ISSN 2278-3091

Volume 9, No.5, September - October 2020

International Journal of Advanced Trends in Computer Science and Engineering

Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse06952020.pdf

https://doi.org/10.30534/ijatcse/2020/06952020

A Prototype Model for Image Encryption using ZigZig Blocks in Inter-Pixel Displacement of RGB Value

Amnesh Goel[1], **Dr. Rakesh Bhujade**[2]
[1]PhD Research Scholar, [2]PhD Supervisor
Department of Computer Science and Engineering, Mandsaur University, Mandsaur, MP 458001, India
Email: *amneshgoel7@gmail.com

ABSTRACT

Amount of information which can be stored within the images, and the movement of images over open network takes to the problem of image theft and breach of confidentiality. To prevent the loss of information from images, it leads the idea of image encryption in which various researchers are trying to encrypt image in such a way that un-authorized users should not be able to access the information kept within image, and for the same purpose researchers have proposed different image encryption techniques with confusing features to keep the images secure when they are moving over open networks. So, in the chain of existing work, we are purposing an image encryption method which is using block formation within the image, and each block is then used in zigzag manner followed by inter-pixel displacement of RGB values within that zigzag area of the block. The block sizes can vary from image to image and this is part of the key.

Key words*:* Zigzag, Inter-pixel, RGB, Image Encryption, block.

1) INTRODUCTION

Image encryption has become the need of the hour of current scenario for those peoples or organizations who are either using images for professional work or for storing official information; in both the cases, an image encryption is important because if images are needed to be share among various users then it must have to pass on public open network [1] which is not safe, and safe flow is only possible when communication channel is purely dedicated for one user or that channel is personal channel which is not possible in the ideal world. So, users need to take a step ahead and must send the images over this open network and must take risk with the confidentiality of data store within images. For such purpose, a need of image encryption technique comes into picture to encrypt the image in such a format that no one other than the authorized user can have access to it.

As images are capable to store huge amount of information as compare to text and for other obvious reasons, usage of images has increased over time. Availability of high quality cameras at low cost enables a common user to take pictures frequently and store them for future reference, but problem arises when someone else who is not authorized to access those images steals the images and use them in a negative way. This is called the image theft, and this is a very common problem these days. According to a report [2] published in 2017 via “United States Digital Image Theft” shows US registered 59% cases against the image theft. Big companies which are heavily dependent on image business are using images for which they are not having authorized licensees, for example “Pinterest”. In 2017, Pinterest found to be using 41% such images for which they did not have any license. So, here comes the need of an image encryption technique (which is very important and genuine need) to keep information safe from unauthorized access. But as the technology is growing rapidly, in the same way usage of images in professional domain is increasing and people are giving more precedence to use images over textual data as information kept within image is more understandable than same information written in textual format as professionals and other naive user takes less time to understand the content shown using pictorial within image. A usual saying is “a picture is worth 1000 words” because a human mind can remember an image easily than remembering the paragraph content. So, in this research paper, we will see an image encryption algorithm which is purely based on the block encryption along with a novel idea of using these blocks in a zig-zag format which is entirely new. And this will give an edge to the whole encryption process compare to other image encryption techniques.

This paper is discussed using 8 sections where section 2 puts a light on the image encryption background and its need. Section 3 describes the related work which has done so far for making images secure. In this section we are discussing several image encryption techniques. Section 4 and 5 deals with the proposed methodology and architectural diagram of proposed model. Section 6 presents a comparative summary of proposed image encryption model with 3 other image encryption techniques based on the zigzag approach. Section 7 concludes the proposed image encryption method. Section 8 discuss the further scope of work.

2) BACKGROUND

Images are now a days widely in use in various professional domains like banking, marketing, sales, e-learning, education, sports, promotion and there are so many other fields which are using images extensively and demand of image usage is making field of image encryption very important, and that's why more number of researchers are inclined towards this field to give outputs based on unalike confusing features, so that they will be able to encrypt the image in a unique way. On the recent developments in banking domain, due to the prevention of fraud of reading magnetic strips of ATM card, banks are replacing the existing ATM machines with the new machines which needs finger scan [3] or thumb scan instead of inserting ATM card and PIN [4] into the machine to complete the transaction. This has its own benefits and drawbacks. For example, reading the thumb scan is again taking a snap of the thumb and sending that as an image over the network to validate the account information. This is opening more room for image theft over the network and we will continue to this discuss this in a while.

In this way, the moment customer will provide the thumb impression over the space provided within machine; the machine will scan the thumb impression and will send this impression to their respective server to authenticate the user instead of traditional system of inserting ATM card into machine which reads the secret code from magnetic strip of ATM card and now server will be responsible to differentiate between authorized and unauthorized user based upon the image instead of textual content of magnetic strip. Now the moment machine will send image to server then there might be possibility that some unauthorized user will access that image and can perform some transactions. So, it is very important in current time to encrypt the image before sending over the public open network. This need of scan in ATM machine came into picture after ATM frauds which are done using duplicate ATM magnetic strips, but this feature has some inbuilt flaw of need of image encryption. So, this conversation is opening a new room for transferring images in a secure manner over the open network because a thumb scan is a personal information.

So, a well-suited image encryption technique is required if we carefully look at the criticality of this subject. Usually any image transfer includes the three main components i.e. a sender, a network, and a receiver.

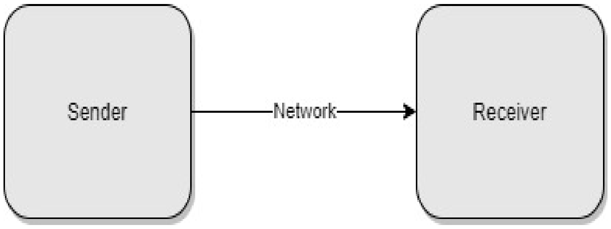


Figure 2.1: Sender, network, and receiver, three components required for image transfer

Sender of the image should be enabled to use the image encryption technique so that when an image moves to the network, it is in its cipher form. And the receiver should be enabled to decrypt the image using decryption process to get the plain image back. Also, the key should be shared among sender and receiver to smoothly execute this entire process.

So, if we discuss in detail then the said system will look like the figure 2.2 where we have elaborated the sender and receiver segment. In this scenario there will be a sender which is having a local database (or any other source of storage, it could be SDD, HDD, detachable storage etc.) containing the images. Sender will be having a networking device to establish the communication with receiver. It could be an external modem or in-built communication system if sender is using a smart phone. In this similar fashion, receiver is also having the similar setup to receive the images. Here, the encryption and the decryption processes are embedded at the sender and received end respectively for secure transmission.

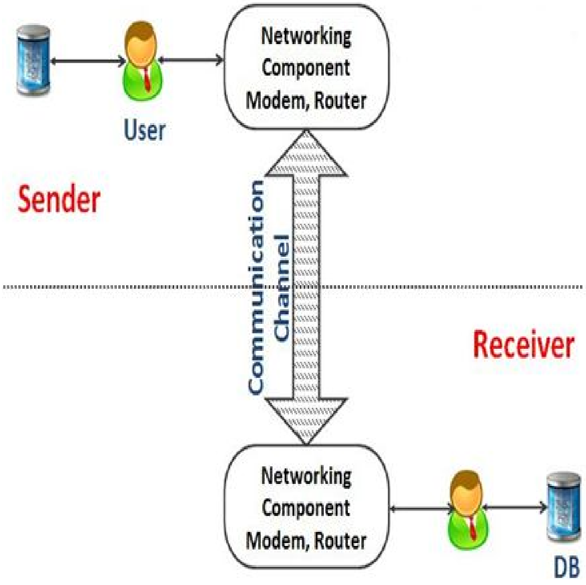

Networking Component Modem, Router
User
Sender
Communication Channel
Receiver
Networking Component Modem, Router
DB

Figure 2.3: Architecture for embedded encryption and decryption Process.

3) Related Work

This section briefly touches upon on the research work that has been done in the image encryption domain. It is not possible to include all those papers in this study, but we have taken few related research papers for this study. Image encryption can be broadly classified into two categories i.e. block encryption and stream encryption [5] [6] [7] [8]. Block encryption takes the entire block for encryption in one attempt whereas the stream encryption takes the stream of bytes for the entire encryption process. Following is a summary of few research papers.

Reji Mathews, Amnesh Goel, Prachur Saxena and Ved Prakash Mishra [9] was proposed in 2011 which focused on manipulation of RGB [10] values of pixel and its displacement as per the predefine key. Circular shift applied on the three components of pixel with different key so that R, G and B values of pixel intermix with the R, G, B value of other pixel which is also terms as explosive inter-pixel displacement [11]. This algorithm was applied in the horizontal direction as well as in vertical direction as per the phase mask and key of phase mask was preserved for decryption purpose.

Amnesh Goel, Reji Mathews & Nidhi Chandra [12] was proposed in 2011 which was further extension of work of Inter-Pixel displacement of the RGB attributes of a Pixel by making the 4 slices and shuffling of those slices before encryption. Slices were made from the center of image and these four slices were diagonally inter exchanged before doing actual image encryption. Proposed work is bit different from this work in terms of shuffling and making slices from center of image of rectangular shape. Review of image encryption techniques was discussed in this paper [13].

Ratnakirti Roy, Shabnam Samima, Suvamoy Changder [14] explains one image encryption algorithm in which the authors used image steganography [15] [16] technique to encrypt the image. The whole process had two steps embedding and extraction. In this paper, authors took one stego image which they used for image steganography purpose. Authors extracted the R, G and B plane out of the stego image, and they mixed this R, G and B planes with R, G and B plane of plain image or the host image. In this way, they performed the image steganography. Authors later presented the histogram analysis [17] of different planes where Red plane did not change, but there were changes in the Blue and the Green planes.

In this paper, Eugenijus Margaritas and Simona Ramanauskaitė [18] proposed an image encryption technique which is based on the image steganography [19]. In this paper authors did not use any stego image for the encryption, rather they created sub-cube of RGB color planes. Instead of using a reference image, authors proposed to segregate all colors (x, y, z) into RGB cube. If any color (x, y, z) is not present in the image then the value will be zero. And later each sub cubes are recursively processed. This algorithm does not change the pixel value, which is commonly used technique in image steganography, instead authors changed the location of color in RGB cube using image color palette transformation.

In this paper, Karthikeyan B, Asha S, Poojasree B [20] proposed a data hiding technique inside the color image using LSB embedding [21] [22]. Authors developed this encryption technique to conceal the text messages in the images. To execute the procedure, binary conversion was proposed to perform of both image and the textual data and in the next step, LSB substitution was performed. However, overall description of proposed method lacks detailing of approach. MSE and PSNR [23] data was shown to validate the approach but still detailing of proposed approach is somewhat missing in the entire paper.

Narendra K Pareek, Vinod Patidar, and Krishan K Sud [24] proposed an image encryption technique which is based high order of diffusion and substitution. They took the key size of 128 bit. They divided the original image into number of blocks. The size of blocks is derived using the encryption key. Each block is further processed using the diffusion and substitution process. Diffusion process is using the zigzag approach to shuffle the pixels of block within the boundary of block. Also, the block pixels are moved horizontally and vertically to other blocks in the substitution process. Authors kept the block size to 8x8 fix size to traverse within the block.

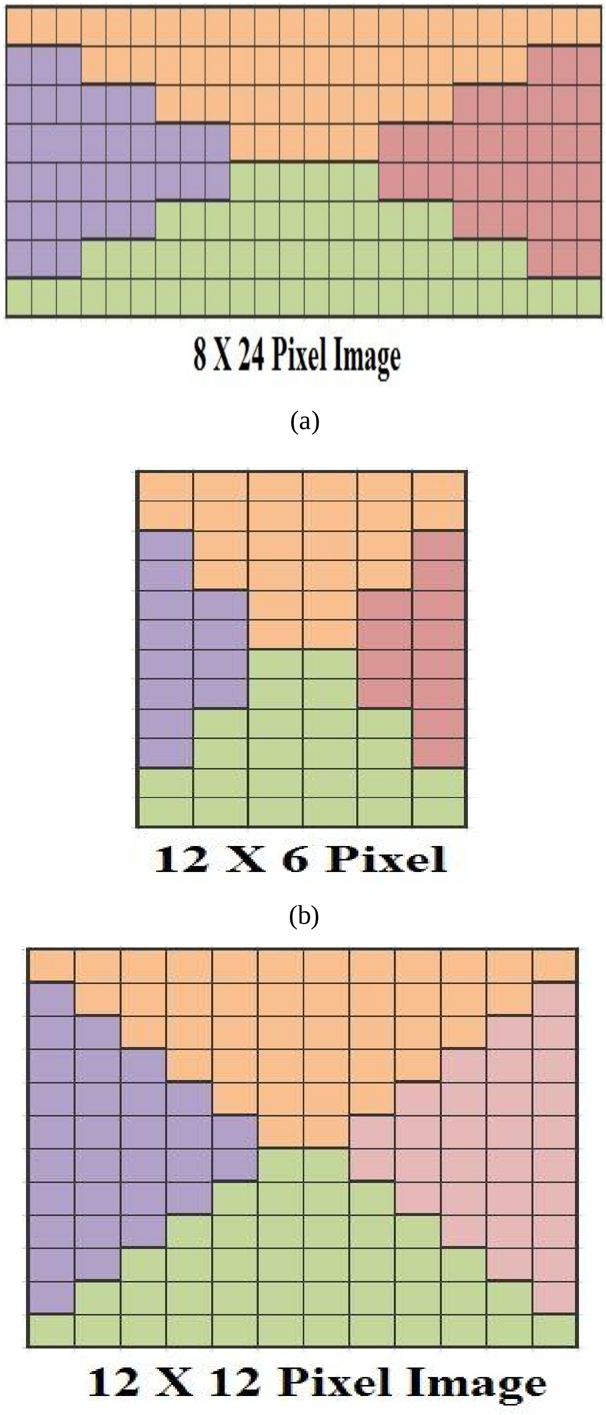
Priya Ramasamy, Vidhyapriya Ranganathan, Seifedine Kadry, Robertas Damaševiˇcius, and Tomas Blažauskas [25] proposed an image encryption technique which is based on the modified zigzag transformation. This is a 3-step process image encryption technique. In the first step, the image is divided into 64 blocks. In the second step, modified zigzag transformation is applied. In the same step, authors proposed to move the first and second pixel to the second last and last position in the image to confuse the zigzag transformation and this is where authors named it as modified zigzag transformation. In the last step, the XOR operation was performed on the RGB plane to get the cipher image. Authors proposed to use a 256-bit key in this case, but they did not explain the details of key and how that is used in the encryption process. Later, authors performed the encryption on 4 different images. Authors presented the histogram analysis to support their results along with the key sensitivity analysis. They changed the original key marginally and results shown in the paper confirms that they did not receive the plain image back. Correlation analysis is also presented in this paper which shows that adjacent pixels are not corelated. A few more different types of analysis techniques are used in this paper to support their results. Authors could have described the key details which is very important for any encryption process.

Changjiu Pu [26] suggested an image encryption technique which is based on the image block and zigzag transformation. In this paper, author proposed this image encryption algorithm which works on the single plane (gray scale) of image. If the image is in color format then the very first step is to convert the color image into Red, Green, and Blue plane. In the second step, image is converted into the blocks and in the third step, zigzag transformation is performed. Zigzag transformation is performed at the block level and not at the pixel level. Author did not discuss the key details which is used for the encryption process. Authors later presented few key analyses to support his results using Histogram analysis, sensitivity testing, scrambling effect etc.

4) PROPOSED METHODOLOGY

In this paper we propose a novel image encryption algorithm which is a four-step process. The novelty of this image encryption techniques is in 2 processes. The first novelty is in zigzag approach that we introduced at block level. And the second novelty is unique combination of blocks, zigzag and inter-pixel explosion of a pixel value. Following steps represents the execution of this image encryption algorithm.

Step 1: The plain image of size X, Y is divided into blocks of n x m where n! =m or n==m depending on the block size. Figure 4.1 show the blocks of different sizes. And this block structure is repeated in the entire image. The block sizes may vary based on the size of image i.e. X, Y (X represents the number of rows and Y represents the number of columns in any given image).



(a)

(b)

(c)

Figure 4.1: highlighting pixel arrangement in an image and different zigzag blocks in different color codes. (a) Pixel arrangement for image of 8 x 12 pixels (b) Pixel arrangement for image of 12 x 6 pixels (c) Pixel arrangement for image of 12 x 12 pixels.

Zigzag block representation is shown in the figure 4.1 for 3 images of different size and these images confirms that boundary of formed blocks will be of zigzag nature. Each individual block is further divided into 4 sections which translates into the zigzag formation. In this image encryption technique, a block may or may not be of the square shape. Blocks may be of rectangular shape (possibly). Usually block encryption methods are based on square blocks and if unauthorized user comes to know that image is encrypted using block encryption then decryption will be bit easy.

At this point of time where we are speaking of dividing the image into blocks and then perform the zigzag operation, it is equally important point to note out is, the proposed method has a defined boundary such that it will work where the image size will support either of the block size discussed above. If the plain image cannot be divided using any of the block size, then that image cannot be encrypted using the proposed prototype model. This is because the plain image size should support the block sizes for further encryption process.

Block size is fixed based on the size of the image so that we can create a finite number of blocks in any given image. This block size is part of the encryption key and this is kept secret and only known at the sender and receiver who is executing this algorithm. First two bits of the encryption key is reserved for the block size formation.

Step 2: In the second step of this image encryption algorithm, we formulate each block (which identified in first step) into a zigzag manner as shown in the figure 4.1. Zigzag approach basically restricted the movement of a pixel in the row or column. Ideally in any pixel permutation algorithm, the pixels are moved in the entire row or entire column. But, in the zigzag manner, entire row or column is not available for free movement of a pixel. Each block is having a logical boundary of 4 sub-blocks which we can be named as left, right, top, and bottom block.

So, the pixel movement is restricted within this logical boundary. For example, if we consider the top block of 4.1 (a) then the first three pixels of row cannot move vertically because this top block is not having any further rows for first three pixels. In the similar pattern, if we consider the top block of 4.1 (b) then it is visible that first column pixels have two rows to move vertically, second column has 4 and so on so forth. And the same logic follows for the left and right blocks as well. This is a unique pattern to form the zigzag blocks within a block. And the logical representation (which is shown in image 4.1 (a), (b), and (c)) may differ than the actual representation in an image.

Step 3: In this step, each individual sub-block is proposed to execute using inter-pixel permutation procedure where a pixel value is moved within the sub-block boundary either in horizontal direction or the vertical direction in a recursive manner. This movement includes the movement of entire pixel and at this point of time, we are not considering dividing the color image into its Red, Blue, and Green plane. To strengthen the whole encryption process, we will also process the inter-pixel permutation on the individual color planes in the entire image. But that will happen in the next step. This step adds 5 bits to the encryption algorithm where first two bits (combination of $2^2 = 4$) represents the recursive nature (number of times this procedure will repeat) and rest three bits (combination of $2^3 = 8$) represents the horizontal and vertical permutation of pixels within sub-block boundary. This step is fairly limited at the block level and pixel values does not go out of the block to the other blocks. In the next step, we will deal with at the entire image level.

Step 4: In this last step, the output of previous step is taken as a whole image and inter-pixel RGB permutation algorithm is planned to execute. At first, the entire image must be divided into Red, Green and Blue planes of the color image and each of these planes are used for inter-pixel permutation. Dividing the image into its Red, Green and Blue planes is not difficult at all, and this can be done easily in any image processing software by executing a set of commands. Following set of commands [27] can be executed in Matlab [28] to get the Red, Blue, and Green plane of a color image.

```
% Read in original RGB image.
plainRGCImage = imread(abc.jpg);

% Extract color channels.
redChannel = plainRGCImage(:,:,1); % Red channel
greenChannel = plainRGCImage(:,:,2); % Green channel
blueChannel = plainRGCImage(:,:,3); % Blue channel
```

We have already discussed the inter-pixel permutation algorithm [9] in the section 2 of this paper. This step further adds 18 bits in the encryption key. 6 bits for each plane is proposed. The first two bit derives the recursive nature of execution. The next bit defines the key for value transformation and remaining three bits represents the horizontal and vertical permutation of pixel. In this way, we get the 6 bits encryption key for Red, 6 bits encryption key for Green and 6 bits for Blue plane of a color image.

Key Analysis: This novel image encryption algorithm proposes to use a **25-bit** encryption key for the core encryption. This is a 4-step encryption process and division of 25 bit key into these steps are as follows.

The first 2 bits are used in step 1 which decide the block formation. Next 5 bits are used in step 3 where the initial 2 bits of 5 are used to decide the recursive nature and next 3 bits of 5 are used for horizontal and vertical permutation. Next 18 bits are used in the step 4 of this image encryption algorithm where we used 6 bits for each plane i.e. Red, Blue, and Green. This key looks sufficient for the encryption process. Large key size makes it difficult for the brute force attack [29] to guess the correct pattern of encryption and smaller key size is easy to guess.

5) ARCHITECTURE

Architecture of the proposed system is shown in figure 5.1 and in this section, we will discuss about 4 important components i.e. Sender, Network, Receiver, and the encryption key of this proposed image encryption technique.

Sender is the first component which is going to send the encrypted images (cipher image). Sender is equipped with the encryption engine which is powered by the encryption key. Sender gets the cipher image out of the encryption engine. Network is the communication system over which cipher image travels to the receiver. Receiver is equipped with the decryption engine which coverts the cipher image into plain image. This decryption engine is powered by the decryption key which is used for the encryption. And the last component of this architecture is the key which is used for encryption and decryption purpose.

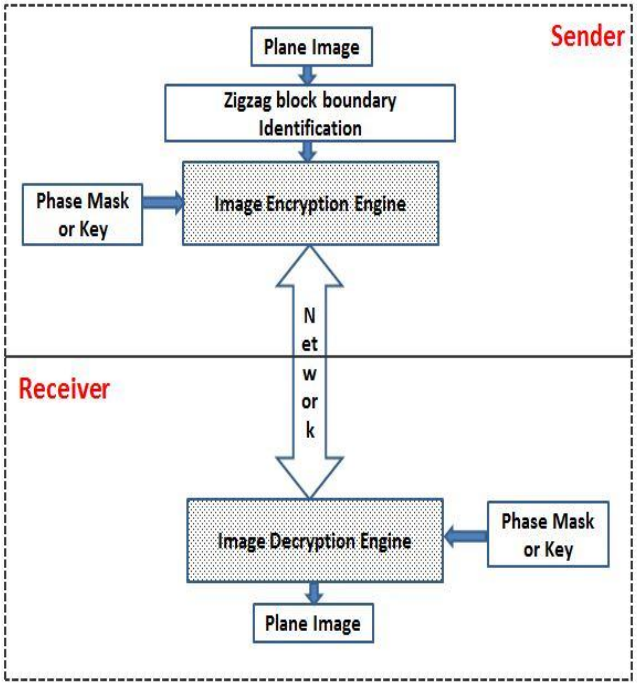


Figure 5.1: Proposed architecture of Image Encryption using zigzag block formation.

Architectural flow of proposed system is shown above where the plain image is used to form the zigzag blocks as shown in figure 4.1 and then that image will be used for image encryption using explosive inter-pixel displacement of RGB values. But as per the size of image, after each row or couple of rows boundary of block gets shrink and when one block moves towards the end of execution there are least pixel left and at the receiver end, receiver need to perform reverse of encryption process and receiver will get the plain image; only receiver need to know about the phase mask or key which is used for the encryption.

6) COMPARATIVE STUDY WITH OTHER SIMILAR APPROACHES

Table 1: Comparison of different image encryption techniques with proposed model

Sr. No.	Comparison point	Proposed Prototype Model	Substitution-diffusion based Image Cipher	An Image Encryption Scheme Based on Block Scrambling, Modified Zigzag Transformation and Key Generation Using Enhanced Logistic—Tent	Image scrambling algorithm based on image block and zigzag transformation
1.	Encryption Approach	Encryption is done at block level, sub-block level and at image level	Encryption is done at block level and image level. A block is not divided into sub-blocks.	Encryption is done at block level and then by performing a XOR operation of RGB channels.	This encryption process works at image level, block level and zigzag transformation.
2.	Number of steps	This is a 4-step process. First step is to get the image into blocks. Second step makes the blocks into zigzag format. Third step executes at block level and fourth step works at the image level.	This is a 3-step process. First step is to make blocks, second step works on the diffusion and third step is substitution.	This is a 3-step process. First step divides the image into blocks, second step performs the modified zigzag transformation and the third step performs the XOR operation between RGB channels.	This is a 3-step process in which the image is converted into gray scale (or RGB planes are extracted out) in the first step. In the second step, blocks are formed and in the final step, zigzag transformation is performed.
3.	Is inter-pixel encryption supported	Yes	No	No	No
4.	Is zigzag methodology applied	Yes	Yes	Yes	Yes
5	Zigzag transformation details	Each block is divided into 4 sub blocks and each sub-block represent area for zigzag transformation.	Zigzag transformation is performed at block level in continuous up-down format.	Modified zigzag transformation is applied in this paper. Only new tweak is that they have replaced the first pixel and second-pixel value with the second last and last pixel value to confuse the zigzag transformation.	Zigzag transformation is performed at the block level and not at the pixel level. The entire block is moved from its position.
6	Key size and details	25 bits for core encryption. Details of each bit of 25 bits are explained in the paper.	128 bits key. But the details are not provided.	256 bits key. But the details are not provided.	Author did not discuss the key size and its details. Author must disclose the key size and the details of key in the encryption process.

Above table shows a comparative study of proposed image encryption model with 3 other zigzag based image encryption techniques. For this study, we have taken few important parameters into account such that the overall encryption approach, zigzag transformation, key size details etc.

7) CONCLUSION

This paper proposed a model for a new image encryption technique where encryption can be done using the zigzag block formation which is safe as compare to other block encryption schemes. This is because, when we decrypt the blocks then usually mindset is, blocks will be of square shape (as taken in the most block encryption techniques) and accordingly user sets the decryption algorithm considering blocks of square size. But if same kind of approach is used to decrypt zigzag blocks then user will never get the plain image properly and each decryption execution will further confuse the image. Here are few strengths that we talked about in this paper regarding this image encryption technique.

1. Block can be of rectangular shape or of the square shape. We have proposed 2 rectangular shape blocks vs 1 square shape block. This will break the traditional decryption mindset which considers the block of square shape in image encryption techniques.
2. Each block is not considered single unit. Each block is further divided into 4 blocks i.e. top, left, bottom, and right. Usually, in the image encryption techniques, a block is processed at one time. But, in this proposed process, we have sub-divided the block into 4 segments. This is further unique steps that we have taken.
3. Block encryption vs the whole image encryption. Usually the block encryption algorithms run the same procedure within the block which they apply on the whole image. In this proposed prototype, the block encryption has two major differences than the encryption which was later applied to whole image. The first difference is a block is further divided into sub-blocks. And the second difference is, block encryption is proposed at the pixel level, where as the image encryption is proposed at the Red, Green, and Blue planes of the color image. This distinction makes the proposed method unique.
4. Diffusion at intra-pixel level is not used because that adds the compute complexity. Inter-pixel movement at RGB level is secure enough because original pixel components are already displaced with other pixel components.

So, with these confusing properties and discussion done in other sections for other block image encryption schemes, this model seems suitable for the image encryption. Considering the novelty of proposed image encryption prototype model, it looks like this is going to be a worthy image encryption scheme because such scheme does not exist.

8) SCOPE FOR FUTURE WORK

In the future work one can continue with the implementation of this proposed work where we can see the experimental results and some potential analyses to evaluate the algorithm. This can also be treated as the future road map. Also, implementation of this work can be chosen along with other distinguish confusing properties to make image encryption stronger and safer. Once we see the implementation of this prototype model then that will be a good chance to compare the results with respect to other image encryption techniques along with the comparison of analysis techniques such as Histogram analysis, Correlation between original and encrypted images, Correlation analysis of adjacent pixels, Information entropy, Key sensitivity analysis, Peak signal to Noise Ratio (PSNR) etc. This will really provide the detail insights of this prototype proposed.

REFERENCES

[1] Open communication - http://en.wikipedia.org/wiki/Open_communication - last accessed on 20th Mar 2020.

[2] A Snapshot of Online Image Theft (Infographic) - https://www.entrepreneur.com/article/309876 - last accessed on 2nd April 2020.

[3] Fingerprint - http://en.wikipedia.org/wiki/Fingerprint_recognition last accessed on 2nd April 2020.

[4] Biometric Atms - https://www.gartner.com/en/information-technology/glossary/ biometric-atms - last accessed on 5th April 2020.

[5] Jakimoski, G. and L. Kocarev. 2001. ―Chaos and Cryptography: Block Encryption Ciphers Based on Chaotic Maps‖. IEEE Transactions on Circuits and Systems—I: Fundamental Theory and Applications. 48(2): 163-169.

[6] Socek, D., Shujun Li, Magliveras, S.S. and Furht, B, "Enhanced 1-D Chaotic Key-Based Algorithm for Image Encryption", First International Conference on Security and Privacy for Emerging Areas in Communications Networks, 2005:406-406.

[7] Deergha Rao and K. Gangadhar, "Modified Chaotic Key-Based Algorithm for Image Encryption and Its VLSI Realization", International Conference on Digital Signal Processing, 2006.

[8] Block encryption and stream encryption study - https://www.cs.utexas.edu/~byoung/cs361/lecture45.pdf - last accessed 20 April 2020.

[9] Reji Mathews, Amnesh Goel, Prachur Saxena & Ved Prakash Mishra, "Image Encryption Based on Explosive Inter-pixel Displacement of the RGB Attributes of a PIXEL", Proceedings of the World Congress on Engineering and Computer Science 2011 Vol I WCECS 2011, October 19-21, 2011, San Francisco, USA. ISBN: 978-988-18210-9-6.

[10] RGB model -http://en.wikipedia.org/wiki/ RGB_color_model – last accessed on 20 April 2020.

[11] Amnesh Goel and Nidhi Chandra, "A Technique for Image Encryption Based on Explosive n*n Block Displacement Followed by Inter-pixel Displacement of RGB Attribute of a Pixel," 2012 International Conference on Communication Systems and Network Technologies, Rajkot, 2012, pp. 884-888, doi: 10.1109/CSNT.2012.190.

[12] Amnesh Goel, Reji Mathews & Nidhi Chandra, "Image Encryption based on Inter Pixel Displacement of RGB Values inside Custom Slices", International Journal of Computer Applications (0975 – 8887), Volume 36– No.3, December 2011.

[13] Amnesh Goel, Dr. Rakesh Bhujade, “A functional review of image encryption techniques”, International Journal of Scientific and Technology Research, 2019.

[14] Ratnakirti Roy, Shabnam Samima, Suvamoy Changder, "A map-based image steganography scheme for RGB images", Int. J. Information and Computer Security, Vol. 7, Nos. 2/3/4, 2015, Copyright © 2015 Inderscience Enterprises Ltd.

[15] Steganography: Hiding an image inside another - https://towardsdatascience.com/steganography-hiding-an-image-inside-another-77ca66b2acb1 - last accessed on 20th April 2020.

[16] Jan Carlo T. Arroyo, Charisse P. Barbosa, Meljohn V. Aborde, Fe B. Yara, Allemar Jhone P. Delima, "An Improved Image Steganography through Least Significant Bit Embedding Technique with Data Encryption and Compression Using Polybius Cipher and Huffman Coding Algorithm", International Journal of Advanced Trends in Computer Science and Engineering, https://doi.org/10.30534/ijatcse/2020/137932020.

[17] Histogram - https://en.wikipedia.org/wiki/Histogram - Last accessed on 19 June 2020.

[18] Eugenijus Margalikas & Simona Ramanauskaitė "Image steganography based on color palette transformation in color space", EURASIP Journal on Image and Video Processing 2019, 82 (2019), https://doi.org/10.1186/s13640-019-0484-x

[19] Marilou O. Espina, Arnel C. Fajardo, Bobby D. Gerardo, Ruji P. Medina, "Multiple Level Information Security Using Image Steganography and Authentication", International Journal of Advanced Trends in Computer Science and Engineering, https://doi.org/10.30534/ijatcse/2019/100862019

[20] Karthikeyan B, Asha S, Poojasree B, "Gray Code Based Data Hiding in an Image using LSB Embedding Technique", International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8, Issue-1, May 2019.

[21] Arun Kumar Singh, Juhi Singh, Dr. Harsh Vikram Singh, "Steganography in Images Using LSB Technique", International Journal of Latest Trends in Engineering and Technology (IJLTET), Vol. 5 Issue 1 January 2015, ISSN: 2278-621X.

[22] S. Sugathan, "An improved LSB embedding technique for image steganography," 2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), Bangalore, 2016, pp. 609-612.

[23] PSNR - https://in.mathworks.com/help/vision/ref/psnr.html - Last accessed on 26th April 2020

[24] Narendra K Pareek, Vinod Patidar, and Krishan K Sud, "Substitution-diffusion based Image Cipher", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.2, March 2011, DOI : 10.5121/ijnsa.2011.3212.

[25] Priya Ramasamy, Vidhyapriya Ranganathan, Seifedine Kadry, Robertas Damaševiˇcius, and Tomas Blažauskas, An Image Encryption Scheme Based on Block Scrambling, Modified Zigzag Transformation and Key Generation Using Enhanced Logistic—Tent Map, Entropy 2019, 21, 656; doi:10.3390/e21070656.

[26] Changjiu Pu, Image scrambling algorithm based on image block and zigzag transformation, Computer Modelling & New Technologies 2014 18(12B) 489-493.

[27] How do I split a color image into its 3 RGB channels? - https://www.mathworks.com/matlabcentral/answers/91036-how-do-i-split-a-color-image-into-its-3-rgb-channels - Last accessed on 19 June 2020.

[28] Matlab - Image Processing Toolbox - https://www.mathworks.com/products/image.html - Last accessed on 19 June 2020.

[29] Brute Force Attacks Defined - https://www.forcepoint.com/cyber-edu/brute-force-attack - Last accessed on 25th April 2020.