Asian Journal of Electrical Sciences
ISSN: 2249-6297 (P) Vol.6 No.1, 2017, pp.1-6
© The Research Publication, www.trp.org.in
DOI: https://doi.org/10.51983/ajes-2017.6.1.1996

A New Encryption and Decryption for 3D MRT Images

Pala Mahesh Kumar
SAK Informatics Pvt. Ltd., Hyderabad, Telangana, India
E-mail: maheshbabu2529@gmail.com

(Received 15 December 2016; Revised 31 December 2016; Accepted 23 January 2017; Available online 30 January 2017)

***Abstract* - Recent years there is a fast development in remote technologies, consistently G-bytes of information hosts been trading between the gatherings. Secure transmission of information is an exceptionally difficult undertaking for private applications, for example, military, common, medicinal and web applications. Here, we expected to present "A New Encryption and Decryption for 3D MRT Images". Our proposed algorithm has shown the robustness over conventional algorithms in terms of secure concern.**

***Keywords:* Image Encryption and Decryption, AES, DES, Edge map.**

I. INTRODUCTION

The vast majority of the media services and remote system technologies were giving ubiquitous comforts to sharing, gathering or appropriating pictures or videos over cell mobile systems, informal communities, for example, WeChat, WhatsApp, face book and so forth, remote open channels and multimedia systems for some organizations and people. Late years there is a quick development in digital information sharing, for example, digital pictures or digital videos. Digital information sharing will be done in different applications, each of them have to transmit the information safely without knowing not unauthorized individual or gathering. For the applications like stockpiling and transmission securing a picture is a testing assignment. For instance, numerous strategic spots like business focuses, budgetary focuses and open transportations will be observed by digital video reconnaissance systems with the end goal of country security. Consistently there is a lot of pictures and videos with secure information, which does not known by unauthorized people have been generated, transmitted or reestablished. Notwithstanding this current, patient's records in restorative pictures, for example, Magnetic Resonance (MR) or Computed Tomography (CT) and medicinal sign reports, for example, electro cardiogram (ECG) or electro encephalogram (EEG) will be shared among the majority of the specialists from various branches of health service organizations (HSO) over remote systems for analysis reason. All these therapeutic pictures, signals and digital videos may contain some private information, which is more secret. Consequently, it is a critical errand to give security to this kind of pictures and videos. Numerous applications, for example, restorative, military, development businesses, style plan enterprises and automobile ventures require filtered information, blue prints and outlines to be ensured against undercover work.

Creating and utilizing plans to upgrade the lifetime of digital pictures or videos is an essential, basic and testing errand, which ensures the substance of unique information for a long time [1]. To ensure a picture or video encryption is a powerful approach [1], which transforms the picture or video into various arrangement. As of late there are such a variety of algorithm has been created to give more security, upgraded quality with simple usage and quicker figuring's. Among every one of them of the techniques have their own particular downsides like computational multifaceted nature, time utilization, not appropriate for 3D pictures and so on., To beat every one of the disadvantages here in the proposed framework we presented another technique called A New Encryption and Decryption for Color Images Using Combined Key Generation that utilizes two mystery key pictures and logical scrambling operation, which will give more security by creating two mystery keys.

II. LITERATURE REVIEW

From the previous decades there are such a large number of picture cryptographic algorithms have been created to shield the pictures from unauthorized gatherings, which were hoping to pulverize the information sent by transmitter. In 1995 the principal picture and video encryption: from digital rights administration to secured personal communication distributed by Pommer Andreas and Uhl Andreas. In [1] the creators said that an incorporated outline of plans for encryption of pictures and videos will be given by picture and video encryption. This reaches from couple of business applications like digital video broadcasting (DVB) or digital audio broadcasting (DAB) to more research situated points and distributed substance. The idea in [2] was distributed by B. Schineir, in which the theorital and viable learning of a cryptosystem has been given to secure the multimedia. It was presented in 1995 and soon it turned into the standard reading material for cryptography courses in everywhere throughout the world. The creator in [3] proposed another invertible 2D map, called Line map, for encryption and decoding of picture, which maps a picture into a variety of pixels and after that maps it back to the first picture. This methodology demonstrates the preferred execution over the beforehand existed 2D maps, in which just change was utilized. Another methodology for picture encryption in [4], which is proposed by kuang tsan lin, this methodology used the both enchantment network scrambling and binary coding technique to shape a half breed encoding strategy to scramble a picture. This won't give any kind of contortion in decoding process, which means that the precise unique picture will be recuperated at the collector end. Anil kumar et. al. in [5] presented another picture encryption technique in light of disordered standard guide which utilizes expanded substitution-dispersion plan. This strategy utilizes straight input shift register to conquer the downsides of existing techniques by including non-linearity. This methodology is very secured and speedier than the customary strategies. Zhi liang zhu et. al. [6] presented a tumult based symmetric picture encryption utilizing a bit level change, in which the Arnold feline guide for bit level stage proposed for a picture cryptosystem to give more security and speedier reproductions. A successful, secured, quick and savvy picture transmission plan proposed in [7] utilizes encryption, compression and secured key trading alongside the picture transmission. As of late, a picture encryption plan taking into account partial Fourier transform (FRFT), solitary worth disintegration and Arnold transform has been proposed in [10] to enhance the security to improve the nature of decrypted picture. Picture encryption technique utilizing bit plane deterioration and scrambling was proposed by qiudong sun [8], which goes for the pixels positions exchanging and changing the dim estimations of pixels in the meantime. This methodology has preferable proficiency and properties over the arbitrary scrambling techniques and it has more stability degree than the traditional strategies, for example, Arnold transform.

III. EXISTING ALGORITHM

The edge mapping will be used in many applications such as image enhancement, segmentation, compression, and recognition. It can also be used in image encryption. This section deals with the existing image encryption and decryption algorithm which is known as an edge map crypt algorithm. Here key will be assumed from edge map, such key image will be generated from another image with the same size as the source image using a particular edge mapping detector such as canny, sobel and prewitt etc., with a selected threshold value.

Algorithm:

Step1: First the input original image will be decomposed into binary bit planes.
Step2: Key image will be generated by applying edge map detector to the other image with the same size of original image.
Step3: Each of them is encrypted by performing an XOR operation with the key-image, which is an edge map created from another image.
Step4: Next, the algorithm inverts the order of all XORed bit planes and combines them together.
Step5: The resulting image is scrambled by using a selected scrambling algorithm to generate the final resulting encrypted image.

The Edgemap Crypt algorithm is illustrated in Fig. 2. Similar to the Bitplane Crypt algorithm, a 3D image can be encrypted by applying the Edgemap Crypt algorithm to all its 2D components individually. The key image will be generated from any of new or existing image with the same size of the original image. It might be an image that can be generated by the user or in the public online database. Conventional edge detectors such as canny, sobel and prewitt etc., can be used to generate an edge mapped image which will have pixel values as only zeros and ones. This algorithm provides flexibility to the user to choose any image and any edge map detector with any threshold value to generate the edge mapped image which is used as a key-image. They also provide the flexibility to use any conventional scrambling scheme. Therefore, the security keys for this algorithm consist of the image or its location which is used to generate the edge map, the type of the edge detector, the edge detector’s threshold, and the security keys of the scrambling algorithm.

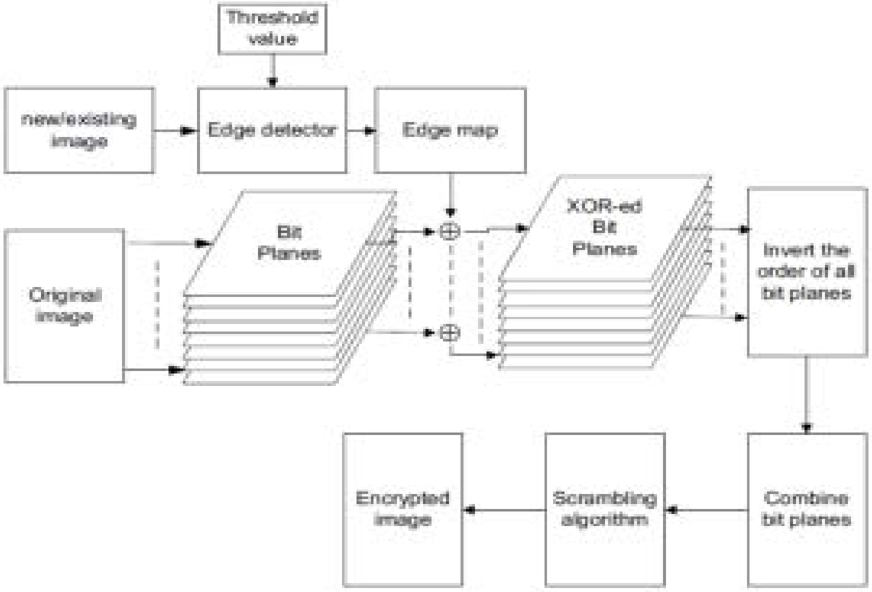


Fig.1 Block diagram of edgemap crypt algorithm

To reconstruct the original image, the users should be provided the security keys which help them to obtain the correct edge map. The decryption process first generates the edge map from the selected image using the security keys. It then unscrambles the encrypted image using the selected scrambling algorithm. Next, it decomposes the unscrambled image into its binary bit planes and performs XOR operation between the edge map and each bit plane. The order of all bit planes is restored to the original order. The reconstructed 2D image/component can be obtained by combining all bit planes.

IV. PROPOSED SYSTEM

Here, we are going to implement the new image encryption and decryption algorithm in such a way that it allows to . encrypt and decrypt both 3D images i.e., Key image and Original image and more importantly, we had implemented new combined key generation (CKG) scheme that uses two key images for improving the security.

A. Encryption Algorithm

Step 1: Select and read 3D MRT image to be encrypted
Step 2: Now, convert the image into number of bit planes using bit plane algorithm
Step 3: Now select and read the two key images with the same size of input image.
Step 4: Convert the key images into binary format
Step 5: Now, apply combined key generation to the new key image by considering XOR, AND, XNOR, and OR operations for the encryption based on user's choice.

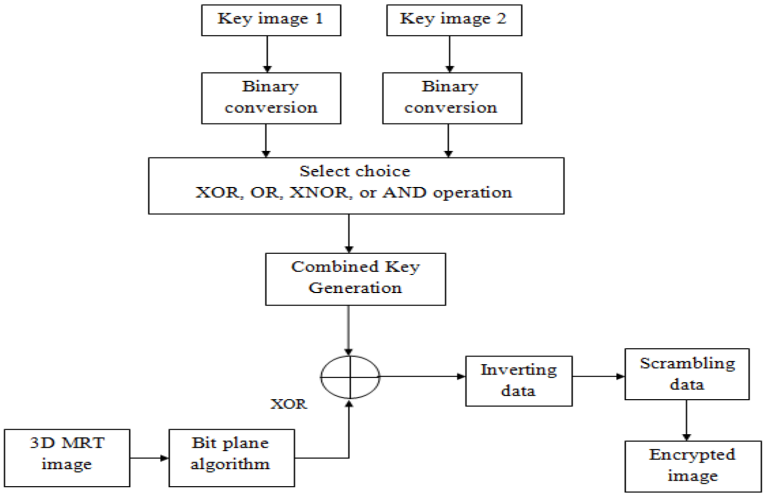


Fig.2 Block diagram of proposed EM-CKG encryption

Step 6: Then do the XOR of bit planes of original MRT image with the new key image.
Step 7: Then the XORed image will be inverted i.e., the bit planes of image will be shuffled for improving the security.
Step 8: Then we had done scrambling operation for more security concern using number to string and binary to decimal operations.
Step 9: Finally, we had a fully encrypted 3D MRT image with the CKG algorithm.

B. Bitplane Algorithm

A bit plane of a digital discrete signal (such as image or sound) is a set of bits corresponding to a given bit position in each of the binary numbers representing the signal.

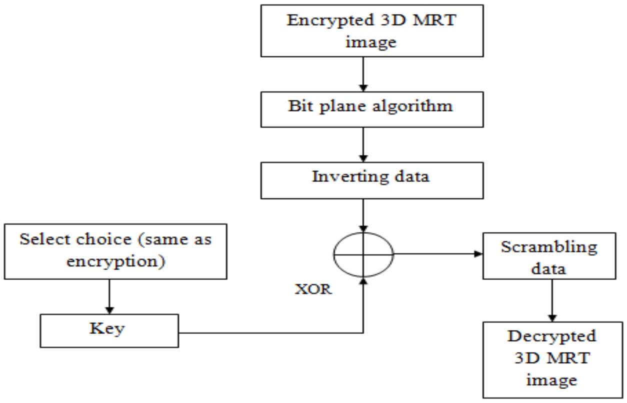
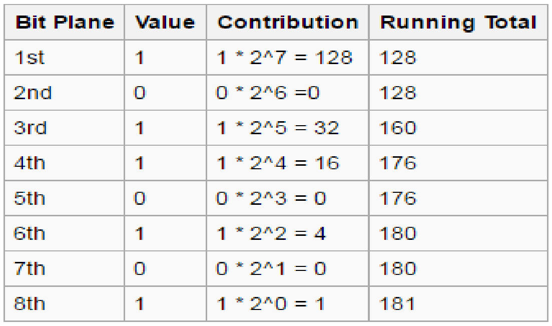


Fig.3 Proposed decryption algorithm

For example, for 16-bit data representation there are 16 bit planes: the first bit plane contains the set of the most significant bit, and the 16th contains the least significant bit. It is possible to see that the first bit plane gives the roughest but the most critical approximation of values of a medium, and the higher the number of the bit plane, the less is its contribution to the final stage. Thus, adding a bit plane gives a better approximation. If a bit on the nth bit plane on an m-bit dataset is set to 1, it contributes a value of $2^{(m-n)}$, otherwise it contributes nothing. Therefore, bit planes can contribute half of the value of the previous bit plane. For example, in the 8-bit value 10110101 (181 in decimal) the bit planes work as follows:

TABLE I BIT PLANE WORK



Bit Plane	Value	Contribution	Running Total
1st	1	1 * 2^7 = 128	128
2nd	0	0 * 2^6 =0	128
3rd	1	1 * 2^5 = 32	160
4th	1	1 * 2^4 = 16	176
5th	0	0 * 2^3 = 0	176
6th	1	1 * 2^2 = 4	180
7th	0	0 * 2^1 = 0	180
8th	1	1 * 2^0 = 1	181

Bitplane is sometimes used as synonymous to Bitmap; however, technically the former refers to the location of the data in memory and the latter to the data itself. One aspect of using bit-planes is determining whether a bit-plane is random noise or contains significant information. One method for calculating this is compare each pixel (X,Y) to three adjacent pixels (X-1,Y), (X,Y-1) and (X-1,Y-1). If the pixel is the same as at least two of the three adjacent pixels, it is not noise. A noisy bit-plane will have 49% to 51% pixels that are noise.

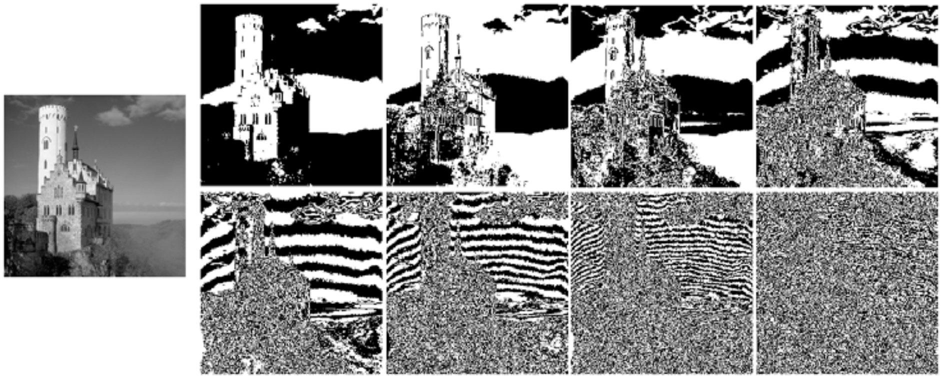


Fig.4 Example of a gray scale image bit planes

C. Inverting

Inversion is done by using a command *"fliplr"*, which is used to flip an array form left to right. This process is used to provide more secure concern to encrypted image after applying logical operations.

D. Scrambling Algorithm

Here, the scrambling is done by using number to string and binary to decimal operations

V. EXPERIMENTAL RESULTS

In this section we are going to discuss the performance analysis of conventional and proposed algorithms for both gray scale and true color images. Experiments have been done on multiple images taken from the websites, databases and various sites. Fig5 show that the original lena.jpg image has been encrypted with key matrices i.e., image baboon.jpg, which is a gray scale image, we can see that the encrypted image will not be decrypted if the key matrix is not available.

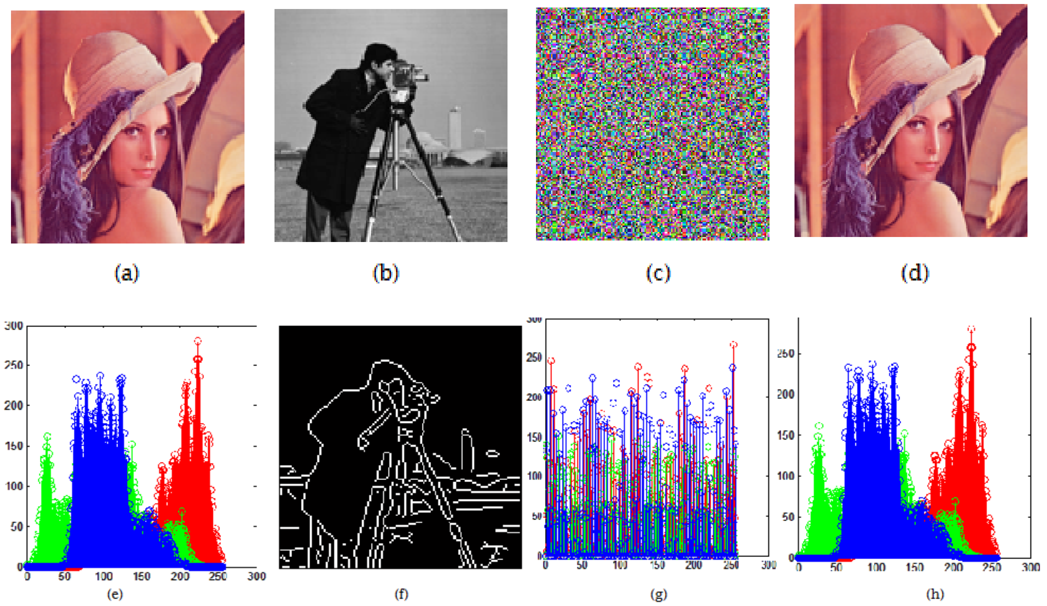


Fig.5.1 Color Image Encryption using Edgemap Crypt Algorithm (A) Original Image (B) Key Image (C) Encrypted Image (D) Decrypted Image (E) Histogram of Original Image (F) Edgemap of Key Image (G) Histogram of Encrypted Image and (H) Histogram of Decrypted Image

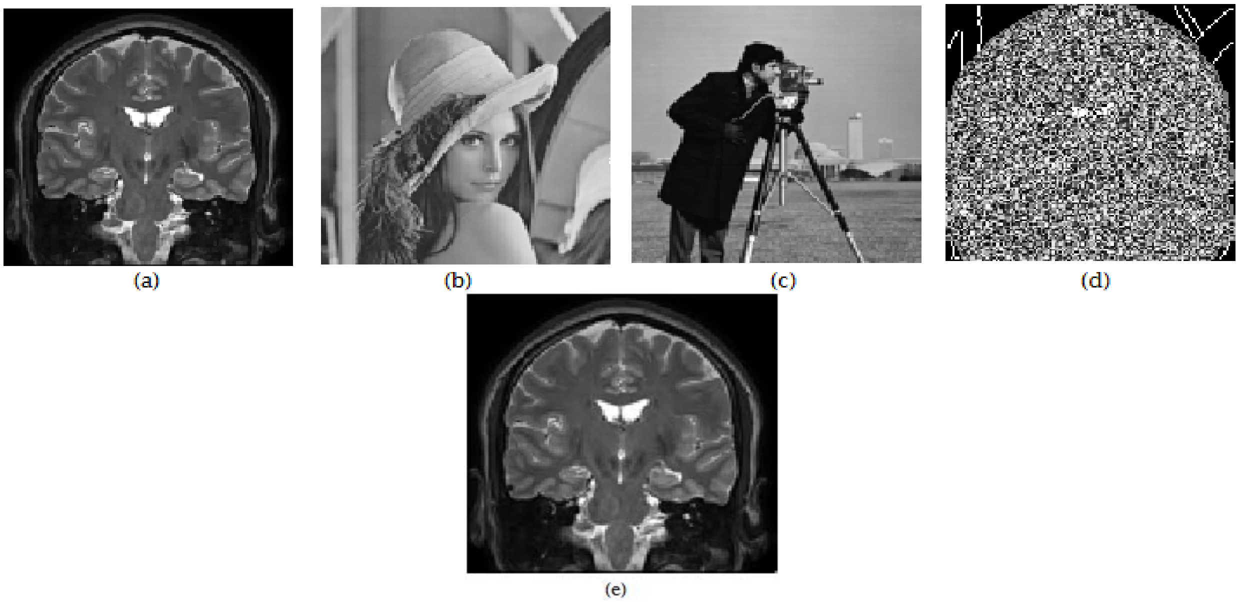


Fig.5.2. (a) original 3D MRT image (b) key image 1 (c) key image 2 (d) encrypted image and (e) decrypted image

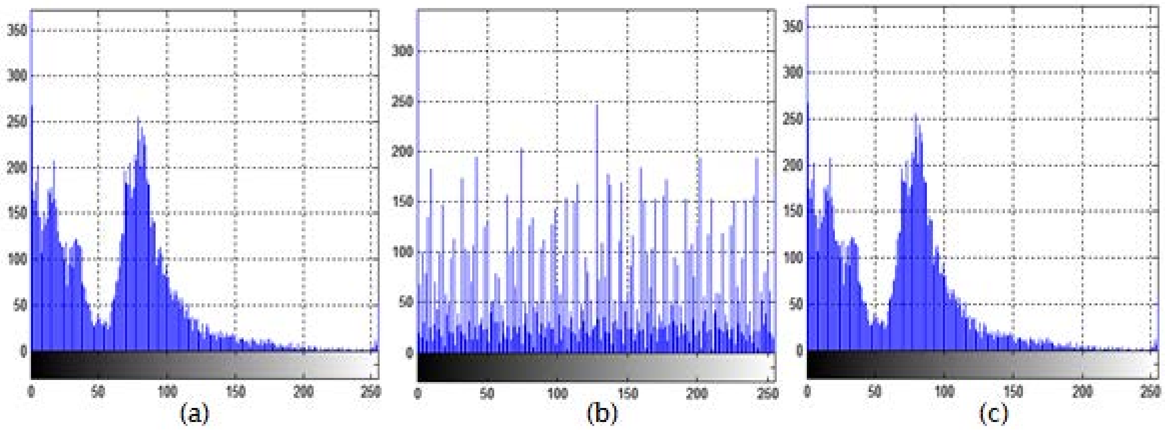


Fig.5.3. (a) histogram of original 3D MRT image (b) histogram of encrypted 3D MRT image and (c) histogram of decrypted 3D MRT image

The decrypted image is almost equal to the original image which has been encrypted by using edgemap crypt algorithm. In fig6 we displayed the edgemap crypt algorithm results with true color image.

VI. CONCLUSION

In this article, we introduced a new encryption and decryption algorithm for 3D MRT images using combined key generation (CKG) with logical operations and scrambling approaches. The proposed algorithm has many advantages over existing single key image algorithm which is known as edge map crypt algorithm. The security concern has been improved effectively. It is very easy to implement in hardware because they operate at the binary levels. They are also suitable for multimedia protection in real-time applications such as wireless networks and mobile phone services.

REFERENCES

[1] A. Pommer, A. Uhl, "Image and video encryption: from digital rights management to secured personal communication", Advances in Information Security, Vol. 15, 161p., 2005

[2] B. Schneier.: Cryptography: Theory and Practice, CRC Press, Boca Raton, 1995.

[3] Yong Feng, Xinghuo Yu, "A Novel symmetric image encryption approach based on an invertible two dimensional map". *35th Annual Conference on Industrial Electronics*, pp.1973-1978, 2009.

[4] Kuang Tsan Lin, "*Hybrid encoding method by assembling the magic-matrix scrambling method and the binary encoding method in image hiding*", Optics Communications, Vol. 284, pp. 1778-1784, 2011.

[5] Anil Kumar and M. K. Ghose, "*Extended substitution-diffusion based image cipher using chaotic standard map*", Communication in Nonlinear Science and Numerical Simulation, Vol.16, Issue 1, pp. 372-382, 2011.

[6] Zhi-liang Zhu, Wei Zhang, Kwok-wo Wong and Hai Yu, "*A chaos-based symmetric image encryption scheme using a bit-level permutation*", Information Sciences, Vol. 181, pp. 1171-1186, 2011.

[7] Kamlesh Gupta and Sanjay Silakari, "*Novel Approach for fast Compressed Hybrid color image Cryptosystem*", Advances in Engineering Software, Vol.49, pp. 29-42, 2012.

[8] Qiudong Sun, Wenying Yan, Jiangwei Huang and Wenxin Ma, "Image encryption based on bit-plane decomposition and random scrambling". *2nd International Conference on Consumer Electronics, Communications and Network*, pp. 2630-2633, 2012.

[9] Y. Zhou, K. Panetta, S. Agaian and C. L. Philip Chen, *"Image encryption using P-Fibonacci transform and decomposition"*, Optics Communications, Vol. 285, pp. 594-608, 2012.

[10] A Linfei Chen, Daomu Zhao and Fan Ge, "*Image encryption based on singular value decomposition and Arnold transform in fractional domain*", Optics Communications, Vol.291, pp. 98-103, 2013.

[11] V S Giridhar Akula, *"A Novel Approach to Encrypt and Decrypt Color images"*, Asian Journal of Computer Science and Technology, The Research Publication, Vol.4, No.2, 2015, pp. 13-17.