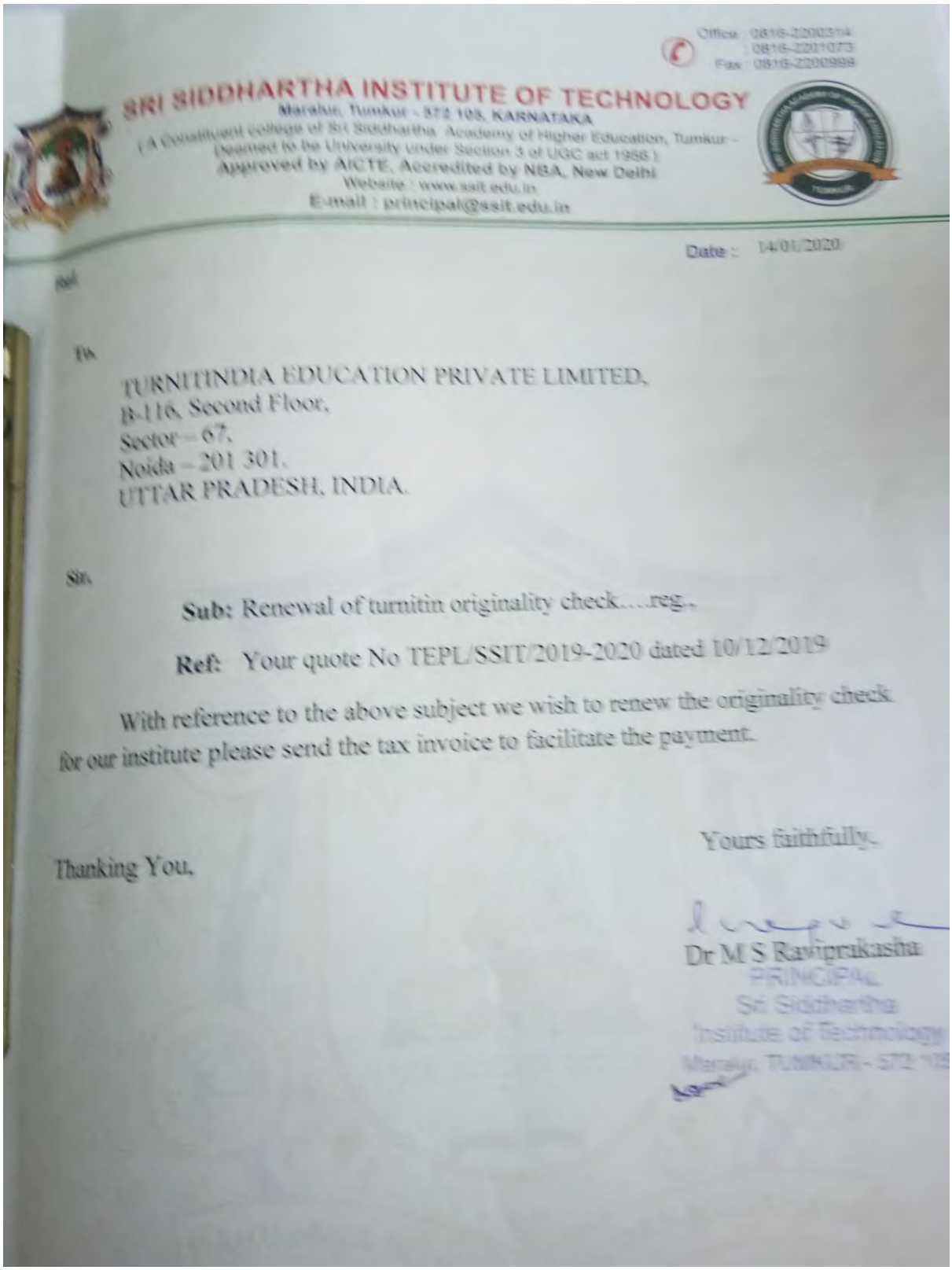
Bill To
GSTIN 29AACTS5707J1Z4
Sri Siddhartha Institute of Technology
Marlur, Kunigal Road
Tumkur, Karnataka 572105
India

Date	Description	Orig. Amount	Amount Due	Discount	Applied Amount
01/28/2020	Invoice #IND12000709	Rs.559,117.72	Rs.559,117.72		Rs.559,117.72

Total Rs.559,117.72

Sri Siddhartha Institute of Technology,

Turnitin details



SRI SIDDHARTHA INSTITUTE OF TECHNOLOGY
Maralur, Tumkur - 572 105, KARNATAKA
(A Constituent college of Sri Siddhartha Academy of Higher Education, Tumkur - Deemed to be University under Section 3 of UGC act 1956)
Approved by AICTE, Accredited by NBA, New Delhi
Website : www.ssit.edu.in
E-mail : principal@ssit.edu.in
Office : 0816-2200314
: 0816-2201073
Fax : 0816-2200999

Date : 14/01/2020

Ref.

To

TURNITINDIA EDUCATION PRIVATE LIMITED,
B-116, Second Floor,
Sector – 67,
Noida – 201 301.
UTTAR PRADESH, INDIA.

Sir,

Sub: Renewal of turnitin originality check....reg.,

Ref: Your quote No TEPL/SSIT/2019-2020 dated 10/12/2019

With reference to the above subject we wish to renew the originality check for our institute please send the tax invoice to facilitate the payment.

Yours faithfully,

Thanking You,

Dr M S Raviprakasha
PRINCIPAL
Sri Siddhartha
Institute of Technology
Maralur, TUMKUR - 572 105

turnitin

TAX QUOTE

Bill To:			Company:	
	Institution Name:	Sri Siddhartha Institute of Technology		Turnitindia Education Private Limited
	Billing Address:	Tumkur-Kunigal Rd, Saraswathipuram, Tumakuru, Karnataka 572105		B - 116, Sector 67, Second Floor, Noida, Uttar Pradesh 201301, India

Contact Name:	Ms. M. H. Mallika	PAN:	AAGCT1109P
Contact Designation:	Chief Librarian	GSTIN:	09AAGCT1109P1Z1
Phone:		Account/Subscription Manager:	Sabyasachi Mukherjee
Email:	[redacted]	Phone:	+91 9811466815
Fax:		Email:	[redacted]
		Quote Number:	TEPL/BS/T/2019-2020
		Quote Date:	26-Nov-2019
		Quote Valid Till:	10-Dec-2019
		Order Type:	Renew
		Proposed Subscription Start Date:	6-Nov-2019
		Proposed Subscription End Date:	5-Nov-2020

APPLICATION/SERVICE DESCRIPTION	INSTITUTION FTE	SUBSCRIPTION DETAILS	END-USER LICENCES Maximum	ENTERPRISE SUBSCRIPTION VALUE (US $)
Turnitin Originality Check	3042	Single-campus Enterprise Subscription 12M	3042	$6,840

PAYMENT OPTIONS	3Y SUBSCRIPTION			
	YEAR 1	YEAR 2 (RENEWAL)	YEAR 3 (RENEWAL)	TOTAL 3Y SPEND
Enterprise Subscription - Annual Payment Plan	$6,840	$6,975	$7,204	$20,949
GST (18%)	$1,196	$1,206	$1,318	$3,770
Total Payable	$7,839	$8,201	$8,842	$24,712

NOTES

1. GST @18% is included in the above amounts; however, the GST rate for Years 2 & 3 is subject to change as per rate notified by Government of India at the time of invoicing.
2. Upon acceptance of this QUOTE in writing via a Purchase Order, Turnitindia Education Pvt. Ltd. will provide an INVOICE payable in equivalent Indian Rupees. The US$ QUOTE AMOUNT will be converted to equivalent INR INVOICE AMOUNT as per the Market Exchange Rate as applicable on the Invoice Date.

PURCHASE ORDER/CONFIRMATION

1. Please raise your Purchase Order in the name of TURNITINDIA EDUCATION PRIVATE LIMITED, as follows:

TURNITINDIA EDUCATION PRIVATE LIMITED, B-116, Second Floor, Sector -67, Noida - 201301, Uttar Pradesh, India

2. Please e-mail the Purchase Order/Confirmation to your **Account Manager** or to **southasia@turnitin.com**
3. The original Purchase Order/Confirmation may be kindly be posted/mailed to:

TURNITINDIA EDUCATION PRIVATE LIMITED
B-116, Second Floor, Sector-67
NOIDA - 201301
Uttar Pradesh, India

BANK DETAILS	
	BENEFICIARY BANK: CITIBANK N.A.
	BENEFICIARY COMPANY: TURNITINDIA EDUCATION PRIVATE LIMITED
	BENEFICIARY COMPANY'S ACCOUNT #: 0714000002
	BENEFICIARY BANK BRANCH IFSC CODE: CITI0000002
	BENEFICIARY BANK BRANCH MICR CODE: 110002002
	BENEFICIARY BANK SWIFT CODE: CITIINBX

Acknowlegement for National Electronic Funds Transfer facility

सिंडिकेटबैंक SyndicateBank

शाखा / Branch Maralur दिनांक / Date 20/2/2020

एनईफटी के अंतर्गत राशि का जमा / अंतरण

Credit/ Transfer the amount under NEFT

हितधिकारी का नाम / Beneficiary's Name: TURNIT INDIA EDUCATION PVT., LIMITED

खाते का स्वरूप / Type of A/c

खाता सं. / A/c No. 0711409 3002

बैंक/Bank CITY BANK N.A.

शाखा/Branch

स्थान / Location केंद्र/Centre

आईएफएस कूट / IFS Code CITI0000002

	₹
राशि / Amount	5,5[illegible]7=73
कुल / **Total**	5,5[illegible]7=73

रुपए (शब्दों में) Rupees (in words) Five Lakh Fifty Nine thousand one hundred en Seventeen Rs Seventy three paise only मात्र / only.

आवेदक का नाम / Applicant's Name PRINCIPAL, SSIT, TMK

खाता संख्या / Account No. 220/424

पैन संख्या / PAN No. मोबाईल : Mobile

(₹ 50,000/- और अधिक राशि के मामले में / for ₹ 50,000/- and above)

खजांची/लिपिक / Cashier/Clerk प्राधिकृत हस्ताक्षरकर्ता / Authorised Signatory Sr

अंतरण की नियम एवं शर्तें पिछले पृष्ठ पर दी गई हैं ।

The terms & conditions of transfer are furnished overleaf.

एस.पी./S.P. 1246 / 30 x 2,50,000 Pads/08-2019/215

DCT and Shuffling based Image Steganography with Enhanced Embedding Capacity and Improved PSNR

by Shyla M. K

Submission date: 01-Jun-2020 11:33AM (UTC+0530)
Submission ID: 1335702814
File name: shyla-SSAHEJIR_paper.doc (318.5K)
Word count: 3590
Character count: 19407

DCT and Shuffling based Image Steganography with Enhanced Embedding Capacity and Improved PSNR

Shyla. M.K [1], Dr. K.B. Shiva Kumar [2], Dr. Rajendra Kumar Das[3]

[1] Assistant Professor, Department of Electronics and communication, SSIT Tumakuru, Karnataka, India.

[2] Professor and H.O.D, Department of Tele-communication, SSIT Tumakuru, Karnataka, India.

[3] Principal, DRIEMS, Tangi, Cuttok, Odisha, India.; drrkd67@rediffmail.com; 09438486086

Abstract: Steganography using image is the technique in which the secret information that can also be considered as payload data is concealed in a cover image or host media. Image steganography is one of the more secured forms of data transfer over an internet. In this image steganography method, the payload image is pre processed in which it is first compressed using discrete cosine transform and the percentage of compression can be decided based on the quality of a payload image required for transmission. Then IDCT is applied at the sender side only to reduce the size of a payload image and hence increasing the embedding capacity. Secondly the compressed payload image is shuffled based on the key generated and the same key is used at the receiver side to de shuffle the payload image. Payload image is made more secured by shuffling it with key. The compressed and shuffled image is then embedded using improved LSB-mapping with modulo-4 method. Experimental results shows improved peak signal to noise ratios and relative entropy values.

Keywords: DCT; IDCT; Image shuffling and relative entropy

1. Introduction

Steganography includes different types of communication methods in a secure manner where the secret information is concealed in a cover image. Some of the historically used of steganography techniques include writing paragraphs of some poetry and in between those lines use the invisible ink to hide secret information, used of micro dots, character marking etc. Steganography and cryptography are two different data hiding methods in the spy craft family: cryptography scrambles a message and converts it in to an unreadable form while steganography hides the message so that it cannot be seen. After cryptography, the transmitted cipher text can be easily noticed by the attacker. But with steganography, the attacker may not know that a hidden message even exists. [1].

Strength of any steganographic algorithms is based on percentage of data hiding and visually less distorted stego image. Therefore it is a challenge for new steganography algorithms to meet the expected increase in the embedding capacity and to maintain the encryption strength of the message. In images the data hiding capacity can be increased by using adaptive strategies that decide where it is better to embed the payload information. In steganography, the embedding capacity can be the highest sequence of bits or bytes that is hidden in a given cover image. Since abundant software tools which

performs encryption and decryption are available it is very difficult to assure security.[2]. Hiding text using either steganography or cryptography may require traditional encryption algorithms but images are quite different from text. Using basic cryptosystems like DES, AES, RSA or may be elliptic curve cryptography, we can encrypt images but it may not become efficient method since because size of an image is more when compared to text, hence traditional cryptosystems take more time to encrypt huge image data and also decryption may results in distorted recovery of payload image. [3].

In the frequency domain approach the images used to hide are transformed in to coefficients using different transformation techniques like DCT, DWT and Integer wavelet transforms. The Discrete cosine transform converts an image in to frequency representation usually by grouping the pixels in to blocks of 8x8 in size of non overlapping type and then converts in to coefficients. These coefficients are quantized and get modified in accordance with the secret data. [4]. The method used in this approach for payload embedding is the improved version of the data hiding algorithm proposed in [5]. In the proposed method the payload image is pre processed where discrete cosine transform and Inverse DCT is done at sender to compress the payload image and hence increase embedding capacity, then shuffling is done using key generated to improve the security of payload image.

2. Literature Survey

Yang Zhang et al. [6] proposed a novel encryption algorithm which is based on exchanging and shifting of two-columns and two rows round robin rule. The algorithm used the concept of random selecting of matrix in a random manner called sub-matrix. Plain text is converted to matrix form which is again scrambled based on random key and random key generated is maintained in a file which should be used for decryption. The algorithm can be operated with a limited number of operations on the matrix. Vinod patidar G.Purohit et al. [7] proposed an image encryption technique through a novel permutation and substitution scheme based on chaotic standard map. In this method, each round of encryption contained three stages, two permutation rounds and one substitution round. In order to speed up the encryption process the permutation and substitution process are performed based on row-by-row and column-by-column instead of pixel-by-pixel. Pseudorandom key is generated based on which the process of permutation is controlled. But in the substitution process the parameters of pixels of each row and column of different layers were merged with the pseudo random number sequences generated.

Huan Zhang et al. [8] introduced an enciphering algorithm which works by rearranging plane-bits and random multiple combinations was done on the transposition of pixel positions and changing of pixel values and hence this algorithm provides large key space, good confusion attributes. S V V Sateesh et al. [9] resulted with a suitable model to reduce the arithmetic complexity which uses modified DCT algorithm to perform image compression and encryption simultaneously. In this technique the both image compression and encryption is done to increase the level of security that can be implemented for real time applications. Lalitha G. et al. [10] proposed the secure transmission of information using image steganography. In the algorithm the image to be transmitted was compressed

using the wavelet compression and then RSA based public key encryption for the security of confidential information. The results were good but they involved very old cryptographic algorithm for encryption.

Nidhi Sethi et al. [11] proposed algorithm which was based on Haar wavelet transform and some logical operations to separate the image pixels. It generated cipher of high quality having excellent diffusion and confusion attributes. Encryption can be done at the time of data transmission; this is to protect their own raw data and miss consumption of it from intruders. In the present situation of attacks on security and wrong utilization of confidential matters or data, several enciphering methods were developing to keep our digital data secret. In this regard, Quist Aphetsi Kester [12] developed a new cryptographic image encryption algorithm for encryption of the images of size mxn by reordering the values of pixels in different layers. A novel data hiding method proposed by shyla.mk et al.[13] was based on DCT on RGB layers and compressed sensing algorithm shows good embedding capacity and enhanced recovery speed.

Luo W.et.al [14] proposed the LSB matching (LSB-M) which is a modified version of LSB method which is based on addition or subtraction of one to a carrier pixel after performing comparison with secret bits. Mielikainen J [15] proposed the new LSB-Modified revisited which will reduce the irregular coordinates produced by previous least significant bit methods. Also LSB-MR method works on the pixel values which is largely depends on correlation with the surrounding pixels and reduces the changes in cover image from 50% to 32%. At the receiver side deciphering using these traditional LSB methods is relatively easy, if once attacker would able to identify it, then they can be easily extract the information from stego image and this becomes disadvantage of these methods.

Bailey K.et.al., [16] Proposed stego color cycle (SCC) technique which spreads secret information over RGB layers of the host image in circular manner. The data is embedded in the order of sequence as red, green, blue and so on and this method used to increase the difficulty in the extraction process. Jamil Ahmad NUR.et.al.,[17] use the random method to embed data in three channels and it is improve the previous SCC method. The above mentioned algorithms may be improved versions than the traditional LSB techniques since they spread the information in three layers of carrier image in various manners, hence retrieving data becomes a challenge for an attacker.

Karim M et al. [18] proposed a new technique to increase the robustness of existing LSB substitution method by using secret key which will improve the security of an algorithm. In the above method, red channel is combined with secret key and together acts as an indicator for data embedding in green and blue layers. The payload information is embedded in green or blue layer based on the order generated using secret key and least significant information of red color layer. An attacker could not be recover easily the secret data without guessing the correct key. And also, the result analysis shows the better visual quality and robustness.

Wang et al. [19] used PVD to give better results against statistical attacks and to enhance embedding capacity; they used modulus function in their algorithm. Beginning PVD is applied on few nearer pixels and afterwards pixel value differencing is applied on the remaining pixels and pixels are considered based on modulus function in order to hide the payload or secret information. Joo, J.

C.et.al.,'s [20] approach an algorithm in order to improve security of the secret information, they use turnover policy which controls unusual changes in the histogram values and developed a method to avoid changes at the edges of the histogram of PVD sub ranges.

Maleki, N.,et.al.,[21] proposed adaptive scheme where four neighborhood pixels and their average differencing value is considered as one block and the secret key is used to determine the current block location and pixels in the edge areas are embedded with Q-bit. Based on PVD and modulus function many other techniques developed to improve PSNR and embedding capacity. [22-24].

3. Proposed method

In this paper, the method considered is to preprocess the payload image that may be secret image to be transmitted over an internet hence this approach can be used for various applications where secret transmission is required with high embeded capacity, added security while embedding secret data. In this approach first payload image is pre processed where it is first compressed using discrete cosine transform and the percentage of compression can be decided based on the quality of a payload image required for transmission. Then IDCT is applied at the sender side only to reduce the size of a payload image. Here only high frequency components will get compressed which cannot be recognized by human perception and hence we can get required visual quality with minimal distortion and at the same time enhanced embedding capacity.

Secondly the compressed payload image is shuffled based on the key generated and the same key is used at the receiver side to de shuffle the payload image. Payload image is made more secured by shuffling it with key. The compressed and shuffled image is then embedded using LSB-mapping with modulo-4 strategy which is used to hide the payload data inside a cover image. The embedding algorithm consider two bits of cover image pixel for data hiding therefore the data hiding capacity can be increased. The above method is as shown in fig.1 which is the block diagram of proposed method of data embedding.

In this proposed technique, after preprocessing of payload image it will be embedded in the cover image. In this method, two bits of payload information in embedded in a cover image pixel. In order to understand the method used in this technique, we will consider an example. Let the payload (PL_i) pixel value to be hidden will be **01**, carrier image pixel is CI_i=10110000, then the corresponding stego pixels (SI_0) will be $SI_0 = CI_0$ i.e., 10110000 no change in carrier pixel value since because our extraction is based on simple addition instead of subtraction, to avoid redundancy barrow bits generated at the time of subtraction. Hence at receiver side we perform $PI_0=SI_0+1$ =10110**001** and the LSB two bits are the recovered secret bits/payload bits similarly one example shows that if CI_2=11001**101** and data embedded that is payload pixel value is **11** then one bit change from carrier and payload pixel values and hence add one to carrier pixel then stego image pixel becomes11001110. Again at receiver side it is addition with one so $PI_2=SI_2+1$=110011**11** where LSB two bits are recovered payload bits. Similar technique is applied to embedded entire payload image by considering modulo-4 strategy.

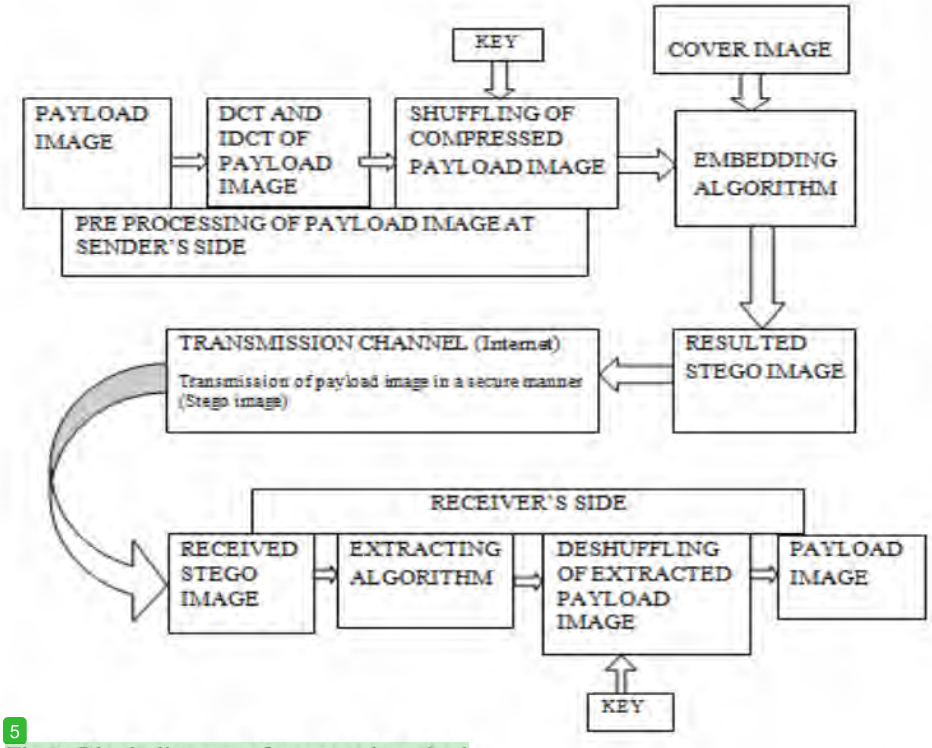


Fig.1. Block diagram of proposed method

3.1 Proposed Algorithm

At the transmitter side, the algorithms undergoes the following steps,

1. Select or choose a cover image of size M X N
2. Select a payload or secret data of size less than or equal to cover image.
3. Compress the payload image using DCT and IDCT technique and percentage of compression can be done for the required visual quality of payload image.
4. Shuffling of compressed payload image is done based on key generated. This shuffling is done to increase the security level.
5. Preprocessed payload image is embedded in the cover image.
6. The obtained stego image with good visual quality is transmitted to the receiver

The extraction process at the receiving end goes as follows;

1. The information is extracted from the received stego image using decoding algorithm which employs addition by one method.
2. Extracted image is de shuffled using the key.
3. The De shuffled image will be almost similar to the original payload image and for lesser payload we will get infinite PSNR which shows exact recovery of original payload image.

4. Experimental Results and Discussion

The algorithm shown above is executed using MAT Lab, version R2017a. Results are tabulated in table.1 and 2, in terms of PSNR and BER values by considering many cover and payload images of different sizes. Table 1 gives the results from the method proposed by Mohanad najm abdulwahed [25] and Table 2 shows the results obtained from the proposed method.

Peak signal to noise ratio values are calculated using equation shown in equation 1. and the corresponding MSE values are calculated using equation 2.

$$PSNR = 10\log_{10}[(255^2)/MSE] \quad (1)$$

$$MSE = 1/(mn)[x(i,j)-x^1(i,j)]^2, \text{ for all } i=1 \text{ to } n \text{ and } j=1 \text{ to } m \quad (2)$$

Bit error rate can be computed as 1/PSNR value and tabulated in table 1 and 2 for different embedding capacity.

Table.1. PSNR and BER for the Mohanad najm abdulwahed's method [25]

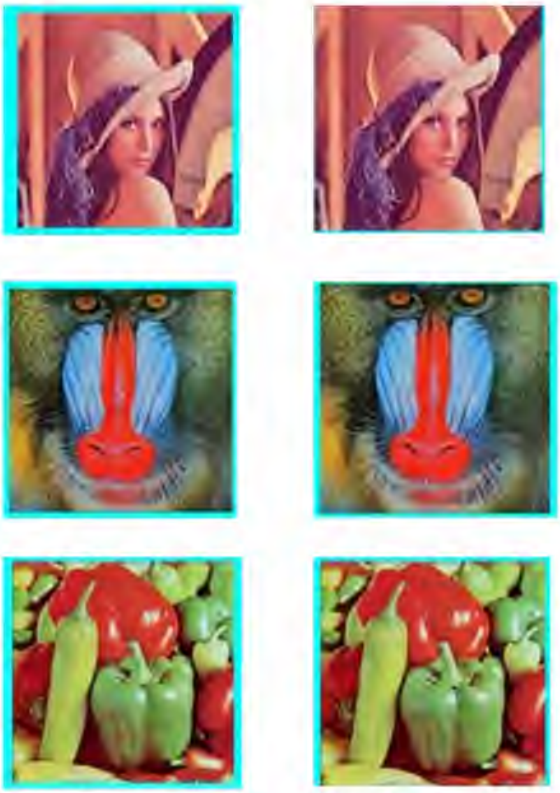
Cover Image 512 X 512	Results from the method[25] For embedding Percentage of 6.25		Results from the method[25] For embedding Percentage of 12.5	
	PSNR	BER	PSNR	BER
Lena	72.58	0.0137	66.61	0.0150
Baboon	72.86	0.0137	66.67	0.0149
Pepper	72.63	0.0137	66.60	0.0150

Table.2. PSNR and BER values for the proposed method

Cover Image 512 X 512	Results from the proposed method For embedding Percentage of 6.25		Results from the proposed method For embedding Percentage of 12.5	
	PSNR	BER	PSNR	BER
Lena	79.99	0.0125	75.70	0.0132
Baboon	80.39	0.0124	78.30	0.0127
Pepper	80.59	0.0124	78.06	0.0128

The values in the above table.2 are obtained from the experimental results done for the cover image of size 512 X512 and different payload image of size 1,31,072 in bits which gives embedding capacity of 6.25% and 12.5% embedding capacity by considering payload image of size 2,65,144 in bits.

Different Cover images considered for experiments and the corresponding stego images obtained are as shown in fig.2.



Cover Image Stego Image

Fig.2. different Cover and Stego images used in the proposed method.

5. Conclusion

Many algorithms for data hiding using steganography are aimed at providing high PSNR so that the resulted stego image is of less distortion and visually appear similar to the original cover image and also in our experiment the PSNR is measured between secret image and reconstructed secret image after extraction from stego image and the results shows highest PSNR values and for some smaller size secret images we are getting infinite PSNR values, indicting the maximum similarity between those images which means that the recovery is reversible and we can extract the secret or payload data without any loss in its content which is the very next important aspect of steganography; sending and receiving the message without any data loss.

The next one more aspect is embedding capacity that is how much data we can hide in a chosen cover image. Our method in this paper can able to hide more than 12.5% of embedding capacity because of DCT compression on payload image. After compression the image is shuffled using key generated in order to increase the security level of a secret image. The proposed algorithm is tested for f set of images with different sizes to meet the increased embedding capacity and PSNR value. The cover and stego images are also compared and tested for rel e entropy and results shows very less value that is 0.007 to 0.002, which shows very less or no difference between cover and stego images and hence the algorithm gives better security, which means small changes in stego image

cannot be noticeable or cannot be under visual perception. The proposed algorithm also resulted with good PSNR and increased embedding capacity.

Reference

[1]. N. F. Johnson and S. Jajodia, "*Exploring steganography: Seeing the unseen*", IEEE computer 31, no. 2 (1998) pp-(26-34).

[2]. C. Hosmer, "*Discovering hidden evidence*", Journal of Digital Forensic Practice 1, no. 1 (2006) pp-(47-56).

[3]. WangHan Shuihua and Yang Shuangyuan, Non-members, "*An Asymmetric Image Encryption Based on Matrix Transformation* ", ECTI transactions on computer and information technology vol.1, no.2 november 2005. Pp-(126-133).

[4]. Rig das, Et.al.,"*A novel Steganography method for image based on huffman encoding*"IEEE-conference

[5]. Shyla.M.K, K.B.Shivakumar, Rajendra Kumar Das, "*Image Steganography using Improved Lsb-Mapping Technique with Enhanced Recovery Speed* ",International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-4, November 2019 pp-(11473-11478).

[6]. Suli Wu, Yang Zhang, Xu Jing, "*A Novel Encryption Algorithm based on Shifting and Exchanging Rule of Bi-column Bi-row Circular Queue*," Computer Science and Software Engineering, IEEE International Conference on, 2008, pp. 841-844.

[7] Vinod Patidar G. Purohit, K. K. Sud, N. K. Pareek, "*Image encryption through a novel permutation substitution scheme based on chaotic standard map*," Chaos-Fractal Theory and its Applications, IEEE International Workshop on, 2010, pp. 164-169.

[8]. Huan Zhang, Ruhua Cai, "*Image Encryption Algorithm Based on Bit-Plane Scrambling and Multiple Chaotic Systems Combination*," IEEE Journal, 2010, pp. 113-117.

[9]. S V V Sateesh, R Sakthivel, K Nirosha, Harish M Kittur, "*An optimized architecture to perform image compression and encryption simultaneously using modified DCT algorithm*," Signal Processing, Communication, Computing and Network Technologies (ICSCCN), IEEE Proceedings of International Conference on, 2011, pp. 442-447.

[10]. Lalitha G, Ashish Jain, U. Raja, "*Secure Transmission of Compound Information Using Image Steganography*," International Journal on Computer Science and Engineering (IJCSE), vol. 3 no. 4, April 2011, pp. 1645-1648

[11]. Nidhi Sethi, Deepika Sharma, "A *New Cryptology approach for Image Encryption*," Parallel, Distributed and Grid Computing, IEEE 2nd International Conference on, 2012, pp. 905-908

[12]. Quist-Aphetsi Kester, "*A cryptographic Image Encryption technique based on the RGB Pixel shuffling*," International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), vol. 2, issue 2, January 2013, pp. 848-854

[13]. M. K. Shyla and K. B. Shiva Kumar, "*Novel Color Image Data Hiding Technique Based on DCT and Compressed Sensing Algorithm*" V. Sridhar et al. (eds.), Emerging Research in Electronics, Computer Science and Technology, Lecture Notes in Electrical Engineering 545, PP.1151-1157. https://doi.org/10.1007/978-981-13-5802-9_99, Springer Nature Singapore Pte Ltd. 2019

[14]. Luo W, Huang F, Huang J. "*Edge Adaptive Image Steganography Based on LSB Matching Revisited*". IEEE Trans Info Forens Sec 2010;5(2):201-214.

[15]. Mielikainen J. "*LSB Matching Revisited*". Sig Proces Let, IEEE 2006; 13(5):285-287.

[16]. Bailey K, Curran K. "*An Evaluation of Image based Steganography Methods*". Multi Tool App 2006;30(1):55-88.

[17]. Jamil Ahmad NUR, Jan Z, Muhammad K. "*A Secure Cyclic Steganographic Technique for Color Images using Randomization*". Tech J Uni Engg Tech Taxila 2014;19(3):57-64.

[18]. Karim M. "*A New Approach for LSB Based Image Steganography Using Secret Key*". In: 14th International Conference on Computer and Information Technology (ICCIT 2011). Dhaka, Bangladesh: 2011. pp. 286-291

[19]. Wang, C. M., Wu, N. I., Tsai, C. S., & Hwang, M. S. (2008). "*A high quality steganographic method with pixel-value differencing and modulus function*". Journal of Systems and Software, 81(1), 150-158.

[20]. Joo, J. C., Lee, H. Y., & Lee, H. K. (2010). "*Improved steganographic method preserving pixel-value differencing histogram with modulus function*". EURASIP Journal on Advances in Signal Processing, 2010(1), 249826.

[21]. Maleki, N., Jalali, M. & Jahan, M. V. (2014). "*Adaptive and non-adaptive data hiding methods for grayscale images based on modulus function*". Egyptian Informatics Journal, 15(2), 115-127.

[22]. Liao, X., Wen, Q., & Zhang, J. (2013). "*Improving the Adaptive Steganographic methods Based on Modulus Function*". IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 96(12), 2731-2734.

[23]. Shen, S., Huang, L., & Tian, Q. (2015). "*A novel data hiding for color images based on pixel value difference and modulus function*". Multimedia Tools and Applications, 74(3), 707-728.

[24]. Liao, X., Wen, Q. Y., Zhao, Z. L., & Zhang, J. (2012). "*A novel steganographic method with four-pixel differencing and modulus function*". Fundamenta Informaticae, 118(3), 281-289.

[25]. mohanad najm abdulwahed (2019). "*Digital image steganography scheme based on sk-lsb substitution and three parameters*", Journal of Theoretical and Applied Information Technology 15th August 2019. Vol.97. No 15,PP(4116-4137).

DCT and Shuffling based Image Steganography with Enhanced Embedding Capacity and Improved PSNR

ORIGINALITY REPORT

21%	11%	12%	9%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	"Image Steganography using Improved Lsb-Mapping Technique with Enhanced Recovery Speed", International Journal of Recent Technology and Engineering, 2019 Publication	5%
2	ijcsmc.com Internet Source	5%
3	khan-muhammad.github.io Internet Source	1%
4	Submitted to Jawaharlal Nehru Technological University Anantapur Student Paper	1%
5	link.springer.com Internet Source	1%
6	Vinod Patidar, G. Purohit, K.K. Sud, N.K. Pareek. "Image Encryption through a Novel Permutation-Substitution Scheme Based on Chaotic Standard Map", 2010 International Workshop on Chaos-Fractal Theories and	1%

Applications, 2010
Publication

7	"Proceedings of ICETIT 2019", Springer Science and Business Media LLC, 2020 Publication	1%
8	Submitted to SASTRA University Student Paper	1%
9	Shahrokh Heidari, Mohammad Rasoul Pourarian, Reza Gheibi, Mosayeb Naseri, Monireh Houshmand. "Quantum red–green–blue image steganography", International Journal of Quantum Information, 2017 Publication	<1%
10	Submitted to Visvesvaraya Technological University Student Paper	<1%
11	Submitted to VIT University Student Paper	<1%
12	Osmita Bardhan, Ansuman Bhattacharya, Bhabani P. Sinha. "A steganographic technique based on VLSB method using RC4 stream cipher", 2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2014 Publication	<1%
13	worldwidescience.org Internet Source	

		<1%
14	pdfs.semanticscholar.org Internet Source	<1%
15	Hong, Wien. "Adaptive image data hiding in edges using patched reference table and pair-wise embedding technique", Information Sciences, 2013. Publication	<1%
16	Submitted to Kyungpook National University Student Paper	<1%
17	Lecture Notes in Computer Science, 2015. Publication	<1%
18	"Emerging Research in Electronics, Computer Science and Technology", Springer Science and Business Media LLC, 2019 Publication	<1%
19	"ICDSMLA 2019", Springer Science and Business Media LLC, 2020 Publication	<1%
20	Lecture Notes in Electrical Engineering, 2014. Publication	<1%
21	Pavninderpal Kaur, Harchet Singh, Anupama Gupta, Akshay Girdhar. "An improved steganographic approach to diminish data	<1%

modification for enhancing image quality", 2014 International Conference on Medical Imaging, m-Health and Emerging Communication Systems (MedCom), 2014
Publication

22	Submitted to Pondicherry University Student Paper	<1%
23	es.scribd.com Internet Source	<1%
24	www.internetworkingindonesia.org Internet Source	<1%
25	Submitted to Universiti Teknologi MARA Student Paper	<1%
26	Submitted to University of Babylon Student Paper	<1%
27	"4th International Conference on Internet of Things and Connected Technologies (ICIoTCT), 2019", Springer Science and Business Media LLC, 2020 Publication	<1%
28	ijceronline.com Internet Source	<1%
29	davinci.newcs.uwindsor.ca Internet Source	<1%
30	Submitted to Napier University	

Student Paper

<1%

31 Submitted to Punjab Technical University
Student Paper

<1%

32 Submitted to Brunel University
Student Paper

<1%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		