International Journal of Scientific Research & Engineering Trends
Volume 4, Issue 4, July-Aug-2018, ISSN (Online): 2395-566X

# Development of an Efficient and Secure Image Transposal Algorithm Using 16 *16 Quantization Table

**Vijay Bhandari**
AISECT University
Bhopal, India
Vph2k14@gmail.com

**Dr.Sitendra Tamarkar**
AISECT University
Bhopal, India
drsitendra@gmail.com

**Dr. Piyush Shukla**
Rajiv Gandhi Technological University
Bhopal,India
pphdwss@gmail.com

***Abstract* – In later a long time, different mystery sharing plans for computerized pictures have been created in arrange to advance communication security. Past strategies in the writing have made endeavours efforts endeavours to accomplish the merits properties for a great mystery picture transposing such as execute (k,n) limit, basic recuperation, no pixel development, the produced covert image are important, the arrange of pictures is elective and lossless recuperation of the mystery image. To the leading of our information, no past mystery sharing scheme accomplishes all the over properties with great quality of important pictures. In this paper, we proposed puzzle image montages based on data stowing away hypothesis to make strides the quality of important pictures with lower computation and great expansibility. In the light of, the proposed plans have the important points of lossless and elective arrange recuperation and no pixel development expansion extension development.This is observing with past advance appear the execution of the planned conspires. The calculations displayed permit distinctive aligned of protection for the data covered up in the covering-document.**

***Keywords*- Quantization, Transformation, Mse, Psnr, Nae, etc.**

## I. INTRODUCTION

For the purpose of the improvement of computer science [4,5,6,12], Web allows people to trade data effectively in expansive magnitude. Interference with, alteration and other defence issues take place and they debilitate intimidate undermine Debilitate the data security seriously.

Therefore, data stowing away, whichever is individual the data security approaches, has showed up. Data covering up can insert mystery data into writings, pictures, recordings and other media intangibly.

Additionally twisting[1,2,45], inserting ability, bit rate and embedding(enclosing)effectiveness are the components whichever influence the execution of an data covering up strategy. Implanting capacity is the most vital figure, which alludes to the amount of hided mystery data. Be that as it may, the implanted mystery data would ordinarily present additional twisting and corrupt the security.

Embedding (enclosing) effectiveness is a worldwide show, which is characterized as the proportion of covering up mystery data to bit rate. In the hope that a great data stowing away strategy ought to be simple to implant and extricate mystery data.The encryption procedure ensures illicit get to of the information in figure 1.

The scrambled image[1,8,14,15,23,24] is a rowdy image[3,16,20] such that not anyone can get the mystery image[5,15] information without the exact key. The Steganography [9,17]contains covered up a computerized picture into another cover mixed media in sequence such as image[15] and video. Steganography method [18,19,30] is utilized when encryption[2,22,25] is not satisfactory.

The reason of Steganography[9] implants secrecy information in reselected image[31,45]].The rest of this original copy arranged as takes after:Section II gives discusses montage figure generation and secret image recovery information.

Section III gives existing methodology descriptions. Section IV proposed technique. Section V gives result and testing results descriptions, Section VI gives experimental results, Section VII conclude the paper.

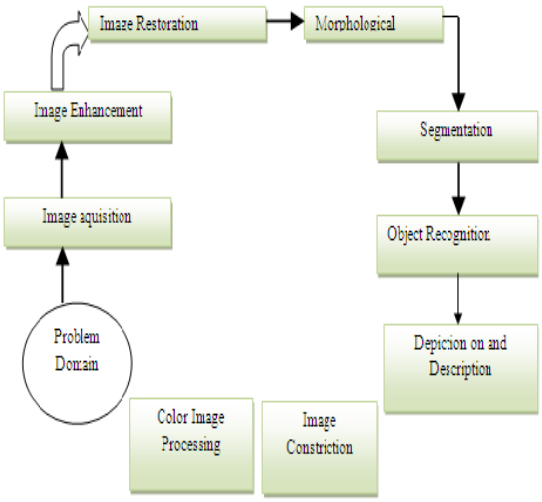


Fig.1 Section diagram of Key phases in artficial picture dispensation(image depiction).

## II.RELATED WORK

**1.An Edge Based Image Steganography with Compression and Encryption.** Security of mystery information has been a major issue of concern from old time. Steganography and cryptography are the two procedures which are utilized to decrease the security threat. Cryptography is an craftsmanship of changing over mystery message in other than human lucid shape. Steganography is an craftsmanship of stowing away the presence of mystery message. These procedures are required to ensure the information robbery over quickly developing organizes.

To accomplish this there is a require of such a framework which is exceptionally less vulnerable to human visual framework. In this paper a unused strategy is going to be presenting for information transmission over an unsecure channel. In this paper mystery information is compressed to begin with utilizing LZW calculation some time recently implanting it behind any cover media. Information is compressed to decrease its estimate. After compression information encryption is performed to increment the security.

Encryption is performed with the offer assistance of a key which make it troublesome to get the mystery message indeed in case the presence of the mystery message is reveled. Presently the edge of mystery message is recognized by utilizing canny edge locator and at that point inserted mystery information is put away there with the offer assistance of a hash work. Proposed procedure is executed in MATLAB and key quality of this extend is its gigantic information covering up capacity and slightest twisting in Stego image i.e. representation. This strategy is connected over different image i.e. representations and the comes about appear slightest twisting in modified image i.e. representation.

**2.Implementation of Image Steganography Algorithm using Scrambled Image and Quantization** Coefficient Modification in DCT To ensure reliability and integrity in information transmission, image steganography is cutting edge knowledge in today's digital world. It can be implement in spatial, time and frequency domain. In this research article, an effective algorithm has been introduced which would embed secret message data, scrambled by Arnold Transform, in frequency domain using the quantization coefficient modification in Discrete Cosine Transform (DCT)[43].

**3. A Fast and Efficient Data Hiding Scheme in Binary Images**

Several data hiding techniques have been proposed in the literature in recent years for binary images. However most of them suffer from image distortion. One such data hiding technique based on optimization and vibrant programming. The technique uses block pattern programming and the resulting images not only contain more data bits, but are also shown to be optimally distortion minimizing[16].

**4. A new covert image transmission technique via secret-fragment-visible montage images by nearly reversible color transformations**

A new covert image transmission technique is proposed, which transforms automatically a given large-volume secret image into a so-called secret-fragment-visible montage image of the same size. The montage image, which looks similar to an arbitrarily selected end image and may be used as a camouflage of the secret image, is yielded by dividing the secret image[26,27] into fragments and transforming their color characteristics to be those of the corresponding blocks of the end image.

Additionally skilled techniques are designed to conduct the color transformation process so that the secret image may be recovered nearly losslessly. A scheme of handling the overflows/underflows in the converted pixels' color values by recording the color differences in the untransformed color space is also proposed. The information required for recovering the secret image is embedded into the created montage image by a lossless data hiding scheme using a key[14].

## III.PROPOSED MODELLING

**1.Problem Definition-** A novel type of digital art, called covert-morsel-visible mortage, has been proposed here, that can be able to present security towards our images or covert communication of covert images.The montage image of this type is soothed of small-scale snippet of an input covert image and though all the snippet of the covert image are clearly seen, they are very tiny in size and so arbitrary in place that people cannot outline out what the basis covert image looks like, but the technique implemented here contains more error rate and has more computation time since it is based on greedy search algorithm.

**2. Proposed Methodology**-It involves following steps:
In the first place we take covert image partition into pantiles then convert each pantile image into a binary value through 16*16 quantization. It can be a form of covert value by combining all the value, after that Embed this covert value in

**Block Representation of Proposed**

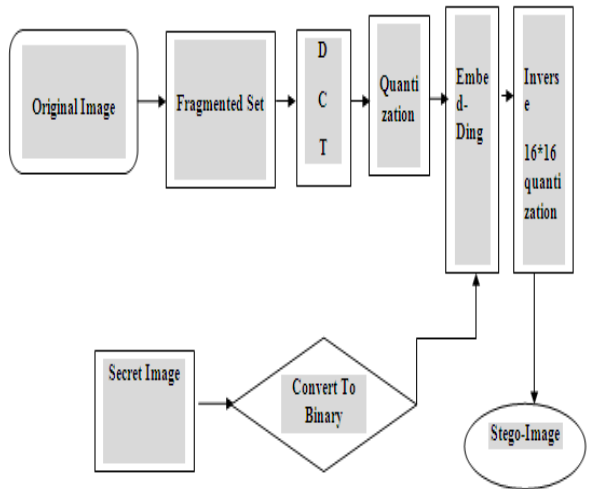


Fig. 2 outline of the proposed work.

Firstly transformation operation performing while quantization is parallel doing function but Embedding is next process and finally we perform inverse transformation.

**3.Transformation**

At this stage the partition of the image in the blocks is done. Each block is denoted by $a_i$ then 16*16 Quantization is applied to each one of the block denoted by $c_i$.

$$C_i = T\ a_i\ T'$$

The chip rate is calculated first which is the ratio of total no. of pixel in the host image by the no. of pixel in pantile ,then the value of chip rate is used to find the pn_sequence which is an array initiated by 1 to the value of chip rate,then temp is calculated by this chip rate and the value of temp rows and temp column is considered from the all pixel value of the face image, the watermarked significance of the pixel of pantile gets embedded in this region of temp rows and temp column.

**4. Quantization**

It is the technique used in image processing to reduce the redundancies, the lossy compression method is utilized here which is accomplished by compressing a extend of values to a as it were quantum esteem.

When the number of discrete symbols or the pixel are assigned by one constant value and then discrete symbols are generated as the pixels are less than this constant value assign to -1 and greater than this constant value are assigned as +1 then by this we can able to reduce the given stream, the flow becomes more packed in.

Most compelling evidence is secret image should be converted into a binary sequence (mi)This binary sequence is embedded in the middle and high frequency region of ci to get stego-block si. Embedding process is based on applying magnitude modulation to the quantized value of the host 16*16 quantization coefficient.

$$S_i(u,v) = \begin{cases} ci'(u,v)+Qstep\ (u,v)/3\ , & \text{if } mi=0 \\ ci'(u,v)-Qstep\ (u,v)/3\ , & \text{if } mi=1 \end{cases}$$

mi = each block of the secret image converted into a binary sequence. Embedding process is based on magnitude modulation to the quantized value of the host 16*16 Quantization coefficients. Embedding requires the selection of a suitable region in which the pantile should be embedded.

**5. Inverse Transformation**

For each stego block $s_i$ ( pixel value is converted in binary), the inverse 16*16 qunatization will be applied to get the output blocks $d_i$.
This is the inverse process of 16*16 quantization as it requires to retrieve the original secret image.

$$d_i = T'\ S_i\ T$$

During extraction the encrypted information need to extract first then the correct sequence of pantiles is obtained.

Block SizeR = 112;
Block SizeC = 112;
whole Block Rows = floor(rows / block Size R);
block Vector R=[block SizeR*ones(1, whole Block Rows), rem(rows, block SizeR)];
whole Block Columns=floor(columns/block Size);
block Vector C = [block SizeC * ones(1, whole Block Cols), rem(columns, block SizeC)];
Now each of the pantile generated is then converted into binary values using,

dec2bin (message (i,j)

Here we use pseudo random number generation for the generation of binary key from image.The tiny image (black and white) can be used for generating TRNGs and also image from paint software (eg. MS-Paint from Windows). The pixel value of the image can be generates with the simple functions in Matlab tool and it is converted into string value.

To convert the pixel value of the image into the binary value from integer, we have to check the RGB value of the each and every pixel. And then compare the pixel value. The corresponding values (0's and 1's) are written in the text file from left to right or in any other format. If there is a small change in the image it leads to a big difference in the generated random numbers.
Here,the concatenated value of the pixel are shown:

101010101011001000000000
010001111101011000000000
101001011111001000000000
100101100100100100000000
011011011111101000000000
100101101111110100000000
010000111111110100000000
101111111101111000000000
010100111010111110010100
111010111111111111101110
100010111111111111000010
101101000101111111111110
011010111100111111110000
011111011111111111001010
011010111111111111010110
101101111111111101111010
001101111111111000000000
111110111111100100000000
010010111111111100000000
111001111111001000000000
010110000110011100000000
111011101110110100000000
010100110001101000000000
101010001011001000000000
000000000000000000000000

From the generated binary value embeddingis performed ,which embedded the secret image into the cover image and send it to the receiver. At the receiver end the binary value is extracted and is again converted into pantile images. These pantile images are then embedded to make a secret image.

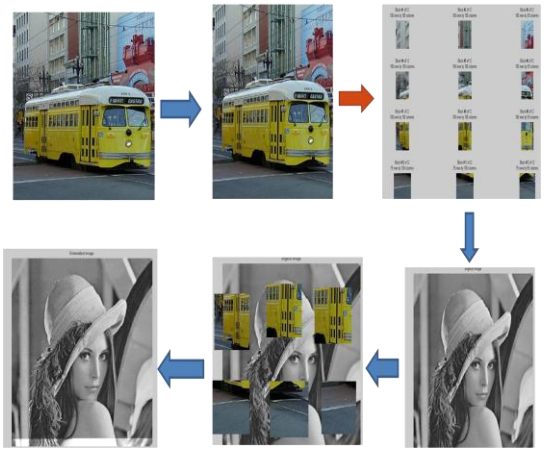

Fig.3 Illustrations of creation of secret-fragment visible montage image

First image is the original image or the secret image then the pixel value of this image is converted into the binary form by using transformation which is the second image and the division of the image take place in the third image the number embedding is done by exchanging the pixel value using 16*16 Quantization algorithm and the resultant image is our montage image[10,14] having some distortion in the pixel value as during embedding may be some noise get entered but the error rate calculated here is less than that of the previous and existing work. The sequence of the pantiles is also maintained here.

## IV.RESULTS AND DISCUSSIONS

As a result we work that gives less compression time.The strategies we are executing here too give a more effective method to verifying the client to get to the unique image. By the distinctive parameter we calculated here we discover ultimately that our proposed work is more proficient than the other procedure.

## ACKNOWLEDGMENTS

Our thanks to the Dr. Piyush Shukla and Dr. Sitendra Tamrakar who guide me a lot and I really thanks to them for a paper writing.i will be grateful for them.

## REFERENCES

[1]. Ching-Nung Yang et al. “extended color visual cryptography for black and white secret image” Elsevier, Theoretical Computer Science, 2016, pp 143-161.

[2]. Dawen Xu et al. “separable and error-free reversible data hiding in encrypted images” Elsevier 2016 ,pp 9-21.

[3]. vijay bhandari, Dr. Sitendra Tamarkar, Dr. Piyush Shukla”A Survey on: creation of montage images” international conference on advances of electronics computer & mathematical sciences 2016.

[4]. Moacir Ponti “image quantization as a dimensionality reduction procedure in color and texture feature extraction” Elsevier 2015,pp 1-12.

[5]. Angel Rose et al. “a covert verifiable scheme for secret image sharing”, Elsevier ,Second International Symposium on Computer Vision and the Internet 2015, pp 140 – 150.

[6]. Tong Qiao “steganalysis of jsteg algorithm using hypothesis testing theory”, Springer open journal EURASIP Journal on Information Security, 2015, pp 1-16.

[7]. Chih-Wei , Shiu, Yu-Chi Chen , Wien Hong “encrypted image-based reversible data hiding with public key cryptography from difference expansion”, Published by Elsevier, 2015.

[8]. Wen-Chung Kuoa,et al. “high capacity data hiding scheme based on multi-bit ecoding function” Elsevier , 2015.

[9]. Rina Mishra, et al. “ an edge based image steganography with compression and encryption” IEEE 2015,International Conference on Computer, Communication and Control.

[10]. Amrita manjrekar “ a novel approach for data transmission technique through secret fragment visible montage image” in Springer ,Emerging Research in Computing, Information, Communication and Applications, 2015.

[11]. Edwina Alias T., Dominic Mathew,"steganographic technique using covert adaptive pixel pair matching for embedding multiple data types in images" IEEE 2015 pp 426-429.
[12]. Rina Mishra et al. "a review on steganography and cryptography" 2015 international conference on advances in computer engineering and applications" IEEE 2015.
[13]. Xingyu Li et al. "a complete color normalization approach to histo-pathology images using color cues computed from saturation-weighted statistics" 2015 IEEE.
[14]. Ya-Lin Lee et al., "a new covert image transmission technique via secret-fragment-visible montage images by nearly reversible color transformations" IEEE transactions on circuits and systems for video technology, vol. 24, NO. 4, APRIL 2014,Pp 695-704.
[15]. Yicong Zhou, et al. "(n, k, p)-Gray Code for Image Systems" IEEE transactions on cybernetics, VOL. 43, NO. 2, APRIL 2013 pp 515-525.
[16]. Gyan, Aparajita "a fast and efficient data hiding scheme in binary images" IEEE 2012 Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing , DOI 10.1109.
[17]. Rong-Jian Chen and Jui-Lin L "novel multi-bit and multi-image steganography using adaptive embedding algorithms with minimum error" IEEE 2011 Fifth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing.
[18]. Sudhir Keshari Et al. "weighted fractional fourier transform based image steganography" IEEE ,International Conference on Recent Trends in Information Systems, 2011.
[19]. Piyush Marwaha, Paresh marwaha "visual cryptographic steganography in images" 2010 Second International conference on Computing, Communication and Networking Technologies IEEE 2010.
[20]. Yuan-Hui Yu , Chin-Chen Chang , Iuon-Chang Lin "A new steganographic method for color and grayscale image hiding" ELSEVIER 2007.
[21]. Lute Kamstra "reversible data embedding into images using wavelet techniques and sorting" IEEE transactions on image processing, VOL. 14, NO. 12, december 2005 ,pp 2082-2091.
[22]. Aloka Sinha et al. "A technique for image encryption using digital signature" Elsevier Science 2003,pp 239-245.
[23]. I-Jen Lai and Wen-Hsiang Tsai "Secret-Fragment-Visible Montage Image–A New Computer Art and Its Application to Information Hiding", IEEE Transactions on Information Forensics and Security, Vol. 6, No. 3, pp. 936- 945, September 2011.
[24]. Aloka Sinha*, Kehar Singh "A technique for image encryption using digital signature" February 2003; optics communication Elsevier.
[25]. Rasika Thakare, B Sumit and Umesh Kulkarni " A Method for Secret Image Transmission to Preserve Privacy" Sensors and Image Processing, Advances in Intelligent.
[26]. Systems and Computing 651 Springer.
[27]. Dinu Coltuc and Jean-Marc Chassery "Very Fast Watermarking by Reversible ontrast Mapping", IEEE SIGNAL PROCESSING LETTERS, VOL. 14, NO. 4, APRIL 2007.
[28]. Ture R. Nielsen, Peter Drewsen, Klaus Hansen "Solving jigsaw puzzles using image features" Pattern Recognition Letters 29 (2008) Elsevier.
[29]. Bing Zeng, et al. "Directional Discrete Cosine Transforms-A New Framework for Image Coding" IEEE Transactions On Circuits And Systems For Video Technology, Vol. 18, NO. 3, MARCH 2008.
[30]. Barnali Gupta Banik, Samir Kumar Bandyopadhyay "Implementation of Image Steganography Algorithm using Scrambled Image and Quantization Coefficient Modification in DCT" IEEE COMPUTER SOCIETY 2015.
[31]. ShanXue Chen and FangWei Li "Color Image Retrieval Based on Vector Quantization" 2010 IEEE.
[32]. Sumeet Kaur, Savina Bansal "Steganography and Classification of Image Steganography Techniques" 2014 International Conference on Computing for Sustainable Global Development.
[33]. H. Nicolas "New Methods for Dynamic Montageking" IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 10, NO. 8, AUGUST 2001
[34]. S.R.Subramanya"image compression techniques getting a handle on various options" IEEE 2001.
[35]. Chao-Tung Yang, William C.C. Chu et.al"Optimizing PSNR for Image atermarking using Summation Quantization on DWT Coefficients" 2015 IEEE 39th Annual International Computers, Software & Applications Conference.
[36]. Jiang Yong Zheng,Dong Hong Liang "A DCT-BASED digital watermarking Algorithm FOR Image", 2012 International Conference on Industrial Control and Electronics Engineering.
[37]. Michael Schukat" Public Key Infrastructures and Digital Certificates for the Internet of Things" 2015 IEEE.
[38]. Deepali G. Singhavi, Dr. P. N. Chatur "A New Method for Creation of Secret-FragmentVisible-Montage Image for Covert Communication" IEEE Sponsored 2nd International Conference on

Innovations in Information Embedded and Communication Systems ICIIECS'15.

[39]. Emilio Garcia-Fidalgo, Alberto Ortiz, Francisco Bonnin-Pascual "Fast Image Montageing using Incremental Bags of Binary Words" 2016 IEEE International conference on Robotics and Automation (ICRA) Stockholm, Sweden, May 16-21, 2016

[40]. Arthe Henriette Pascaline e.t al "Using Photomontage and Steganographic techniques for Hiding Information inside Image Montages" 2015 IEEE

[41]. Z. w.liao et. al. "Image Processing Using Template Model And Wavelet Domain Hidden Markov Model" Proceedings of the Third International Conference on Machine Learning and Cybernetics, Shanghai, 26-29 August 2004

[42]. Manoranjan Mohanty, Muhammad Rizwan Asghar, and Giovanni Russello "2DCrypt: Image Scaling and Cropping in Encrypted Domains" IEEE Transactions On Information Forensics And Security.

[43]. Rupesh Gupta et al."New Proposed Practice for Covert Image Combing Cryptography Stegnography and Watermarking based on Various Parameters"IEEE 2014.

[44]. Sumedha Sirsikar, Jagruti Salunkhe "Analysis of data hiding using Digital Image Signal Processing" 2014 International Conference on Electronic Systems, Signal Processing and Computing Technologies.

[45]. Santhosh Kumar B J, Roshni Raj V K and Anjali Nair "Comparative Study on AES and RSA Algorithm for Medical images" International Conference on Communication and Signal Processing, April 6-8, 2017, India.

[46]. Lute Kamstra, Senior Member, and Henk J. A. M. Heijmans "Reversible Data Embedding Into Images Using Wavelet Techniques And Sorting" IEEE Transactions On Image Processing, Vol. 14, No. 12, December 2005.

[47]. Anu Aryal,Shoko Imaizumi,Takahiko Horiuchi, and Hitoshi Kiyay "Integrated Algorithm for Block-Permutation-Based Encryption with Reversible Data Hiding" Proceedings of APSIPA Annual Summit and Conference 2017.

[48]. Asawari S. Chavan, Amrita A. Manjrekar"Data Embedding Technique Using Secret Fragment Visible Montage Image for Covered Communication" 2015,International Conference on Information Processing (ICIP) Vishwakarma Institute of Technology. Dec 16-19, 2015 IEEE.

[49]. Carlo Blundo and Clemente Galdi"Hiding Information in Image Montages" British Computer Society 2003.

[50]. Güzin Ulutas, Mustafa Ulutas, Vasif V. Nabiyev"A NEW CASCADED SECRET IMAGE SHARING SCHEME"2012 IEEE.

[51]. Zhibin Pan,Xiaoxiao Ma1, Xiaoman Deng "New reversible full-embeddable information hiding method for vector quantisation indices based on locally adaptive complete coding list" Published in IET Image Processing Received on 11th November 2013

[52]. Xuehu Yan · Shen Wang,Ahmed A. Abd El-Latif · Xiamu Niu"New approaches for efficient information hiding-based secret image sharing schemes"SPRINGER 2013.

[53]. Young-Chang Ho,Department of Information Management, National Central University, Jung"Visual cryptography for color images" Pattern Recognition The Journal Of The Pattern Recognition Society , 2003.

[54]. vijay bhandari, Dr. Sitendra Tamarkar, Dr. Piyush Shukla"A new model of M-secure image via quantization"Springer 2017 IDEA 2K17 IN RGPV BHOPAL.

[55]. vijay bhandari, Dr. Piyush Shukla "Design and Development of Symmetric Cipher for Text Data" SPRINGER 2017 in AMER GREEN.

## Author

Hello I am Vijay Bhandari , phd research scholar in cse branch from AISECT UNIVERSITY BHOPAL,INDIA.I did my B.E from LNCT Bhopal in 2007 and M.Tech from UTD SOIT Bhopal ,RGPV in 2009 .I have published more than 20 researh papers in reputed journals and conference like SPRINGER , ELSEVIER,IEEE, IET, SCOPUS etc.I would like to thanks my guide and co-guide who helped me a lot during research.