# A SECURE METHOD FOR HIDING SECRET DATA ON CUBISM IMAGE USING HYBRID FEATURE DETECTION METHOD

**Vinsa Varghese[1], Ragesh G.K[2]**

[1]*MTech Scholar, Dept. of Computer Science and Engineering, Adi Shankara Institute of Engineering and Technology, Kalady, Kerala, India*

[2]*Assistant Professor, Dept. of Electronics and Communication, Adi Shankara Institute of Engineering and Technology, Kalady, Kerala, India*

## Abstract

*Data Hiding is a method that hide confidential data in a cover medium so that it can be kept as most secure. This secure data hiding method consists of two types of information, a set of secret information that is to be embedded and a set of the cover medium in which the information is kept. The main aim of data hiding is to keep the data as secure as possible and also to protect from the hackers. Data can be hided in various domains such as text, audio, video and on images. The significant importance in which the images are used for data hiding is that the human beings are very weak in analyzing the small color changes .Data can be kept secure in medical images, aerial images, texture images and also on art images. Aesthetic data hiding is a new form of data hiding by the use of art image generated by some art image generation algorithm. People are attracted by the art image and thus they are not noticed about the hidden data. Thus data can be kept more securely. Cubism images are a type of paintings in which they are formed by analyzing an image or objects from multiple viewpoints. Cubism paintings are composed of intersecting line segments and various regions from different viewpoints. Line-Based Cubism Art image is created based on the concepts of cubism art. Data Hiding and lossless recovery is carried out with security measures. Secret Data is embedded using the Hybrid Feature Detection Method; Two Component LSB Substitution for edge areas and Adaptive LSB Substitution for smooth areas. Randomization of the data string that is to be embedded and Randomization of the regions is done in order to improve security. AES Encryption is also used to provide security against attacks. The Proposed method achieved improved capacity and better resistance to various Steganalysis attacks like Histogram Analysis and Chi-Square Attack.*

***Keywords:*** *Two Component LSB, Adaptive LSB, AES Encryption, Steganalysis, Chi-Square attack, Histogram Analysis*

----------***----------

## 1. INTRODUCTION

Data hiding is a promising and secure technique for information security, authentication, copyright protection, etc. Data hiding means information represented by some data are hidden in a cover medium to kept these data as secure. Different data hiding algorithms are implemented on images. But in most cases, the cover media is permanently distorted due to data hiding and thus the original medium is difficult to restore. Due to this there is no proper way to recover the marked media back to the original media without distortion. In least significant bit-plane (LSB) embedding method, the LSB bits are replaced with the data and the bit replacement is difficult to memorize and thus this method is not invertible.

A new form of data hiding that uses an art image generation algorithm enhances the camouflage effect for various information-hiding applications is proposed. An art image created based on the cubism properties from a source image, called line-based Cubism art image. This image generation is implemented based on the concepts of line-type Cubism. Line segments from the source image are detected by appropriate image processing techniques such as canny edge detection algorithm and hough transform. From various line segments that they obtained, only the relevant ones are kept after removing noise line segments. Regions formed by the prominent lines are created by extending the appropriate line segments and the pixels in each region are recolored identically by the average color of each of the region .The method finds line segments in the source image by the Canny edge detection technique and the Hough transform. Then it combines the nearby line segments and extends the remaining lines to the image boundaries. Thus the created regions are recolored by their average colors by creating the original source image . Then, based on the properties of the Cubism image creation process, a new data hiding method based on the Hybrid Feature Detection method is proposed. The secret data is hided on the Green and Blue components of the edges by using Two Component LSB Substitution method. Also the data is hided on the smooth areas of the Cubism image by using Adaptive LSB Substitution method. Inorder to ensure security randomization of data string and randomization of processing order of the regions is done. The secret data is encrypted with AES encryption method to provide high security from various attacks.

Steganalysis is a methodology used to detect steganography at variances between various bit patterns. The main objective of steganalysis is to determine whether the cover medium have hidden information embedded into them, and whether it can recover the secret information. In the cryptanalysis the hidden message is encrypted and the message is scrambled. But in the case of steganalysis the original media may or may not be with hidden data. The steganalysis process starts with a set of suspected information streams and then the set is reduced with the help of advance statistical methods.

## 2. CREATION OF CUBISM ART IMAGE

Line-based Cubism art image is based on the characteristics of the Cubism image created from lines and segmented regions from multiple viewpoints. From the input source image, prominent line segments are detected and rearranged to produce an abstract art image of the Cubism. Canny edge detection recognizes edges of differing characteristics based on the requirements.

### Algorithm 1: Cubism Art Image Creation

### Stage 1 Creating crossing-image lines.

Step 1. Perform Canny edge detection to find the edge points in source image S, thus producing in a new image S´.
Step 2. Perform the following steps to find prominent line segments in S´.
2.1 Find line segments L1, L2, . . . , Lm, in S´ by applying the Hough transform on S´, results in a second new image S´´.
2.2 Select the prominent line segments in S´´ with lengths larger than threshold value Lmin.
2.3 Compare every line pair Li and Lj with $i \neq j$ in S´´ and if the distance Dij between Li and Lj is smaller than Dmin, then delete Li if the length of Li is smaller than that of Lj ;or delete Lj , otherwise.
Step 3. Extend each of the remaining line segments in S´´ to the boundaries of S´´, and regard the source image S as being partitioned by these extended lines to form regions.

### Stage 2 Re-coloring intact regions.

Step 4. Create a binary image T of the size of S with initial pixel values all set to be 0.
Step 5. Fill the value of 1 into those pixels in T which correspond to those lying on each of the extended line segments in S´´.
Step 6. Perform following steps to re-color the regions in S.
6.1 Perform region growing in binary image T in a raster-scan method, and segment out 0-valued regions, R1, R2, ….., Rk, each of which is enclosed by a group of 1-valued line segments in S´´.
6.2 Compute the area Ai of each segmented region Ri in T and the average RGB color values (Cir, Cig, Cib) of all the pixels in Ri and re-color each pixel in Ri of S by the color values (Cir, Cig, Cib) , i = 1, 2, . . . , k.
6.3 Re-color all lines in S corresponding to the 1-valued extended lines in T with white color.
Step 7. Take the final S as line-based Cubism art image C.

## 3. DATA EMBEDDING ON SMOOTH AREAS OF CUBISM ART IMAGE USING ADAPTIVE LSB SUBSTITUTION METHOD

The Adaptive LSB Substitution is done on the Cubism art image as follows:
For each and every pixel of RED, GREEN and BLUE components of color image across smooth areas, the following embedding process is done:
1. If the value of the current pixel say cpi, is in the range 240 <= cpi >=255, then embed 4 bits of secret data in 4 LSB's of red and green component and embed 8 bits of secret data in 8 LSB's of blue component of the pixel.
2. If the value of cpi is in the range 224 <= cpi >=239 then embed 3 bits of secret data into the 3 LSB's of red and green component and embed 7 bits of secret data in 7 LSB's of blue component of the pixel.
3. If the value of cpi is in the range 192 <= cpi >=223 then embed 2 bits of secret data into the 2 LSB's of red and green component and embed 6 bits of secret data in 6 LSB's of blue component of the pixel.
4. If the value of cpi in the range 0 <= cpi >=192 then embed 1 bit of secret data into 1 LSB of the red and green component and embed 5 bits of secret data in 5 LSB's of the blue component of the pixel.

Similar method is implemented for extracting the hidden text from the image.

## 4. DATA EMBEDDING ON EDGE AREAS OF CUBISM ART IMAGE USING TWO COMPONENT LSB SUBSTITUTION METHOD

An image is composed of pixel values where each pixel value is addressed by three color components: Red, Green and Blue component. The Red component represent the Most Significant Byte, Green and Blue component represent the Least Significant Byte of data based on the intensity of color component. A new steganography method based on two components (Green and Blue) is proposed for hiding secret data on edge areas of the Cubism image created. The visual perception is high for red component, intensely for green component and least for blue component. Based on this concept maximum changes is done in blue and green component and none of the bits of red component is used for data embedding. In this method, 4 bits of green component and 4 bits of blue component is used for hiding secret data. The method is done by embedding 4 bits of secret data into 4 LSB's of blue component followed by embedding 4 bits of secret data in 4 LSB's of green component in each of the pixel.

## 5. DATA ENCRYPTION USING ADVANCED ENCRYPTION STANDARD

AES is a block cipher that operates on blocks of data, applying the transformation to each block. The transformation is done by using the encryption Key. AES

use symmetric keys, that uses the same key to encrypt the data The same key is also used to decrypt it. There are different types of AES based on the key size.AES-128 consists of ten rounds of processing, for AES-192 there are 12 rounds of processing and for AES-256 there are 14 rounds of processing. For AES-128 ,the user inputs 128 bytes of plain text along with an encryption key and outputs 128 bytes of cipher text. For decryption the cipher text along with the encryption key is given and decrypt it and produces the original plain text.

The encryption is done with an Add round key followed by 9 rounds of four stages such as Byte Substitution, Shifting of rows, Mix the columns and Add round key and a tenth round of three stages. The same process is done for both encryption and decryption. The decryption algorithm is the inverse of the encryption algorithm. The tenth round does not perform the Mix Columns stage.

## 6. EXPERIMENTAL RESULTS

In this work the line based cubism art image is created based on the features of the cubism art. The implementation is done with an input source image, relevant line segments in the image are detected and rearranged to form an art image of the Cubism flavor. Data hiding is done by using Hybrid Feature Detection method for 8 set of images. Performance Evaluation is done by using PSNR calculation. The maximum embedding capacity for all images is calculated and steganalysis is done by histogram analysis and chi-square distance.

Histogram is a graphical representation of a digital image. It is based on the number of pixels for each of the color component. Based on the histogram a viewer will be able to judge the entire color component distribution of an image.
The chi-squared distance calculates the distance between sets of vectors. The chi-squared distance between two vectors is defined as: d(x,y) = sum( (xi-yi)^2 / (xi+yi) ) / 2; Histograms of images are compared by using chi-squared distance.

The quality of reconstructed image can be tested by PSNR method. PSNR is an abbreviation of Peak Signal-to-Noise Ratio. It is used to describe the quality of data. PSNR is the ratio between the maximum possible power of a signal and the power of corrupting noise that affects. If the PSNR value is higher, it indicates that the reconstruction is of higher quality.

**Table -1:** Performance Evaluation using PSNR Value

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Source Image |  |  |  |  |  |  |  |  |
| Stego Image |  |  |  |  |  |  |  |  |
| PSNR | 71.782dB | 71.2923dB | 69.0739dB | 71.5392dB | 70.1123dB | 73.2782dB | 69.3641dB | 70.8762dB |

**Table -2:** Embedding Capacity Computation

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Source Image |  |  |  |  |  |  |  |  |
| Stego Image |  |  |  |  |  |  |  |  |
| Data Capacity | 236871.5 Bytes | 231515.5 Bytes | 232606.5 Bytes | 237636.5 Bytes | 234562.5 Bytes | 237871 Bytes | 234133.5 Bytes | 237864 Bytes |

**Table -3:** Chi-Square Distance between Cover image and Stego-image

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Source Image |  |  |  |  |  |  |  |  |
| Stego Image |  |  |  |  |  |  |  |  |
| Red Plane | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Green Plane | 5.9388e-05 | 3.7804e-05 | 3.2064e-05 | 4.3754e-05 | 4.2771e-05 | 4.3753e-05 | 5.001e-05 | 5.0016e-05 |
| Blue Plane | 5.6262e-05 | 2.3215e-05 | 2.0508e-07 | 4.0633e-05 | 4.6137e-05 | 5.938e-05 | 5.3138e-05 | 5.9412e-05 |

## 7. CONCLUSIONS

In this paper a new data hiding method is proposed combining the Hybrid Feature Detection method with the cubism art image. The data is hided securely in edge areas as well as on smooth areas .At first a cubism image is created from the source image by using canny edge detection and enhanced hough transform. The cubism image is created by prominent line extraction and region recoloring. Then data is kept inside the cubism image by using Two component LSB Substitution and Adaptive LSB Substitution. The Two Component LSB Substitution hides data in edge areas of the images and Adaptive LSB Substitution method hides data in smooth areas.The security is also ensured by encrypting the secret data by standard AES encryption.

The proposed method is tested for a set of eight images and the performance evaluation is done by PSNR calculation and embedding capacity is computed. It achieves better imperceptibility for the stego-images and also achieves high data embedding capacity. For this method, steganalysis is also done for the set of all images by using two steganalysis measures, Chi-Square Attack and Histogram Analysis. It is proved that it is more secure from steganalysis attacks by ensuring the security measures.

As a future work, in the cubism art image created along with secret data keeping it is also ensured with image authentication by using a hashing mechanism.

## REFERENCES


[1] Shan-Chun Liu and Wen-Hsiang Tsai,"Line-Based Cubism-Like Image—A New Type of Art Image and its Application to Lossless Data Hiding," IEEE Trans. Inf. Forensics Security, vol. 7, no.5,Oct. 2012.

[2] C. K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," Pattern Recog., vol. 37, pp. 469–474, Mar. 2004.

[3] D. C.Wu and W. H. Tsai, "Embedding of any type of data in images based on a human visual model and multiple-based number conversion," Pattern Recog. Lett., vol. 20, pp. 1511–1517, Aug. 1999.

[4] Z.Ni, Y.Q. Shi, N. Ansari, andW. Su, "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar. 2006.

[5] C. W. Lee and W. H. Tsai, "A lossless large-volume data hidingmethod based on histogram shifting using an optimal hierarchical block division scheme," J. Inform. Sci. Eng., vol. 27, no. 4, pp. 1265–1282, 2011.

[6] J. Fridrich, M. Goljan, and R. Du, "Lossless data embedding—New paradigm in digital watermarking," EURASIP J. Appl. Signal Process., vol. 2, pp. 185–196, 2002.

[7] M. Awrangjeb andM. S. Kankanhalli, "Reversible watermarking using a perceptual model," J. Electron. Imag., vol. 14, no. 013014, Mar. 2005.

[8] J. Tian, "Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug. 2003.

[9] J. Canny, "A computational approach to edge detection," IEEE Trans. Pattern Anal. Mach. Intell., vol. 8, no. 6, pp. 679–698, Nov. 1986.

[10] R. C. Gonzalez and R. E.Woods, Digital Image Processing, 2nd ed. Upper Saddle River, NJ: Prentice-Hall, 2002.

[11] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber,"Lossless Generalized-LSB Data Embedding," IEEE Trans. Image Process., vol. 14, no. 2, Feb. 2005.

[12] C. C. Lin, W. L. Tai, and C. C. Chang, "Multilevel reversible data hiding based on histogram modification of difference images," Pattern Recognition, Vol. 41, 2008, pp. 3582-3591

[13] M. Naseem, Ibrahim M. Hussain, M. Kamran Khan, and Aisha Ajmal ,"An Optimum Modified Bit Plane Splicing LSB Algorithm for Secret Data Hiding," International Journal of Computer Applications, Vol. 29,no.12, Sept.2011

[14] Marghny Mohamed, Fadwa Al-Afari and Mohamed Bamatraf,"Data Hiding by LSB Substitution Using Genetic Optimal Key Permutation," International Arab Journal of e-Technology, Vol. 2, no. 1, Jan. 2011

[15] M. Nosrati, R. Karimi, H. Nosrati, and A. Nosrati ,""Embedding stego-text in cover images using linked list concepts and LSB technique," World Applied Programming, vol .1, no .4, Oct. 2011

[16] A. Hertzmann, "A survey of stroke-based rendering," IEEE Comput. Graphics Applicat., vol. 23, no. 4, pp. 70–81, Jul./Aug. 2003.

[17] A. Hertzmann, "Fast paint texture," in Proc. 2002 Int. Conf. Computer Graphics & Interactive Techniques (SIGGRAPH 2002), Annecy, France, Jun. 3–5, 2002, pp. 91–96.

[18] D. Mould, "A stained glass image filter," in Proc. 14th Eurographics Workshop on Rendering, Leuven, Belgium, 2003, pp. 20–25.

[19] D. Mould, "Stipple placement using distance in a weighted graph," in Proc. Int. Symp. Computational Aesthetics in Graphics, Visualization & Imaging, Banff, Alberta, Canada, 2007, pp. 45–52.

[20] A. Hausner, "Simulating decorative mosaics," in Proc. 2001 Int. Conf. Computer Graphics & Interactive Techniques (SIGGRAPH 01), Los Angeles, CA, Aug. 2001, pp. 573–580.

[21] Y. Z. Song, P. L. Rosin, P. M. Hall, and J. Collomosse, "Arty shapes," in Proc. Computational Aesthetics in Graphics, Visualization & Imaging, Lisbon, Portugal, 2008, pp. 65–72.

[22] Westfeld, Andreas and Andreas Pfitzmann. "Attacks on Steganographic Systems: Breaking the Steganographic Utilities EzStego, Jsteg, Steganos, and S-Tools–and Some Lessons Learned," 3rd International Workshop on Information Hiding (2000).

[23] I. Avcibas, N. Memon and B. Sankur, "Steganalysis using Image Quality Metrics," IEEE Transactions on Image Processing, vol. 12, no. 2, pp. 221 – 229, February 2003.

[24] S. Dumitrescu, X. Wu and N. Memon, "On Steganalysis of Random LSB Embedding in Continuous tone Images," Proceedings of the International Conference on Image Processing, vol. 3, pp. 641 – 644, June 2002.

[25] T. Pevný, P. Bas, and J. Fridrich. "Steganalysis by subtractive pixel adjacency matrix," In Proceedings of the 11th ACM Multimedia & Security Workshop, pages 75–84, Princeton, NJ, September 7–8, 2009.

[26] C. Stanley. "Pairs of Values and the Chi-squared Attack," Master's thesis, Department of Mathematics, Iowa State University, 2005.

[27] K. Lee, A. Westfeld, and S. Lee. "Category Attack for LSB Steganalysis of JPEG Images," Lecture Notes in Computer Science, vol. 4283, pp. 35-48, 2006.

## BIOGRAPHIES

**Vinsa Varghese** is a MTech Student at Adi Shankara Institute of Engineering and Technology, Kalady in Mahatma University, Kottayam. Her interest areas include Image Processing, Steganography, Information Hiding and Information Security

**Ragesh G. K** is an Assistant professor at Adi Shankara Institute of Engineering and Technology, Kalady in Mahatma Gandhi University.