International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org
Volume 7, Issue 4, April 2018 **ISSN 2319 - 4847**

An Approach for Image Encryption based on Partitioning of Bit Pattern

Miss. Ankita P. Pande

M.E. (CSE), Prof. Ram Meghe College of Engineering & Management, Amravati, Maharashtra, India.

ABSTRACT

Nowadays, the safety of digital images draws much concentration due to the fast progress of an information technology and the computer networks. Therefore, for protecting such images during transmission and storage, I have proposed a new secret key image encryption approach by using block-based image transformation. Proposed encryption approach is based on partitioning of a bit pattern where the target image is simply encrypted by dividing it into 8×8 blocks without any overlapping and converting each block of an image into other form. At the receiver side, target image is recovered from the scrambled image by applying the exactly inverse method. Different experimentations are carried out on different images like Lena.jpg, Babbon.png, Jetplane.tif, etc. to verify the effectiveness of the proposed approach. The experimental outputs of the proposed approach shows that the correlation between image pixels is noticeably reduced by using the proposed algorithm. The experimental outputs also shows the good entropy value of an obtained encrypted image and thus provides good level of image security.

Keywords: Image encryption, Image Transformation, Image correlation, Image entropy.

1. INTRODUCTION

The fast progress of an information technology allow digital images to be easily communicated over the Internet in an open network and hence chances of leakage also increased. Hence, such images must be protected from leakages as these images might contain either private or confidential data. There are various areas where high image security is required such as satellite image, medical imaging, military database and services, etc. Hence, the need of using some security techniques arises.

Currently, various security approaches are available for securing images during transmission, for which image encryption and image steganography [1]-[3] are the preferred approaches and each of these approach offers different level of image security. Image Steganography is a data hiding technique, where a secret target data is totally hidden into a cover media such that an intruder will not be aware of the presence of the hidden data. A key problem of image steganography is struggling to insert a large amount of data into a cover image of same size. In this case, the secret target image must be greatly compressed before hiding into any cover image. But, this could result in distorted image and there are many applications, such as military images, medical images where distortions are not acceptable, hence such data compression are generally unfeasible. Another technique for providing image security and avoiding the limitation of data hiding is image encryption [4]-[7]. There are several image encryption methods presented in the mid of 1990s. Particular image encryption method provides acceptable image quality at the receiver side whereas other provides degraded images. Also some image encryption methods have less processing speed while other has high processing speed. These points motivated me to implement a new system for providing security to images being transfer, by keeping in mind the safety of an image. Proposed approach is meant to improve the safety level of an image by using a new type of block-based image transformation approach which is more secure, and efficient. The experimental result showed that the high level of image security is achieved, as correlation between pixels of an image is noticeably reduced and entropy value of an encrypted images is increased by using the proposed approach.

2. LITERATURE REVIEW

Chan, and Fekri [8] presented the first use of finite-fields wavelets in cryptography. They proposed a two-round private key cryptographic approach using the finite-field wavelet for enhanced computational complexity over DES and AES encryption algorithm. They showed that there approach is simple in structure and is not damageable to known cryptanalytic attack.

Ran Tao et al. [9] proposed an image encryption techniqueusing multiple orders of Fractional Fourier Transformation **(**FRFT). They suggested that their proposed method could be used with double or further image encryptions and they have used compression with proposed encryption method for improving the space complexity and security of an image.

Dang and Chau [10] and, Razzaque and N.V. Thakur [11] have combined image encryption with image compression and their order of using these two techniques are also different. But, the main aim of both the authors are same and that is to satisfy both bandwidth and security requirements of image.

Amrane Houas et al. [12] proposed an algorithm for encrypting binary images and also for encrypting databases of binary images containing images of same size. They have used a key gained from the proposed transformation in the form of image both for image encryption and decryption. Their results also shown a good value of correlation and entropy for some standard images.

Lai and Tsai [13] have proposed an image transmission method using Secret-Fragment-Visible Mosaic Imagesfor both color images and text-type grayscale document images. For secure communication of secret images, they produced mosaic image by placing tiles of secret image into blocks of most similar target image selected from database of an images.

Lee and Tsai [14] resolved the weakness of [13] by avoiding the need of target image database. They also solved the difficulty of hiding a large amount of message data into the cover image but it is limited to color images only.

3. PROPOSED WORK

In this section, I have described the proposed image encryption and decryption approach in detail by using algorithms

Algorithm 1. Image encryption (Sender side)

Input: 8-bit image

Output: 8-bit encrypted image, three word collections, 1-bit LSB image, and 1-bit MSB image.

Step-1: Read 8-bit image of size $N \times N$ or $N \times M$ from disk.

Step-2:Divide the given image into 8×8 blocks without any overlapping.

Step-3: Find 1-bit LSB plane of acquired image.

Step-4: Find first word collection from LSB-bit plane obtained in Step-3.

Step-5: Find 3-bit image of remaining bit counter from remaining planes of an acquired image.

Step-6: Find 6-bit image of remaining bit value from corresponding remaining bit counter image obtained in Step-5.

Step-7: Apply recursion on 6-bit remaining bit value image obtained in step-6 till I get 2-bit remaining bit value image.

Step-8: Send 8-bit concatenated image obtained by combining three remaining bit counter images, three word collection, one 1-bit LSB image and 1-bit MSB image to the receiver.

Step-9: STOP

and proper diagrams.

The detailed working at sender side is depicted in Fig. 1. The double rectangle in Fig. 1 represents the images to be send to the receiver.

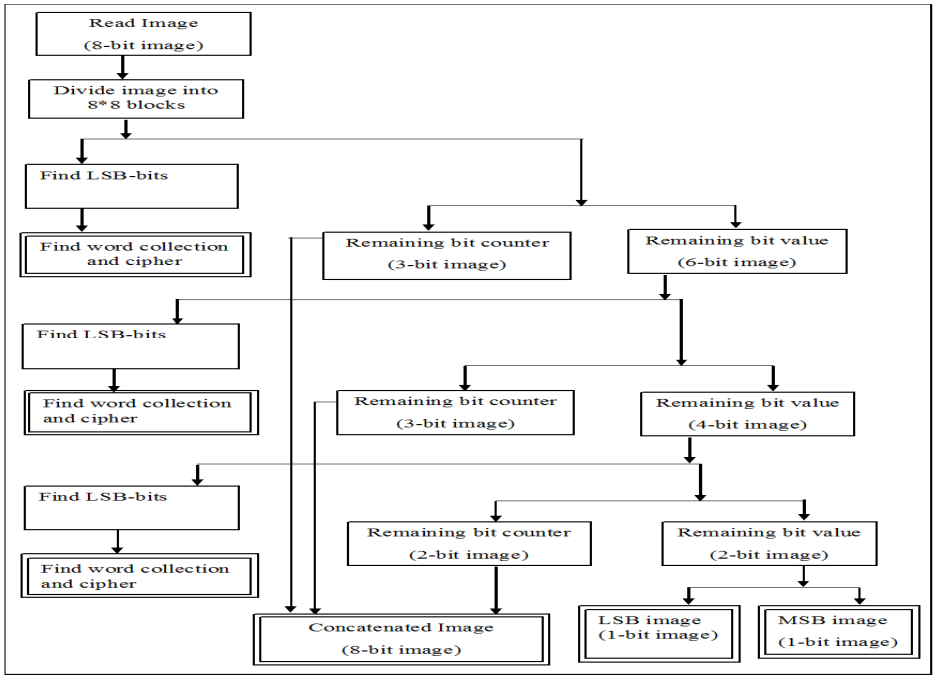

Fig. 1. Detailed procedure at sender side

The detailed stepwise working of proposed approach at sender side is as follows:

1. First read the image of size $N \times N$ or $N \times M$from disk. An image could be grayscale image or colour image of any size. Proposed image encryption approach could be applied to any of the formats of images like jpg, png, tiff.
2. Divide the given image into 8×8 blocks without any overlapping and each block contains 8×8 pixels.If (N/8) and (M/8) gives integer value, then image is perfectly divisible, else image is not perfectly divisible. In this case we have to pad extra bits to make image perfectly divisible.
3. Find the LSB-bits from the bit pattern of all the image pixels by using the logic of even and odd. That is, if intensity value of the pixel is even, then LSB-bit is 0. Otherwise, LSB-bit is 1.
4. Next find word collection. For this, first take the LSB-bits of the first block and find the character set of 8 characters from LSB-bits. Find corresponding word by combining all the characters of obtained character set and cipher the obtained word. The same procedure is applied to each block of an image in order to get ciphered word collection.
5. Find remaining bit counter from the pixel's remaining bits. (i.e. bits excluding LSB-bits). Therefore remaining bit counter will be any number between 0 and 7, hence remaining bit counter image can be presented as 3-bit image. If leading bit is 0, then supress leading 0-bits, make count of number of bits remained and record number of bits remained as remaining bit counter. If leading bit is 1, then remaining bit counter will be 7.
6. The remaining bit value is any decimal number corresponding to 3-bit remaining bit counter. Therefore, it would be in the range 0 to 63, and can be presented as 6-bit image. If remaining bit counter is N, then remaining bit value will be any number from 0 to 2^{N-1}.
7. Apply recursion on remaining bit value till we get two 1-bit images.

Algorithm and diagram at receiver side is as given below:

Algorithm 2. Image decryption (Receiver side)

Input: 8-bit encrypted image, three word collections, 1-bit LSB image, and 1-bit MSB image.

Output: Original 8-bit image

Step-1: Split 8-bit concatenated image into three remaining bit counter images.

Step-2: Combine two 1-bit images.

Step-3: Obtain remaining bit value images by combining respective remaining bit counter image and image obtained in step-1.

Step-4: Repeat step-3 until we obtain original 8-bit image.

Step-6: STOP

At recipient side, the acquired image can be reacquired by applying the inverse transformation. The inverse transformation algorithm for recovering an input image is described in Fig. 2.

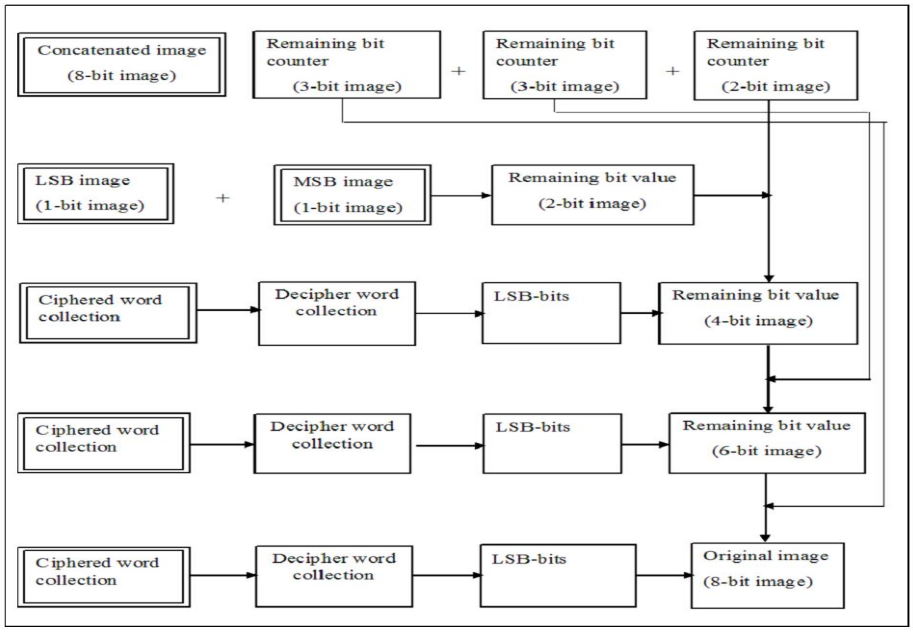

Fig. 2. Detailed procedure at receiver side

The detailed stepwise working of proposed approach at receiver side is as follows:

1. Take 8-bit concatenated image. Split this concatenated image into three remaining bit counter images. That is 3-bit, second 3-bit, and 2-bit remaining bit counter images.
2. Take two 1-bit images and combine these images to form 2-bit remaining bit value image.
3. Combine 2-bit remaining bit value image obtained in step-2 and 2-bit remaining counter image obtained in step-1.
4. Then take first 32×32 ciphered word collection, decipher this word collection. Find LSB-bits from obtained word collection. Now combine image obtained in step-3 and LSB-bits obtained in step-4 to get 4-bit remaining bit value image.
5. Combine 4-bit remaining bit value image obtained in step-4 and 3-bit remaining counter image obtained in step-1.
6. Next take second 32×32 ciphered word collection, decipher this word collection. Find LSB-bits from obtained word collection. Now combine image obtained in step-5 and LSB-bits obtained in step-6 to get 6-bit remaining bit value image.

7. Combine 6-bit remaining bit value image obtained in step-6 and 3-bit remaining counter image obtained in step-1.
8. At last take third 32×32 ciphered word collection, decipher this word collection. Find LSB-bits from obtained word collection. Now combine image obtained in step-7 and LSB-bits obtained in step-8 to get original 8-bit image.

4. EXPERIMENTAL RESULTS AND DISCUSSION

Here, I have shown the performance of the proposed image encryption approach. The proposed approach is implemented with MATLAB 2012 and 64-bit operating system with 4GB RAM and i5 processor. I have performed experiments on different images accessed from the standard image database of image processing. The results for "Lena.png" of size 256 x 256 are listed in following figures. Fig. 3 shows the GUI of the proposed approach which includes the original image, three encrypted images, and the regenerated image. Fig. 4 (a) shows the primary word collection gained from an acquired image, Fig. 4 (b) shows the succeeding word collection gained from the first remaining bit value image, and Fig. 4 (c) shows the third and the last word collection acquired from the second remaining bit value image.

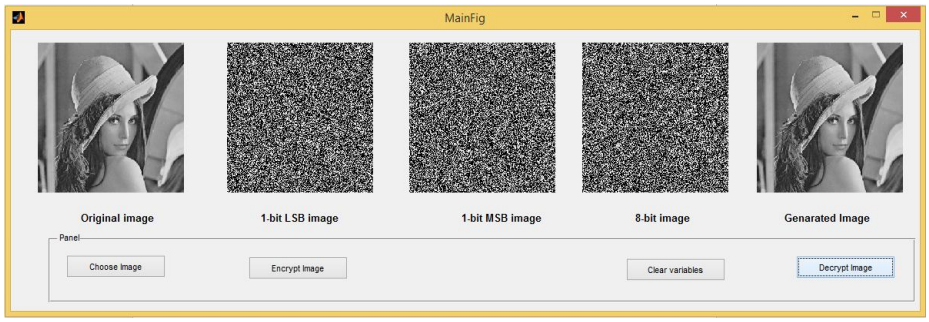

Fig. 3. GUI of the proposed approach for Lena of size 256×256.

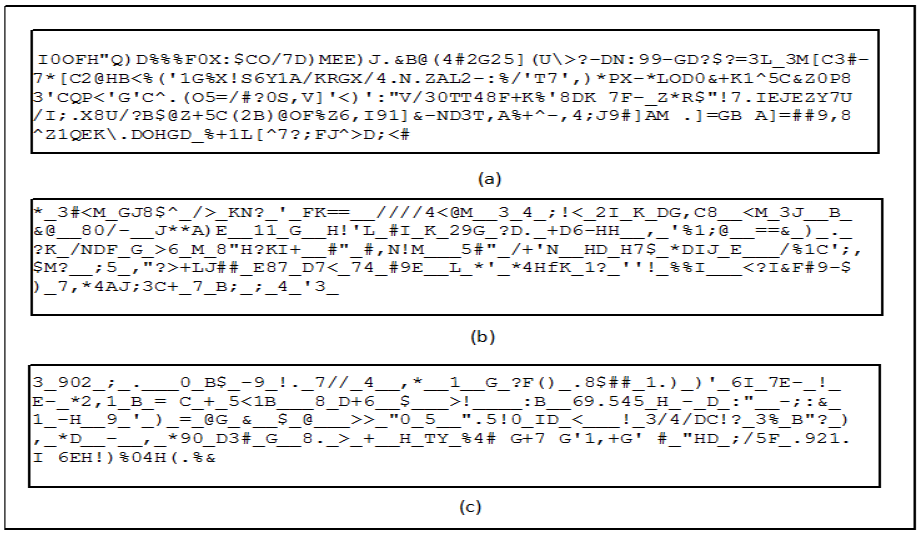

Fig. 4. Ciphered word collection (a) First word collection obtained from a given image (b) Second word collection gained from the remaining bit value image (c) Third word collection gained from the second remaining bit value image.

4.1 Correlation between adjacent pixels: Correlation is anestimate of the relationship between adjacent pixels and it should be low for better image security. There is a high correlation between two adjacent pixels in original image, while in encrypted one, I have tried to keep correlation between pixels at minimum level. The experimental result shown in Table 1 confirms that the correlation between image pixels is considerably decreased by using the proposed approach.

Table 1: Correlation for some standard images

Image	1-bit LSB image	1-bit MSB image	8-bit image
Lena.jpg	-2.888646e-03	-1.689164e-03	-1.620483e-03
Cameraman.png	-2.146068e-03	4.026071e-04	2.524795e-02
Fig0107(e).tif	-4.311931e-02	-4.492321e-02	-3.942115e-02

4.2 Entropy: Entropy is numeric value used to measure the uncertainty relationship with random variable, and it should be high for stronger encryption. In case of an image, the encryption reduces the shared information among encrypted image variables and hence, increases the entropy value. Table 2 shows the entropy value obtained for some standard images using proposed approach.

Table 2: Entropy of some standard images

Image	1-bit LSB image	1-bit MSB image	8-bit image
Lena.jpg	5.393163e+00	5.387227e+00	5.406696e+00
Cameraman.png	5.381865e+00	5.393625e+00	5.362596e+00
Fig0107(e).tif	5.618379e+00	5.625232e+00	5.661985e+00

4.3 Histogram Analysis: The histogram analysis explains how pixels in an image are break down by plotting the number of pixels at all intensity level. Hence, I considered histogram analysis to examine the efficiency and security level provided by the proposed approach and found that the histogram of the transmitted 8-bit image is not similar as that of the histogram of encrypted images and the histogram of an encrypted images are almost uniformly distributed, thus provides good image security.

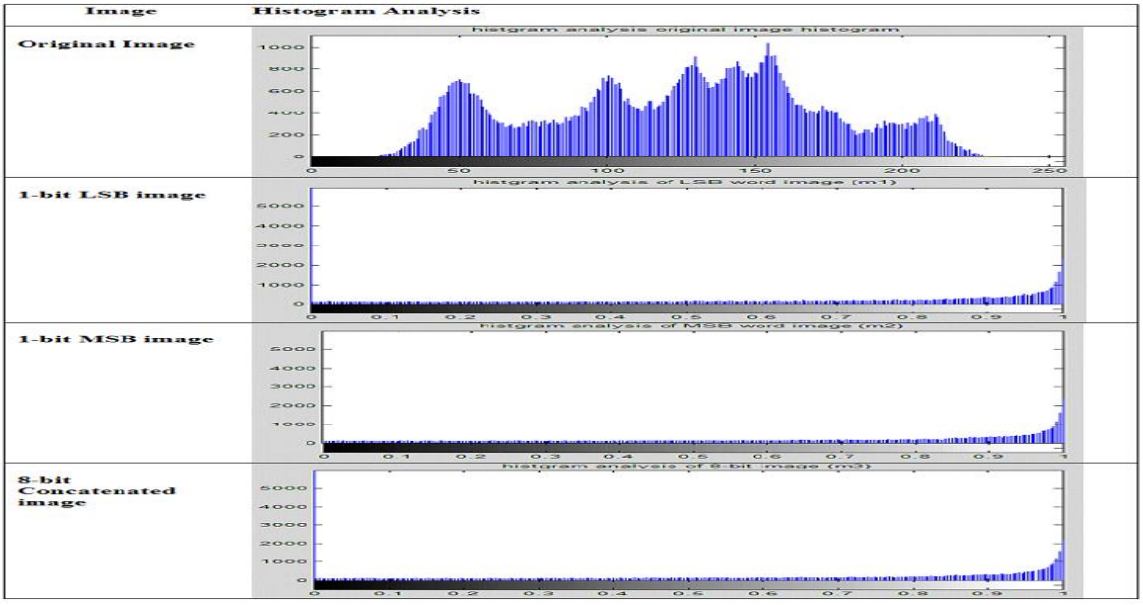

Fig. 5. Histogram analysis of Lena.jpg

In Table 3, results of proposed encryption approach is compared with block based transformation [4].The above results of the proposed approach show that,

1.Correlation between the neighboring pixels is greatly reduced by the proposed algorithm. Hence, provide higher security.

2.The entropy achieved by the proposed algorithm is nearly same as that of [4].

Table 3: Comparison of proposed work with block based transformation [4]

Image	**Performance Evaluation Parameter**			
	Proposed Approach		Block Based Transformation [4]	
Lena.png	Correlation	Entropy	Correlation	Entropy
1-bit LSB image	-2.888646e-03	5.393163e+00	0.0063	5.5286
1-bit MSB image	-1.689164e-03	5.387227e+00		
8-bit concatenate image	-1.620483e-03	5.406696e+00		

5. CONCLUSION AND FUTURE SCOPE

In this paper, a new approach for encrypting imagesusing partitioning of a bit pattern has been proposed. This approach aims at improving thesecurity level of an encrypted image by reducing the correlation among image pixels and improving the entropy value of an encrypted image. Experimental outputs of the proposed approach showed that, the proposed encryption approach provides good level of image security and is robust to any statistical attacks.

In future, a mechanism can be designed to securely transmit the encrypted image with low memory requirement and one can use proposed approach in combination with other image encryption algorithms to further increase the security level of an image.

References

[1] Der-Chyuan Lou and Chia-Hung Sung, "A Steganographic Scheme for Secure Communications Based on the Chaos and Euler Theorem", *IEEE Transactions on Multimedia*, vol. 6, no. 3, pp. 501-509, June 2004.
[2] Bingwen Feng, Wei Lu, and Wei Sun, "Secure Binary Image Steganography Based on Minimizing the Distortion on the Texture", *IEEE Transactions on information Forensics and Security*, vol. 10, no. 2, pp. 243-255, Feb. 2015.

[3] Yu-Chee Tseng, Yu-Yuan Chen, and Hsiang-Kuang Pan, "A Secure Data Hiding Scheme for Binary Images", *IEEE Transactions on Communications*, vol. 50, no. 8, pp. 1227-1231, Aug. 2002.

[4] Mohammad Ali Bani Younes and Aman Jantan, "Image Encryption Using Block-Based Transformation Algorithm",*IAENG International Journal of Computer Science*, vol. 35, no. 1, pp. 15-23, Feb. 2008.

[5] Subramania Sudharsanan, "Shared Key Encryption of JPEG Color Images", *IEEE Transactions on Consumer Electronics*, vol. 51, no. 4, pp. 1204 – 1211, Nov. 2005.

[6] Jakimoski G and Kocarev L., "Chaos and cryptography: block encryption ciphers based on chaotic maps", *IEEE Transactions on Circuits and Systems*, vol. 48, no. 2, pp. 163 - 169, Feb. 2001.

[7] Aarti Devi, Ankush Sharma, and Anamika Rangra, "A Review on DES, AES and Blowfish for Image Encryption & Decryption", *International Journal of Computer Science and Information Technologies*, vol. 6, pp. 3034-3036, 2015.

[8] Kevin Sean Chan, and Faramarz Fekri, "A Block Cipher Cryptosystem Using Wavelet Transforms Over Finite Fields",*IEEE Transactions on Signal Processing*, vol. 52, no. 10, pp. 2975 – 2991, Oct. 2004.

[9] Ran Tao, Xiang-Yi Meng, and Yue Wang, "Image Encryption With Multiorders of Fractional Fourier Transforms", *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 4, pp. 734-738, Dec. 2010.

[10] Philip P. Dang and P. M. Chau, "Image Encryption for Secure Internet Multimedia Applications", *IEEE Transactions on Consumer Electronics*, vol. 46, no .3, pp. 395-403, Aug. 2000.

[11] Abdul Razzaque & Nileshsingh V. Thakur, "An Approach to Image Compression and Encryption",*International Journal of Image Processing and Vision Sciences*, vol. 1, no. 2, 2012.

[12] Amrane Houas, Zouhir Mokhtari, Kamal Eddine Melkemi, and Abdelmalik Boussaad "A novel binary image encryption algorithm based on diffuseRepresentation", *AnInternational Journal on Engineering Science and Technology*, vol. 19, no. 4, pp. 1887–1894, Dec.2016.

[13] I. J. Lai and W. H. Tsai, "Secret-fragment-visible mosaic 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, Sep. 2011.

[14] Ya-Lin Leeand Wen-Hsiang Tsai, "A New Secure Image Transmission Technique via Secret-Fragment-Visible Mosaic Images by Nearly Reversible Color Transformations", *IEEE Transaction on Circuits and Systems for Video Technology*, vol. 24, no. 4, pp. 695-703, Apr. 2014.

AUTHOR

Ankita P. Pandereceived B.E. (Information Technology) from SGB Amravati University and completed M.E. (Computer Science and Engineering) from SGB Amravati University in 2015.