ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 9, September 2022

A Wavelet Based Digital Image Watermarking Technique through Encryption with DCT

[1] Manohar Gosul, [2] Nisarg Gandhewar

[1] Research Scholar, Department of CSE, Dr. A.P.J. Abdul Kalam University, Indore, Madhya Pradesh, India.
[2] Professor, Department of CSE, Dr. A.P.J. Abdul Kalam University, Indore, Madhya Pradesh, India.

Abstract*— Recently, due to the increase in popularity of the Internet, the problem of digital data security over the Internet is increasing at a phenomenal rate. Watermarking is used for various notable applications to secure digital data from unauthorized individuals. Digital image watermarking is an attractive research area since it protects the multimedia data from unauthorized access. Digital images are widely communicated over the internet. The security of digital images is an essential and challenging task on shared communication channel. In the era of big data and networking, it is necessary to develop a secure and robust digital watermarking scheme with high computational efficiency to protect copyrights of digital works. Digital watermarking is need for the security of digital images to achieve security goals, i.e. confidentiality, integrity and availability. With the use of sophisticated signal/image processing algorithms, manipulations and duplications of audio, images, and videos are much easier. Hence, content authentication through encryption and resistance to general attacks such as noise, compression, and geometric has become an urgent and important issue. Hence in this work a wavelet based digital image watermarking technique through encryption with DCT (Discrete Cosine Transform) is presented that can guarantee robustness of image against salt and pepper attack.

Keywords: Digital image watermarking, encryption, Discrete Cosine Transform, security and robustness.

I. INTRODUCTION

Multimedia technology is improving day by day. Therefore, it is easy to modify, duplicate, reproduce, and distribute the digital image during communications via local networks and throughout the Internet with low cost and immediate delivery without quality degradation. Image security and privacy are a significant concern for the multimedia revolution.

Due to the remarkable development of the Internet, users are now allowed easy storage, duplication, and distribution of digital data/contents for many applications. However, with the development of digital technology and networking, fast, accurate, and cheap digital transmission means bring opportunities to countless businesses but also pose new challenges, including infringement, piracy, and arbitrary tampering with digital products (such as electronic publications, audio, video, animation, and image products). This leads to the problems of digital information security and digital product copyright protection [1].

However, security and copyright protection of digital content is a challenging task in the current era. Identity theft, copyright violation, and ownership identification are growing crimes, and we have seen cybercrime in a general increase. Encryption, steganography, and watermarking are some popular techniques used to provide security for digital content [2]. Encryption techniques offer important security components such as confidentiality, integrity, and authentication of digital data. Encryption converts pixel/information values of the data into an unreadable secret code for unauthorized users. However, the data is insecure once it is decrypted. On the other hand, steganography is the science of hiding data in which the intended information is concealed in such a way that only the concerned communicating parties understand the concealed message. It offers a major advantage since the secret data is hidden within the host and exchanged without generating any kind of visible alert to the attackers. However, bandwidth constraints are a major drawback associated with steganography.

Due to the limitations mentioned thus far, digital watermarking has been developed by various authors to offer copyright protection and content authentication for digital content [3]. In this technique, different kinds of digital data are inserted into images for maintaining their security and privacy while the visual quality of the cover data is preserved. Furthermore, digital watermarking offers protection against tampering, access control, ownership authentication, non-repudiation, indexing, save memory, and bandwidth requirements.

Digital image watermarking is a significant advancement of technology in recent years for identifying ownership information of copyright holders and providing multimedia security [4]. This technology embeds the watermark data into a multimedia product (such as text, image, audio, and video) and later extracts or detects it from the watermarked product to assert the product.

This watermarking (data hiding) technique is the one in which we can add some multimedia image, audio, or video. Nowadays, watermarking is being used in each and every field, either the data are saved on cloud, screaming on television, printed on any piece of paper or the data are saved anywhere in any kind of form. This technique basically

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 9, September 2022

involves embedding secret information into the digital image which needs to be protected in the form of watermark such that the resulting image is resistant and robust to numerous standard data processing techniques such as filtering, re-sizing, and cropping to name a few. But with the advancement in technology, the integrity of schemes is also being compromised as attackers have developed techniques to discard the watermark to make it protected. A watermark thus should be added in a way that it remnants irremovable and perceptible as long as its enduring feature of the digital data and information remains standardized [5].

Watermark being the identity of the content owner needs protection even after removed from the original document or image or video. Encryption provides additional security to the original watermark image in the event of unauthorized watermark extraction and manipulation [6]. By the application of transforms such as DFT, DCT and DWT, watermarking can be applied in the frequency domain. Watermarking techniques using DCT are found to be more robust as compared to simple techniques applied in temporal domain. Transform domain algorithms are robust against common signal and image processing operations like contrast enhancement, low-pass filtering, brightness adjustment, blurring.

Hence in this paper, a wavelet based digital image watermarking technique through encryption with DCT is presented.

II. LITERATURE SURVEY

Nazir A. Loan, Nasir N. Hurrah, Shabir A. Parah, Jeon W. Lee, Javaid A. Sheikh et. al., [7] presents Secure and Robust Digital Image Watermarking using Coefficient Differencing and Chaotic Encryption. The host image is divided into 8×8 non-overlapping blocks prior to DCT application, and the watermark bit is embedded by modifying difference between DCT coefficients of adjacent blocks. Arnold Transform is used in addition to chaotic encryption to add double layer security to the watermark.

A.S.Kapse, Sharayu Belokar, Yogita Gorde, Radha Rane, Shrutika Yewtkar et. al., [8] presents Digital Image Security Using Digital Watermarking. Digital image safety and integrity the top prioritized issue in today's information explosion. Digital watermarking is an efficient solution to avoid illegal copying of information from multimedia networks. Robustness of watermark can be explained in terms of successful recovery of watermark from recovered content which may contain different types of noises and compression effects.

Mirza Abdur Razzaq, Mirza Adnan Baig, Ashfaque Ahmed Memon, Riaz Ahmed Shaikh et. al., [9] presents Digital Image Security: Fusion of Encryption, Steganography and Watermarking. It comprises of three key components: (1) the original image has been encrypted using large secret key by rotating pixel bits to right through XOR operation, (2) for steganography, encrypted image has been altered by least significant bits (LSBs) of the cover image and obtained stego image, then (3) stego image has been watermarked in the time domain and frequency domain to ensure the ownership.

Khalil Shekaramiz, Alireza Naghsh, Najafabad et. al., [10] presents Embedding and Extracting Two Separate Images Signal in Salt & Pepper Noises in Digital Images based on Watermarking. In this paper, we introduce a method for watermarking the two separate digital signals in six bits of applied salt & pepper noises to a digital image; since the salt & pepper noises are placed randomly throughout the image.

Mohammad Shahab Goli, Alireza Naghsh et. al., [11] presents Introducing a New Method Robust Against Crop Attack In Digital Image Watermarking Using Two-Step Sudoku. In this method, the watermark image is scattered in two sudoku table layouts with different solutions and is watermarked in the host image. Using this method, the watermark image is repeated 81 times in the host image, and to this effect the watermark image can be reconstructed using other segments when cropped by the attacker.

R. Surya Prakasa Rao, Dr. P. Rajesh Kumar et. al., [12] presents An Efficient Genetic Algorithm Based Gray scale Digital Image watermarking for Improving the Robustness and Imperceptibility. The Proposed Genetic Algorithm based Digital Image watermarking scheme is improved by embedding the watermark in Third Level DWT of original image, after applying Singular Value Decomposition (SVD) to watermark image. The Genetic Algorithm optimization technique (GA) is used for best scaling factor (SF) to modify the SVD coefficients of watermark image.

Lukman Çerkezi, Gökçen Çetinel et. al., [13] presents RDWT (Redundant Discrete Wavelet Transform) and SVD (Singular value Decomposition) Based Secure Digital Image Watermarking Using ACM (Arnold Cat Map). In the proposed watermarking scheme, RDWT is performed to decompose the cover image into four sub-bands. Then SVD is applied to the LL sub-band of the cover image. The chaotic watermark is generated by applying ACM to the original watermark.

Madhuri Rajawat, D S Tomar et. al., [14] presents A Secure Watermarking and Tampering detection technique on RGB Image using 2 Level Discrete Wavelet Transform (DWT). This paper presents digital watermarking for their classification, application, techniques, attacks and also tampering detection in digital watermarking. They proposed a new algorithm for digital watermarking and tampering detection technique, by combining these techniques, we can improve the security of image.

Asna Furqan, Munish Kumar et. al., [15] presents a Study and Analysis of Robust DWT-SVD Domain Based Digital Image Watermarking Technique Using MATLAB. This paper presents a robust and blind digital image watermarking

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 9, September 2022

technique to achieve copyright protection. In order to protect copyright material from illegal duplication, various technologies have been developed, like key-based cryptographic technique, digital watermarking etc.

III. DIGITAL IMAGE WATERMARKING TECHNIQUE THROUGH ENCRYPTION WITH DCT

In this work, a wavelet based digital watermarking technique through encryption with DCT is presented. The proposed watermarking embedding method is shown in Figure 1. There are various color spaces for representing a image. In the RGB color space, since each channel is highly correlated, this space is not suitable for watermarking applications. On the other hand, many studies related to watermarking prefer to consider the Y channel of the YUV color space as the embedding channel as the Y channel typically contains more bits than the other channels This means that the scheme of embedding watermark information in Y channel is more robust.

For these reasons, we select Y channel to embed a watermark. The detailed steps to embed the watermark bits are explained as follows: Extract the Y channel of the host image. To embed the watermark bits, the host image is converted into YCbCr channels, and the Y channel of the host image is extracted. Select the embedding blocks. The extracted Y channel is partitioned into non-overlapping blocks of size *S* x *S*. To improve the robustness of the proposed method against cropping attacks, the embedding blocks are randomly selected according to a given key. Next Calculate *D*(*p*; *q*). Using equation 3, we can calculate only *D*(*p*; *q*) without repeating from 0 to *M* -1 with *u* and *v*. then Calculate the variation value Δ by following two sub-steps

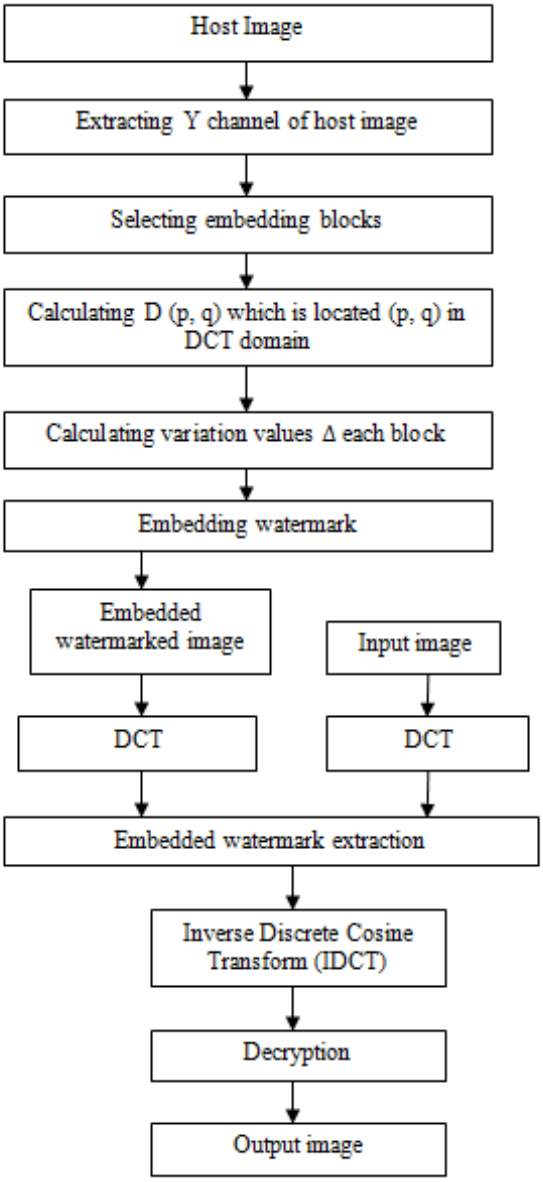


Figure. 1: flowchart of presented digital image watermarking technique

A watermark bit is embedded by adding the values calculated using the equation 1 according to Δ, to each pixel.

$$I^*(x,y) = I(x,y) + \frac{2}{M}c(p)c(q)\Delta\cos[p,x]\cos[q,y], \forall x, \forall y \ldots \quad (1)$$

Where, $I^*$is the watermarked image, I (*x*; *y*) is an element of the *x*-th row and the *y*-th column in image I . Furthermore, I^*(*x*; *y*) is an element of the *x*-th row and the *y*-th column in image I^*. Therefore, by adding the values calculated using Equation (1) to each pixel, it can be applied equally to an embedding watermark in the DCT domain. Moreover, as the proposed method has a simpler operation than the DCT, it can reduce the computational time, which is important for real-time watermarking.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 9, September 2022

The two sub-steps to calculate Δ are as follows and calculate D'. Suppose a watermark bit is w; then D', which will be embedded, is calculated according to the following rules, where $w \in \{0, 1\}$:

$$R = round\left(\frac{D(p,q)}{Q_{step}}\right) .. (2)$$

$$d = \begin{Bmatrix} \frac{Q_{step}}{2}, if\ (R\ mod\ 2) xor\ (w) = 0 \\ \frac{-Q_{step}}{2}, if\ (R\ mod\ 2) xor\ (w) = 1 \end{Bmatrix} (3)$$

$$D' = R \times Q_{step} + d \quad (4)$$

Here, mod represents a modular function and *Qstep* represents the quantization step. next Calculate Δ. The variation value Δ is calculated by using the following equation

$$\Delta = D' - D(p,q) \quad (5)$$

The watermark bit is embedded by adding the values obtained using equation (1) to all the pixels of the embedding block. This step provides a result equal to that of substituting D' with the DCT coefficient of (p; q). The abovementioned Steps are repeated to embed all the watermark bits into the host image.

A DCT expresses a finite sequence of data points in terms of the sum of the cosine functions oscillating at different frequencies. DCTs are important to numerous applications in science and engineering. The DCT of an image of size M x M is as follows:

$$D(p,q) = \frac{2}{M} c(p)c(q) \sum_{x}^{M} \sum_{y}^{M} I(x,y) cos_{p,x}\ cos_{q,y}\ \forall p, \forall y\ (6)$$

Assuming that the length of the image of size $M \times M$ is N; the direct application of equation (6) will require $O(N)$ operations. Lastly, the addition of the values to each pixel requires $O(N)$ operations. That is, the total computational complexity of the proposed method is $O(N)$. Therefore, the proposed method has lower complexity than other methods.

The original input image is decomposed using two-dimensional (2D) DCT to obtain the relevant scaled images with reduced size. Also, the encrypted watermark image is decomposed using 2D DCT to obtain decomposed scaled watermark images.

The watermark extraction is exactly reverse procedure of watermark embedding. The algorithm presented in this paper is non-blind and therefore requires original input image and encryption key for watermark extraction and detection. The similarity between the original watermark image and extracted watermark image is measured using three parameters: Mean Square Error (MSE), Normalized Correlation Coefficient (CC), and Peak Signal to Noise Ratio (PSNR). In general, value of CC > 0.75 and PSNR > 30 dB is considered acceptable. Also, it is necessary to evaluate these watermarking parameters at various signal processing attacks.

IV. RESULT ANALYSIS

In this section result analysis of presented wavelet based digital image watermarking technique through encryption with DCT is discussed. Here we used public datasets to easily compare the presented method to the earlier methods. CVG-UGR (4 of the test images from Computer Vision Group, University of Granada) and USC-SIPI (University of Southern California-Signal and Image Processing Institute) are used as the host images. Present watermarking technique is implemented using MATLAB. In this paper, Lena image and baboon image of size 90×90 are selected as input and watermark images which are shown in Fig. 2.

(a) (b)

Figure. 2: Original input images (a) baboon image and (b) lena image

The Fig. 3 shows the watermark extracted images of original images.

(a) (b)

Figure. 3: embedded watermark extracted images (a) lena imgae and (b) baboon image

The performance of the presented algorithm is evaluated through three parameters MSE, CC, and PSNR. Also, the comparison of the experimentally obtained parameters is performed under two different conditions with and without attacks. The general attacks such as salt-and-pepper noise is considered.

The mean square error between the original image D(p,q) and the reconstructed image O(p,q) is given by $MSE = \frac{1}{pq} \sum p, q\ (D\ (p,q) - O(p,q))^2$ (7)

Where, p and q represents the size of the Image.

PSNR is calculated to examine the quality of the watermarked image. The PSNR is expressed as

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 9, September 2022

$$PSNR = 10\ log \frac{(2^v - 1)^2}{MSE} \quad (8)$$

Here, 'v' is the minimum number of bits that can represent possible maximum intensity in a given image.

The Normalized Correlation coefficient is expressed as

$$CC = \frac{\sum_{x=1}^{m}\sum_{y=1}^{n} w(x,y) \times w*(x,y)}{\sum_{x=1}^{m}\sum_{y=1}^{n}[w(x,y) \times w*(x,y)]^2}$$

Where, w(x, y) is actual embedded image bits at coordinates (x,y) and w*(x, y) is the extracted logo bit at coordinates (x, y) and m×n is dimensions of image.

The table 1 represents the parameter evaluation of presented technique.

Table 1: Watermarking Parameters

Parameter	With salt and pepper noise	Without attacks
MSE for Lena image	0.12	0.10
PSNR (dB) for Lena Image	43.6	43.8
CC for Lena Image	0.89	0.91
MSE for Baboon image	0.14	0.11
PSNR for Baboon image	42.7	42.9
CC for baboon image	0.85	0.87

Presented technique has especially demonstrated better robustness against salt and pepper noise attack. Presented algorithm is simple to implement and provides some security to watermark through encryption key that can be suitable for applications such as Facebook and what's up that runs on android operating systems based devices.

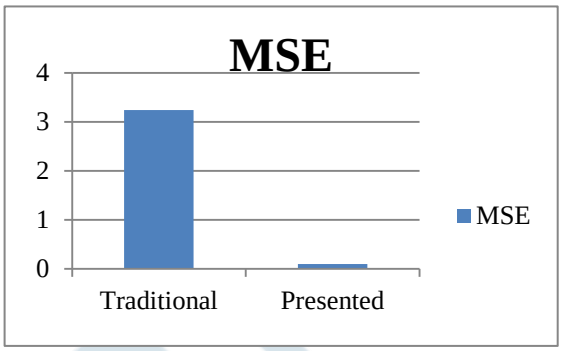
The watermarking parameters of presented watermarking technique through encryption with DCT and traditional watermarking technique is compared which is represented in table 2.

Table 2: Performance Comparison

Watermarking techniques	MSE	PSNR
Earlier watermarking technique	3.24	36.7
Presented wavelet based digital image watermarking technique	0.10	43.1

As can be seen from Table 2, the average PSNR of the presented method is more than 42 dB, and the MSE of the proposed method is <1. That is, the proposed method showed better effectiveness for digital image watermarking.

The comparison of MSE between traditional and presented watermarking technique is shown in Fig. 4.



The presented watermarking technique has greater MSE than earlier approach. Therefore presented wavelet based digital image watermarking through encryption with DCT have greater results in terms of MSE, CC and PSNR.

V. CONCLUSION

In this work a wavelet based digital image watermarking technique through encryption with DCT is presented that guarantee the robustness against salt and pepper attack. Through the experiments, appropriate parameter set is selected and investigated the performance metrics like PSNR (Peak Signal to Noise Ratio), Mean Square Error, Normalized Correlation Coefficient (CC) to evaluate the performance of presented technique. Furthermore, we investigated the robustness for salt and pepper watermark attack. When the image is not attacked, the watermark information can be extracted completely. The watermark detected by this algorithm is more similar to the original watermark. The watermark has strong robustness and can resist different attacks. The results showed that the presented technique has the most robust performance through tests using two publicly available datasets. The robustness of presented technique is compared with traditional watermarking techniques. Compared to traditional methods, presented technique has better results in terms of MSE, CC and PSNR.

REFERENCES

[1] Lei Pei, "Research on Digital Image Watermarking Algorithm Based on Scrambling and Singular Value Decomposition", Hindawi Journal of Mathematics Volume 2022, Article ID 4656010, 10 pages, doi.org/10.1155/2022/4656010

[2] A. K. Singh, S. Thakur, Alireza Jolfaei, Gautam Srivastava, "Joint Encryption and Compression-Based Watermarking Technique for Security of Digital Documents", ACM Transactions on Internet Technology, Vol. 21, No. 1, Article 18, 2021, doi.org/10.1145/3414474

[3] Sowmya S, Sahana Karanth , Sharath Kumar, "Protection of data using image watermarking technique", Global

Transitions Proceedings 2 (2021) 386–391, Elsevier B.V, doi: 10.1016/j.gltp.2021.08. 035

[4] Mahbuba Begum and Mohammad Shorif Uddin, "Analysis of Digital Image Watermarking Techniques through Hybrid Methods", Hindawi, Advances in Multimedia Volume 2020, Article ID 7912690, 12 pages, doi.org/10.1155/2020/7912690

[5] Kamal Nayan Kaur, Divya, Ishu Gupta and Ashutosh Kumar Singh, "Digital Image Watermarking Using (2, 2) Visual Cryptography with DWT-SVD Based Watermarking", Springer Nature Singapore Pte Ltd. 2019, doi.org/10.1007/ 978-981-10-8055-5_8

[6] Sarita P. Ambadekar, Jayshree Jain and Jayshree Khanapuri, "Digital Image Watermarking Through Encryption and DWT for Copyright Protection", Springer Nature Singapore Pte Ltd. 2019, doi. org/10.1007/978-981-10-8863-6_19

[7] Nazir A. Loan, Nasir N. Hurrah, Shabir A. Parah, Jeon W. Lee, Javaid A. Sheikh, " Secure and Robust Digital Image Watermarking using Coefficient Differencing and Chaotic Encryption", Information Security Solutions for Telemedicine Applications, IEEE ACCESS, Volume 6, 2018, doi:10.1109/ ACCESS.2018.2808172

[8] A.S.Kapse, Sharayu Belokar, Yogita Gorde, Radha Rane, Shrutika Yewtkar, "Digital Image Security Using Digital Watermarking", International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056, Volume: 05 Issue: 03, 2018

[9] Mirza Abdur Razzaq, Mirza Adnan Baig, Ashfaque Ahmed Memon, Riaz Ahmed Shaikh, " Digital Image Security: Fusion of Encryption, Steganography and Watermarking", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 5, 2017

[10] Khalil Shekaramiz, Alireza Naghsh, Najafabad, "Embedding and Extracting Two Separate Images Signal in Salt & Pepper Noises in Digital Images based on Watermarking", 3rd International Conference on Pattern Recognition and Image Analysis (IPRIA 2017) April 19-20, 2017

[11] Mohammad Shahab Goli, Alireza Naghsh, "Introducing a New Method Robust Against Crop Attack In Digital Image Watermarking Using Two-Step Sudoku", 3rd International Conference on Pattern Recognition and Image Analysis (IPRIA 2017) April 19-20, 2017, 978-1-5090-6454-0/17

[12] R. Surya Prakasa Rao, Dr. P. Rajesh Kumar, "An Efficient Genetic Algorithm Based Gray scale Digital Image watermarking for Improving the Robustness and Imperceptibility", International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) – 2016, 978-1-4673-9939-5/16

[13] Lukman Çerkezi, Gökçen Çetinel, "RDWT and SVD Based Secure Digital Image Watermarking Using ACM", 978-1-5090-1679-2/16, 2016 IEEE

[14] Madhuri Rajawat, D S Tomar, "A Secure Watermarking and Tampering detection technique on RGB Image using 2 Level DWT", 2015 Fifth International Conference on Communication Systems and Network Technologies, 978-1-4799-1797-6/15, DOI 10.1109/CSNT.2015.245

[15] Asna Furqan, Munish Kumar, "Study and Analysis of Robust DWT-SVD Domain Based Digital Image Watermarking Technique Using MATLAB", 2015 IEEE International Conference on Computational Intelligence & Communication Technology, 978-1-4799-6023-1/15, DOI 10.1109/CICT. 2015.74