iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** IV **Month of publication:** April 2017

DOI: http://doi.org/10.22214/ijraset.2017.4088

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 5 Issue IV, April 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A Novel Secure Image Transmission Algorithm Using Reversible Color Transformations

K. Ayyanna[1], Veeresh.K[2], Kalyan. J[3], Hymavathi. K[4], Mounica. M[5]
[1,2,3,4,5]*Department Of ECE, Bits-Kurnool*

Abstract: ***A secure image transmission strategy is proposed, which changes consequently a given substantial volume mystery images into a purported mystery piece unmistakable mosaic images of the same size. The mosaic images, which seems to be like an subjectively choose target images and may be utilized as a disguise of the mystery images, are yielded by isolating the secret image into parts and changing their color qualities to be those of the relating pieces of target image. Capable strategies are intended to direct the shade change process so that the mystery images may be recovered about losslessly. A plan of taking care of the floods/undercurrents in the changed over pixels' shade values by recording the color contrasts in the untransformed color space is additionally proposed. The data needed for recovering the secret image is inserted into the made mosaic images by a lossless information concealing plan utilizing a key. Great exploratory results demonstrate the attainability of the proposed system.***

Keywords: Color transformation, Data hiding, Image encryption, Mosaic image, Secure image transmission.

I. INTRODUCTION

As of now, images from different sources are every now and again used and transmitted through the web for different applications, for example, online individual photo collections, private venture chronicles, report stockpiling frameworks, therapeutic imaging frameworks, and military images databases. These images typically contain private or secret data so that they ought to be secured from splitting at middle of transmissions. As of previous, number have been proposed for securing images transmission, for which two regular methodologies are images encryption and information adding away. Images encryption is a common method that makes utilization of the common property of a images, for example, high repetition and solid spatial relationship, to get an encoded images based on Shannon's disarray and dissemination properties . The encoded images is a clamour images so that nobody can acquire the mystery images from it unless he/she has the right key. Notwithstanding, the encoded images is a trivial record, which can't give extra data before decoding and may stimulate an assailant's consideration amid transmission because of its arbitrariness in structure. An option to dodge this issue is information concealing that conceals a mystery message into a spread images so that nobody can understand the presence of the mystery information, in which the information kind of the mystery message explored in this paper is a Images. Existing information concealing systems mostly use the procedures of LSB substitution , histogram moving, distinction development , expectation blunder development , recursive histogram adjustment , what's more discrete cosine/wavelet changes . Nonetheless, keeping in mind the end goal to diminish the contortion of the ensuing images, an upper destined for the bending worth is normally situated on the payload of the spread images. A dialog on this rate distortion issue can be found in . Along these lines, a fundamental issue of the systems for concealing information in images is the trouble to implant a lot of message information into a solitary images. Particularly, if one needs to conceal a mystery images into a spread Images with the same size, the mystery images must be exceptionally packed ahead of time. For instance, for an information concealing system with an installing rate of 0.5 bits every pixel, a mystery images with 8 bits every pixel must be packed at a rate of in any event 93.75% in advance with a specific end goal to be covered up into a spread images. Anyway, for some applications, for example, keeping or transmitting medicinal images, military images, authoritative reports, and so forth., that are profitable with no remittance of genuine mutilations, such information pressure operations are generally illogical. Also, most images pressure systems, for example, JPEG packing, are not suitable for line drawings and literary representation, in which sharp complexities between adjoining pixels are regularly destructed to wind up detectable curios . In this paper, another procedure for secure images transmission is proposed, which changes a mystery Images into a genuine mosaic images with the same size and resembling a preselected target images.

The change methodology is controlled by a mystery key, and just with the key can an individual recuperate the mystery images about losslessly from the mosaic images. The proposed strategy is roused by Lai and Tsai , in which a new sort of machine craftsmanship images, called mystery part obvious mosaic images, was proposed. The mosaic images is the aftereffect of reworking

of the pieces of a mystery images in mask of an alternate images called the target images preselected from a database. At the same time an undeniable shortcoming of Lai and Tsai is the necessity of an extensive images database with the goal that the created mosaic images can be sufficiently like the chose target images. Utilizing their strategy, the client is not permitted to choose openly his/her most loved images for utilization as the target images. It is consequently coveted in this study to evacuate this shortcoming of the system while keeping its legitimacy, that is, it is planned to outline another system that can change a mystery images into a secret fragment- noticeable mosaic images of the same size that has the visual appearance of any uninhibitedly chose target images without the need of a database. As delineation, Fig. 1 demonstrates a result yielded by the proposed system. Particularly, after a target images is chosen self-assertively, the given mystery images is initially partitioned into rectangular pieces called tile images, which then are fit into comparable obstructs in the target images, called target pieces, as indicated by a likeness standard focused around color varieties. Next, the color normal for each one tile images is changed to be that of the comparing target obstruct in the target images, coming about in a mosaic images which resembles the target images. Applicable plans are likewise proposed to lead almost lossless recuperation of the first mystery images from the ensuing mosaic images. The proposed technique is new in that a significant mosaic images is made, interestingly with the images encryption strategy that just makes pointless commotion Images. Likewise, the proposed technique can change a mystery images into a camouflaging mosaic images without squeezing, while an information concealing system must conceal an exceptionally compacted form of the mystery images into a spread images when the mystery images and the spread images have the same information..

II. LITERATURE SURVEY

Recently, many methods have been proposed for securing image transmission, for which two common approaches are image encryption and data hiding. Image encryption is a technique that makes use of the natural property of an image, such as high redundancy and strong spatial correlation, to get an encrypted image based on Shannon's confusion and diffusion properties .The encrypted image is a noise image so that no one can obtain the secret image from it unless he/she has the correct key. However, the encrypted image is a meaningless file, which cannot provide additional information before decryption and may arouse an attacker's attention during transmission due to its randomness in form. An alternative to avoid this problem is data hiding hides a secret message into a cove image so that no one can realize the existence of the secret data, in which the data type of the secret message investigated in this paper is an image. Existing data hiding methods mainly utilize the techniques of LSB substitution , histogram shifting , difference expansion , prediction-error expansion , recursive histogram modification ,and discrete cosine/wavelet transformations .However, in order to reduce the distortion of the resulting image, an upper bound for the distortion value is usually set on the payload of the cover image. A discussion on this rate distortion issue can be found previous. Thus, a main issue of the methods for hiding data in images is the difficulty to embed a large amount of message data into a single image. Specifically, if one wants to hide a secret image into a cover image with the same size, the secret image must be highly compressed in advance. For example, for a data hiding method with an embedding rate of 0.5 bits per pixel, a secret image with 8 bits per pixel must be compressed at a rate of at least 93.75% beforehand in order to be hidden into a cover image. But, for many applications, such as keeping or transmitting medical pictures, military images, legal documents, etc., that are valuable with no allowance of serious distortions, such data compression operations are usually impractical. Moreover, most image compression methods, such as JPEG compression, are not suitable for line drawings and textual graphics, in which sharp contrasts between adjacent pixels are often destructed to become noticeable arti facts.

III. PROPOSED METHOD

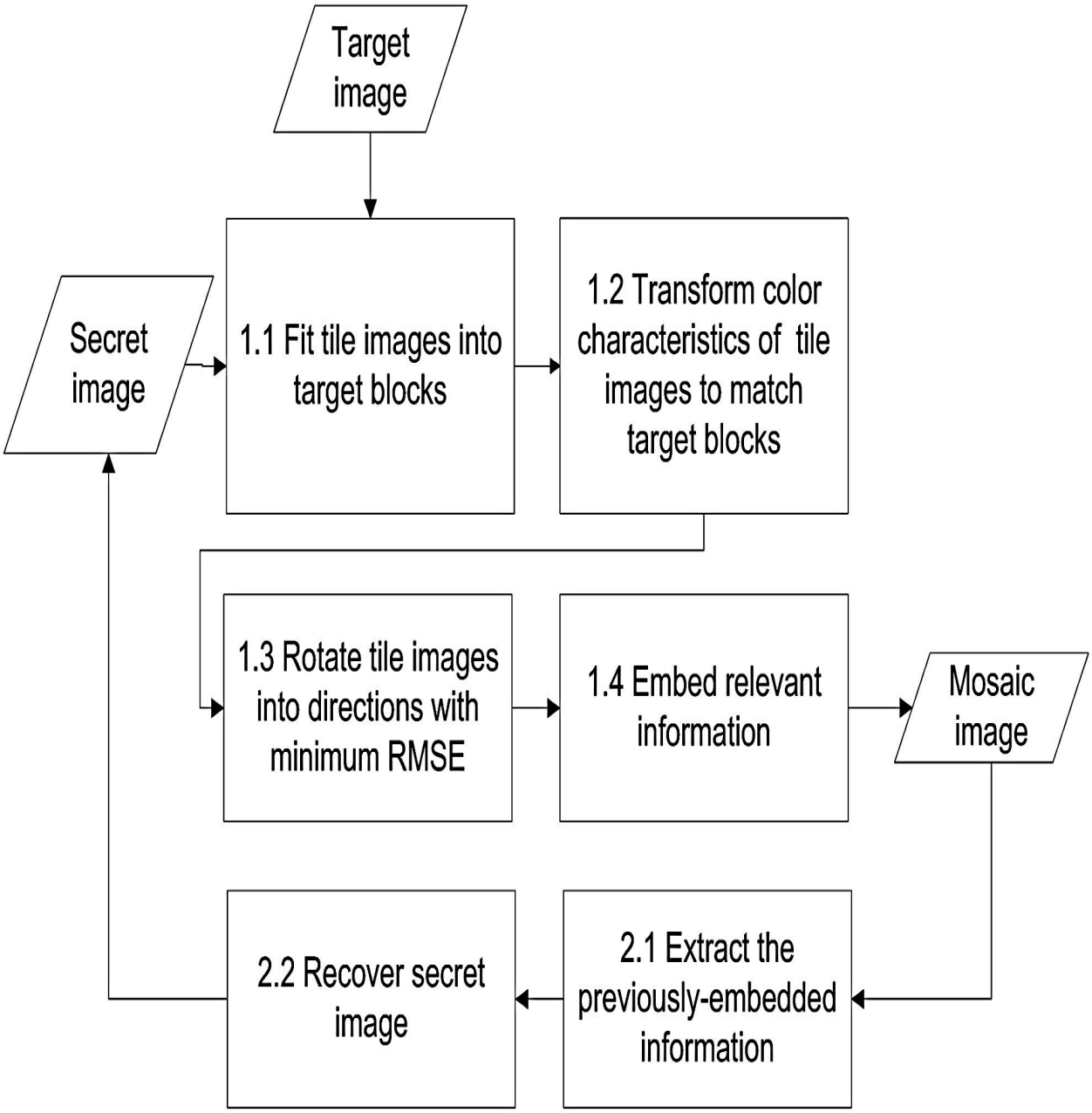
Another strategy for secure picture transmission is proposed, which changes a mystery picture into a significant mosaic picture with a similar size and resembling a preselected target picture. The change procedure is controlled by a mystery key, and just with the key can a man recoup the mystery picture about losslessly from the mosaic picture. The proposed strategy is enlivened by Lai and Tsai, in which a new sort of PC workmanship picture, called mystery piece unmistakable mosaic picture, was proposed. The mosaic picture is the aftereffect of revamp of the pieces of a mystery picture in camouflage of another picture called the objective picture preselected from a database. Be that as it may, a conspicuous shortcoming of Lai and Tsai is the necessity of a substantial picture database so that the created mosaic picture can be adequately like the chose target picture. Utilizing their technique, the client is not permitted to choose unreservedly his/her most loved picture for use as the objective picture.

It is thusly craved in this review to evacuate this shortcoming of the technique while keeping its legitimacy, that is, it is planned to outline another strategy that can change a mystery picture into a secret fragment- noticeable mosaic picture of a similar size that has

Volume 5 Issue IV, April 2017
ISSN: 2321-9653

the visual appearance of any uninhibitedly chose target picture without the need of a database.

The proposed technique incorporates two fundamental stages as appeared by the stream graph of Fig. 2: 1) mosaic picture creation and 2) mystery picture recuperation. Fig. 2. Stream graph of the proposed technique. In the main stage, a mosaic picture is yielded, which comprises of the sections of an information mystery picture with shading amendments as per a comparability measure in view of shading varieties. The stage incorporates four phases: 1) fitting the tile pictures of the mystery picture into the objective pieces of a preselected target picture; 2) changing the shading normal for each tile picture in the mystery picture to wind up noticeably that of the comparing target hinder in the objective picture; 3) pivoting each tile picture into a bearing with the base RMSE esteem with deference to its comparing target square; and 4) installing significant data into the made mosaic picture for future recuperation of the mystery picture. In the second stage, the inserted data is extricated to recoup about losslessly the mystery picture from the created mosaic picture. The stage incorporates two phases: 1) extricating the installed data for mystery picture recuperation from the mosaic picture, and 2) recouping the mystery picture utilizing the extricated data.



, Fig. Flow diagram of the proposed method

Volume 5 Issue IV, April 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

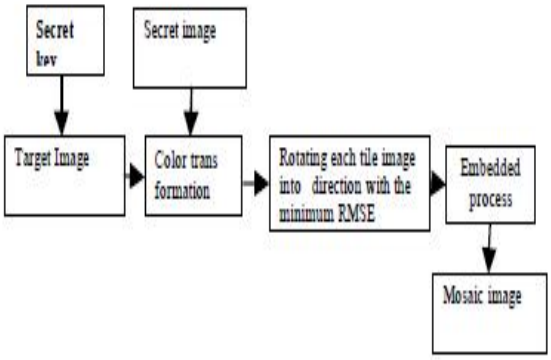


Figure1: Mosaic image creation block diagram

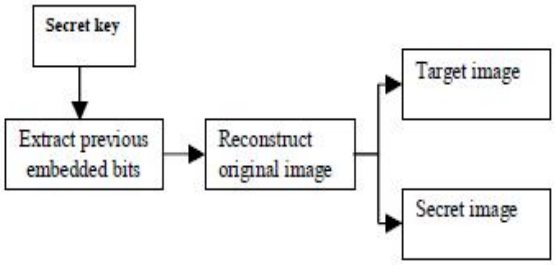
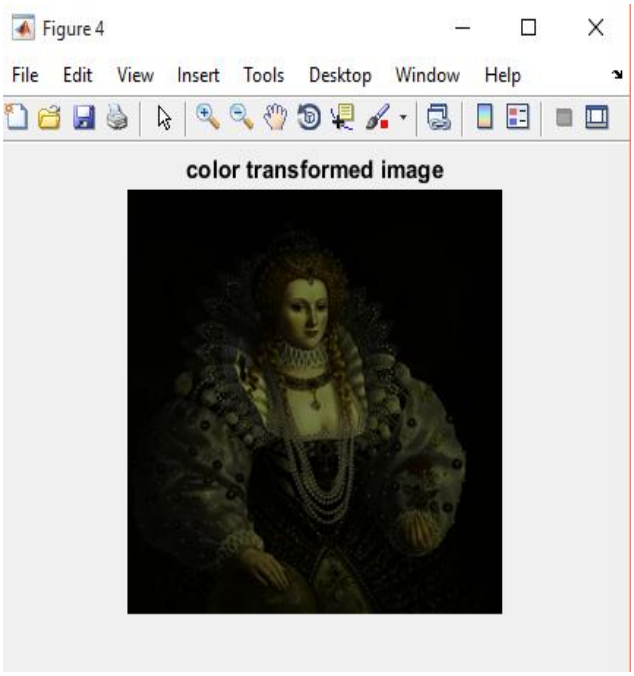
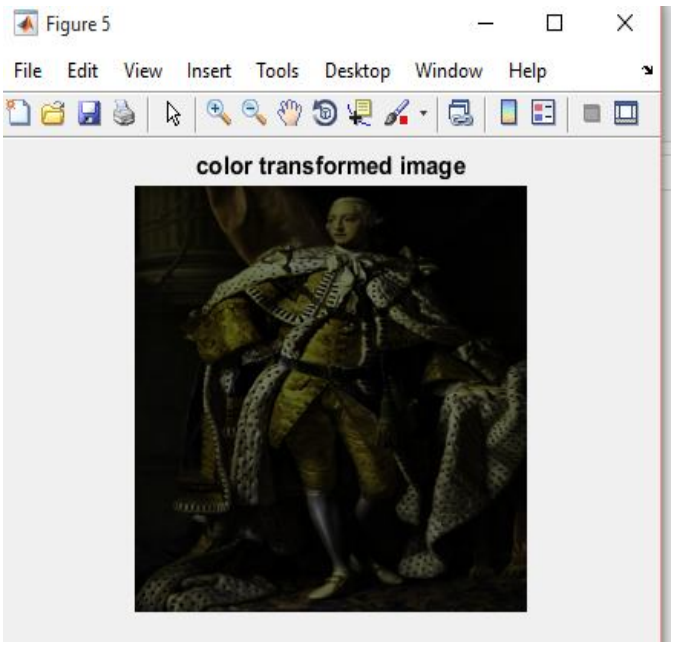


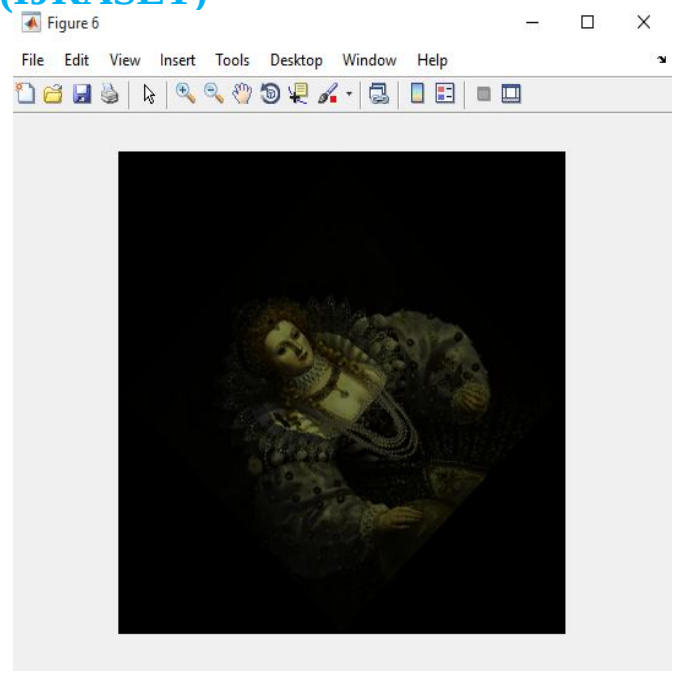
Figure: 2 Extract secret image and target image Block diagram

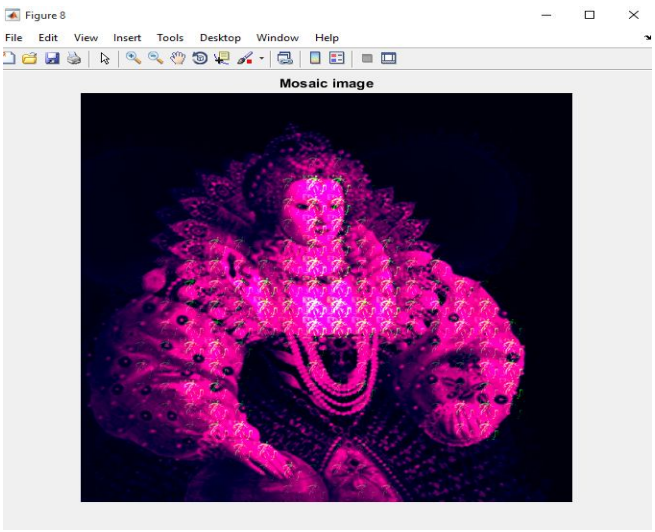
IV. SIMULATION RESULTS

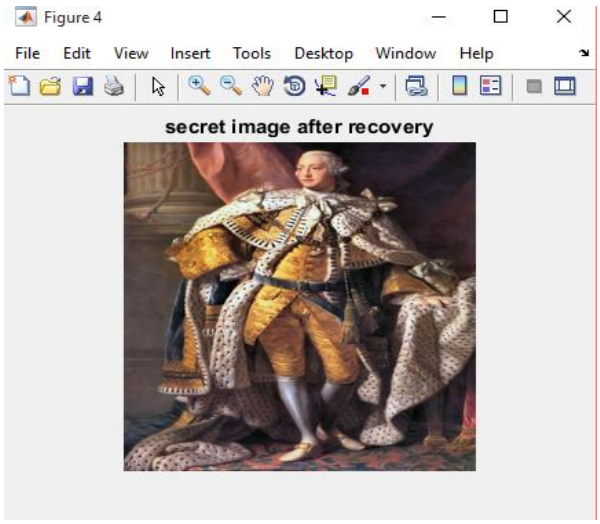


Volume 5 Issue IV, April 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)









Volume 5 Issue IV, April 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

V. CONCLUSION

Another secure Images transmission technique has been proposed, which not just can make genuine mosaic Images at the same time likewise can change a mystery Images into a mosaic one with the same information size for utilization as a disguise of the mystery Images. By the utilization of fitting pixel color changes and an adroit plan for taking care of floods and undercurrents in the changed over estimations of the pixels' colors, mystery fragment visible mosaic Images with high visual similitude's to subjectively chose target Images can be made with no need of a target Images database. Likewise, the first mystery Images can be recouped about losslessly from the made mosaic Images. Great test results have demonstrated the plausibility of the proposed technique. Future studies may be guided to applying the proposed technique to Images of shade models other than the RGB.

REFERENCES

[1] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," Int. J. Bifurcat. Chaos, vol. 8, no. 6, pp.1259–1284, 1998
[2] G. Chen,Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," Chaos Solit. Fract., vol. 21, no. 3, pp. 749–761, 2004
[3] L. H. Zhang, X. F. Liao, and X. B. Wang, "An image encryption approach based on chaotic maps," Chaos Solit. Fract., vol. 24, no. 3, pp. 759–765, 2005.
[4] H. S. Kwok and W. K. S. Tang, "A fast image encryption system based on chaotic maps with finite precision representation," Chaos Solit. Fract., vol. 32, no. 4, pp. 1518–1529, 2007.
[5] S. Behnia, A. Akhshani, H. Mahmodi, and A. Akhavan, "A novel algorithm for image encryption based on mixture of chaotic maps," Chaos Solit. Fract., vol. 35, no. 2, pp. 408–419, 2008.
[6] D. Xiao, X. Liao, and P. Wei, "Analysis and improvement of a chaosbased image encryption algorithm," Chaos Solit Fract., vol. 40, no. 5, pp. 2191–2199, 2009.
[7] V. Patidar, N. K. Pareek, G. Purohit, and K. K. Sud, "A robust and secure chaotic standard map based pseudorandom permutationsubstitution scheme for image encryption," Opt. Commun., vol. 284, no. 19, pp. 4331–4339, 2011
[8] C. K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," Pattern Recognit.., vol. 37, pp. 469– 474, Mar. 2004.
[9] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar. 2006.
[10] J. Tian, "Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol., vol. 13 no. 8, pp. 890–896, Aug. 2003.
[11] Y. Hu, H.-K. Lee, K. Chen, and J. Li, "Difference expansion based reversible data hiding using two embedding directions," IEEE Trans. Multimedia, vol. 10, no. 8, pp. 1500–1512, Dec. 2008.
[12] V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y.-Q. Shi, "Reversible watermarking algorithm using sorting and prediction," IEEE Trans. Circuits Syst. Video Technol., vol. 19, no. 7, pp. 989–999, Jul. 2009.
[13] X. Li, B. Yang, and T. Zeng, "Efficient reversible watermarking based on adaptive prediction-error expansion andpixel selection," IEEE Trans. Image Process., vol. 20, no. 12, pp. 3524–3533, Dec. 2011.
[14] W. Zhang, X. Hu, X. Li, and N. Yu, "Recursive histogram modification: Establishing equivalency between reversible data hiding and lossless data compression," IEEE Trans. Image Process., vol. 22, no. 7, pp. 2775–2785, Jul. 2013.
[15] J. Fridrich, M. Goljan, and R. Du, "Invertible authentication," Proc. SPIE, vol. 3971, 2001, pp. 197–208.
[16] C. C. Chang, C. C. Lin, C. S. Tseng, and W. L. Tai, "Reversible hiding in DCT-based compressed images," Inf. Sci., vol. 177, no. 13, pp. 2768–2786, 2007.
[17] S. Lee, C. D. Yoo, and T. Kalker, "Reversible image watermarking based on integer-to-integer wavelet transform," IEEE Trans. Inf. Forens. Secur., vol. 2, no. 3, pp. 321–330, Sep. 2007.
[18] W.-H. Lin, S.-J. Horng, T.-W. Kao, P. Fan, C.-L. Lee, and Y. Pan, "An efficient watermarking method based on significant difference of wavelet coefficient quantization," IEEE Trans. Multimedia, vol. 10, no. 5, pp. 746–757, Aug. 2008
[19] X. Hu, W. Zhang, X. Hu, N. Yu, X. Zhao, and F. Li, "Fast estimation of optimal marked-signal distribution for reversible data hiding," IEEE Trans. Inf. Forens. Secur., vol. 8, no. 5, pp. 187–193, May 2013.
[20] W. B. Pennebaker and J. L. Mitchell, JPEG: Still Image Data Compression Standard. New York, NY, USA: Van Reinhold, 1993, pp. 34–38.

BIBLIOGRAPHIES

K. Ayyanna completed his Master's Degree in Telematics and signal processing from National Institute of technology Rourkela and presently working as an Assistant Professor in Brindavan Institute of Technology and science,Kurnool,A.p His area of interest are signal processing, image processing,communication systems.He is a life time member of ISTE.

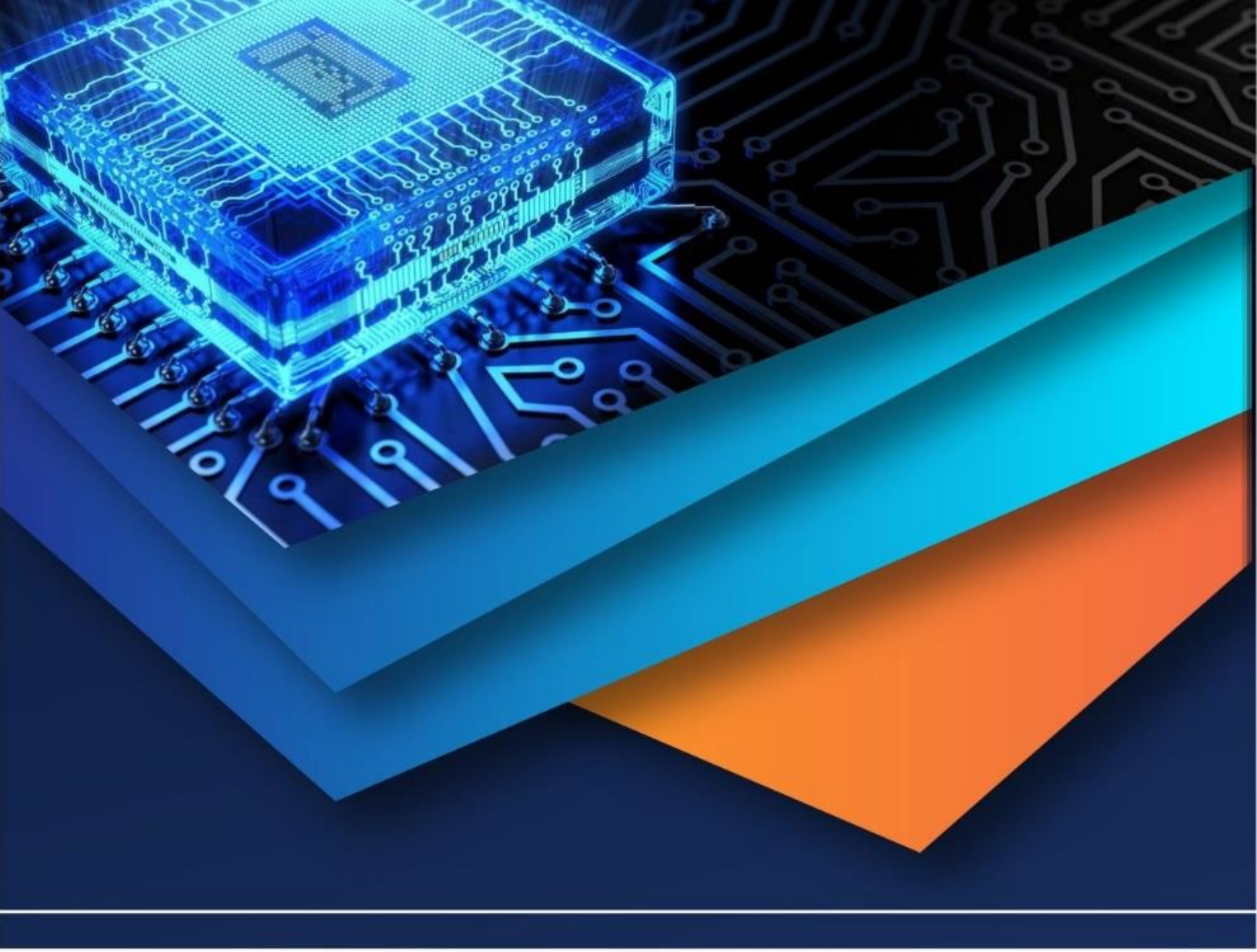
Volume 5 Issue IV, April 2017
ISSN: 2321-9653

K. Veeresh, pursuing B.tech from BITS-KNL, DEPT OF ECE, Kurnool.

K. Hymavathi, pursuing B.tech from BITS-KNL, DEPT OF ECE, Kurnool.

M. Mounica, pursuing B.tech from BITS-KNL, DEPT OF ECE, Kurnool.

J. Kalyan ,pursuing B.tech from BITS-KNL, DEPT OF ECE, Kurnool.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY