Journal of Information Systems Engineering and Management
2025, 10(23s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Novel Method of Highly Secured Image Encryption Technique

Dr.N.Krishna Chaitanya[1*], Dr.C.Padmaja[2], Dr.C.Gangaiah Yadav[3], Dr.C.Prakasa Rao[4] Dr.M.V.Sruthi[5], Dr.D.Rajani[6]
[1]*Dean II&D and Professor of ECE Department, Sree Venkwateswara College of Engineering, North Rajupalem, Nellore, Andhra Pradesh, India – 524316, Email ID: nosinakc@gmail.com*
[2]*Assistant Professor, ECE Department, GNITS, Hyderabad, Email ID: c.padmaja@gnits.ac.in*
[3]*Associate Professor, ECE Department, Chaitanya Bharathi Institute of Technology, Proddatur, Kadapa district, Andhra Predesh, India – 516360, Email ID: ganga.486@gmail.com*
[4]*Principal & Professor of CSE, Sree Venkwateswara College of Engineering, North Rajupalem, Nellore, Andhra Pradesh, India – 524316, Email ID: prakashsvcn@gmail.com*
[5]*Associate Professor & HOD, ECE Department, Dr.K.V.Subba Reddy Institute of Technology, Kurnool, Andhra Pradesh, India, Email ID: shruthimv@gmail.com*
[6]*Professor & HOD, ECE Department, Sree Venkwateswara College of Engineering, North Rajupalem, Nellore, Andhra Pradesh, India – 524316, Email ID: rajini.d2010@gmail.com*
**Corresponding author*

ARTICLE INFO

Received: 23 Dec 2024
Revised: 10 Feb 2025
Accepted: 24 Feb 2025

ABSTRACT

A major challenging issue in the today's internet is the secure transmission of the images. There are methods that are been developed for secure transmission, but there is every possibility for acquiring the image and to change the content in the image. Most of the methods are complex and diesign is also very difficult. In this paper, we proposed a novel method for transmitting the image over the internet. The proposed method is based on original image to be sent, a cover image which is also called as reference image, three secret keys or passwords. It's like a triple protection with the help of secret keys and at the same time cover image is used to encode the pixel values in to index values. After images decryption, the image quality has been verified with the original image for the image quality assessment. In the proposed method it is very difficult to retrieve the original image from the encrypted image.

Keywords: Image, data image, cover image, Encryption, decryption, key, index value, pixel value.

1. INTRODUCTION

Image processing [1] is all about taking an image; process it and return an image as output. The processing may be display and print, image editing, image enhancement, feature detection and image compression. Image processing is majorly used in biology astronomy, medicine, security, biometric, satellite, Textiles, material Science, military, film industry, document processing, graphic arts, printing industry. The methods of image processing [2-4] are analog and digital image processing. The principle advantage of Digital Image Processing methods is its versatility, repeatability and the preservation of original data precision. Image is a two dimensional light intensity function f(x,y), where x and y are spatial coordinates.

Images are classified [5] as

(a) Binary image
(b) Gray scale image
(c) Colour image and
(d) Multispectral image

The RGB (Red, Green and Blue) colour model [6] is very close to the way we perceive colour with the R, g and b receptors in our retinas. The basic colour in the television or any other display is because of the mixture of R, G and B. It is the basic colour model used in computers and for web graphics, but it cannot be used for print production. These images are shared or transferred securely via internet. There are a number of methods available for image security.

The process of converting readable format into unreadable format is called encryption and the information after the encryption process is called "Cipher text". The process of retrieving the original information from the cipher text is called decryption. The study on encryption and decryption is called cryptography [7]. There are two types of cryptography techniques [8]. They are secret key and public key cryptography techniques [14] [15]. Here we used secret key cryptography technique, where the key is known to only sender and receiver.

2. LITERATURE REVIEW

There is a number of image encryption techniques proposed. In this section some of the existing techniques are discussed. Image Encryption Using Affine Transform and XOR Operation proposed by Nag Amitava, et al [9]. This method is based on the shuffling of image pixels and then XOR with the original image. The total key size used in this method is 64 bit key.

Permutation based image encryption technique proposed by pavani, et al [10]. This method is based on random pixel permutation to maintain the quality of the image. The technique involves three different phases in the encryption process. The first phase is the image encryption. The second phase is the key generation phase. The third phase is the identification process. This method provides confidentiality to colour image with less computations Permutation process is much quick and effective. The key generation process is unique and is a different process. It is a simple technique, where the intruders can able to retrieve the original image.

Data encryption using images that explore random spatial distribution method proposed by Gadhella et al.[11]. In this method, encryption and decryption is performed by replacing each pixel value with ASCII value. The major disadvantage of this method is it is a time consuming process.

Image Cryptography proposed by Niraj Kumar and Prof Sanjay Agrawal [12]. In this method requires two different public keys in the cryptography process. Key generation function coding is different from encryption and decryption program due to hide values from the user and hacker. This method requires more computation time and power.

A fast colour image encryption algorithm based on hyper-chaotic systems proposed by Norouzi B et al. [13]. This method consists of two stages based on permutations and diffusion stages. In permutations stage pixels are shifted from one place to other, where as in diffusion stage, the pixel values of the shuffled image is modified. This method requires a large key space then only the plain image and cipher image are entirely different.

A novel triple image encryption method has been proposed by xingyuan wang et al. [16]. In this method, authors proposed three stages, such as generation of key generation, three gray plane images are encrypted, and the cipher images are included in the colour image. The process is complicated, because in the second stage, it requires SHA algorithm for encryption.

Sara T Kamal has proposed a method [17] for medical image encryption that is based on splitting of the image into blocks. Then these image blocks are scrambled using zig zag pattern. Then ration will be done, and finally permutation is performed. This method is used only for the encryption of medical images, and it is tested on other types of images.

Ahmad et al., has proposed a method for image encryption using chaotic sequence [18] that uses various functions like tent, logistic and sine maps. Along with these it is also uses OR or XOR operation. But the problem with this method is that, it can't be implemented for all the types of images and it is suitable only for gray scale image.

Ruoyu zhao et al., proposed an encryption method [19] for the images that are stored in the cloud. It is based on three pixel extract scheme. The problem in this method is that, finding the formulae for the rank functions that are used in the method.

Bouteghrine et al., proposed a method [20] for image encryption for colour images using three dimensional discrete time chaos system that is based on confusion and diffusion mechanisms. This can be implemented using FPGA along with real time images.

Chun lai li et al., proposed a method [21] for image encryption which is based on multiplication diffusion and with bit level scrambling. This method is used only for encryption of gray scale images. The efficiency of the system is low. There is a scope for improvement in proving better image encryption. At the same time this method is not suitable for colour image [22] encryption.

M Z Talhaoui et al., proposed a method [23] for image encryption using bulban chaotic map. In this method the pixels are processed to either row or column level. In addition with the map function, it also uses modulo function for performing the image encryption. This is not suitable for colour images and high resolution images.

Manish Gupta et al., proposed a method [24] for image encryption. In this method keys are generated based on crossover and mutation operations. Here the 64 bit plain text is encrypted using 80 bit key. Here the method can be enhanced by using the more number of bit flips in the key generation.

Each of the image encryption method has its own problem. Here we proposed a image encryption method, which is very difficult to decrypt for the hackers with a cover image and with three secret keys. Proposed method is described in the next section.

3. PROPOSED METHOD

Proposed method is processed with original image, cover image and with three secret keys. Here we need two images called original image which is to be transferred and a cover image for providing the security for data image. Proposed method looks simple, but it most effective to provide the security for the image data. The entire image encryption method is based on a plain image, reference image, three secret keys and three random data. For the image encryption, we have used colour images. This method is very effective because of three secret keys that are used in the process of encryption. Each secret key is involved with a random number. That means someone wants to decrypt the image data certainly it requires three keys along with three random numbers, which is usually not possible to identify. Image security is provided not only with respect to number of keys, it also based on the reference image. The reference image is called as cover image. The requirement for the cover image is that, it needs to have complete range of colours in the image. Whether it is transmitting image or the cover image, it is divided into three planes. This will be providing the data in a deep fine format. The security is provided through each and every plane of the image. Though the image is splitted in RGB planes, the processing is done with the pixel location value called index instead of pixel value. If the third party user finds the image data, it appears like random data and unable to understand the data in it. Even it is very difficult identify that, it is a colour image. Means that, the proposed method provide multi level image data security with the aspects of image planes, three security keys, and three random data used. Let's see the actual procedure how the data encryption and decryption is done. Fig.1 shows the encryption process. In this process a data image, cover image, three secret keys (or also called as passwords) and random data is used. In the encryption block diagram both cover and data images are divided in to RGB planes. By using cover image, the pixel values of data image are changed into index values. Here the pixel value of a plane is verified in the cover image, if both the pixel values are matched, then the index location of pixel value in cover image is retrieved and it has been used further instead of pixel values. This means, the operations are not performed directly on pixels rather performed on index values. The major function that has been used in both encryption and decryption is the ex-or [25][26]. This is a very powerful operator which is popularly used in security algorithms.

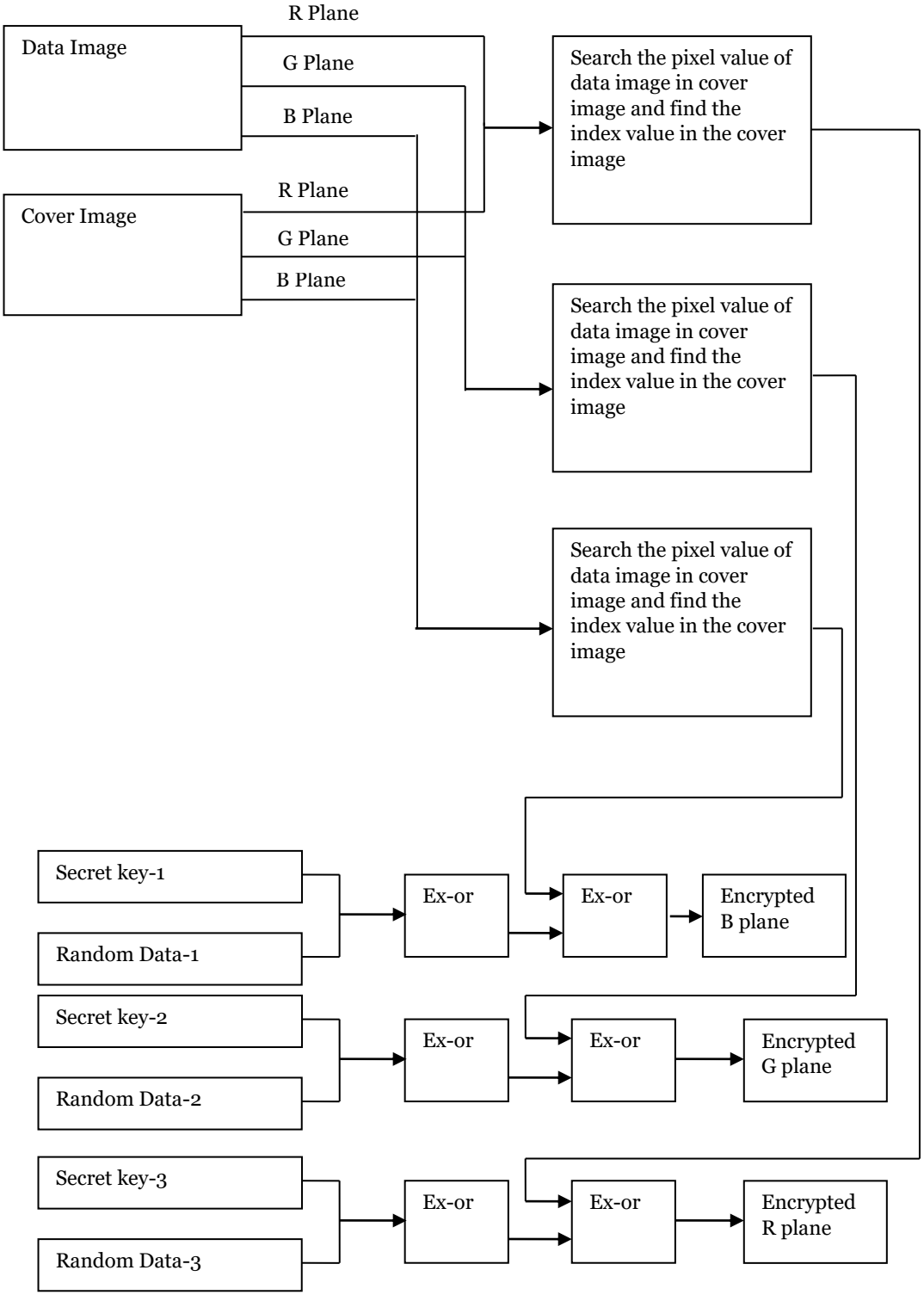

Fig.1: Encryption Block Diagram

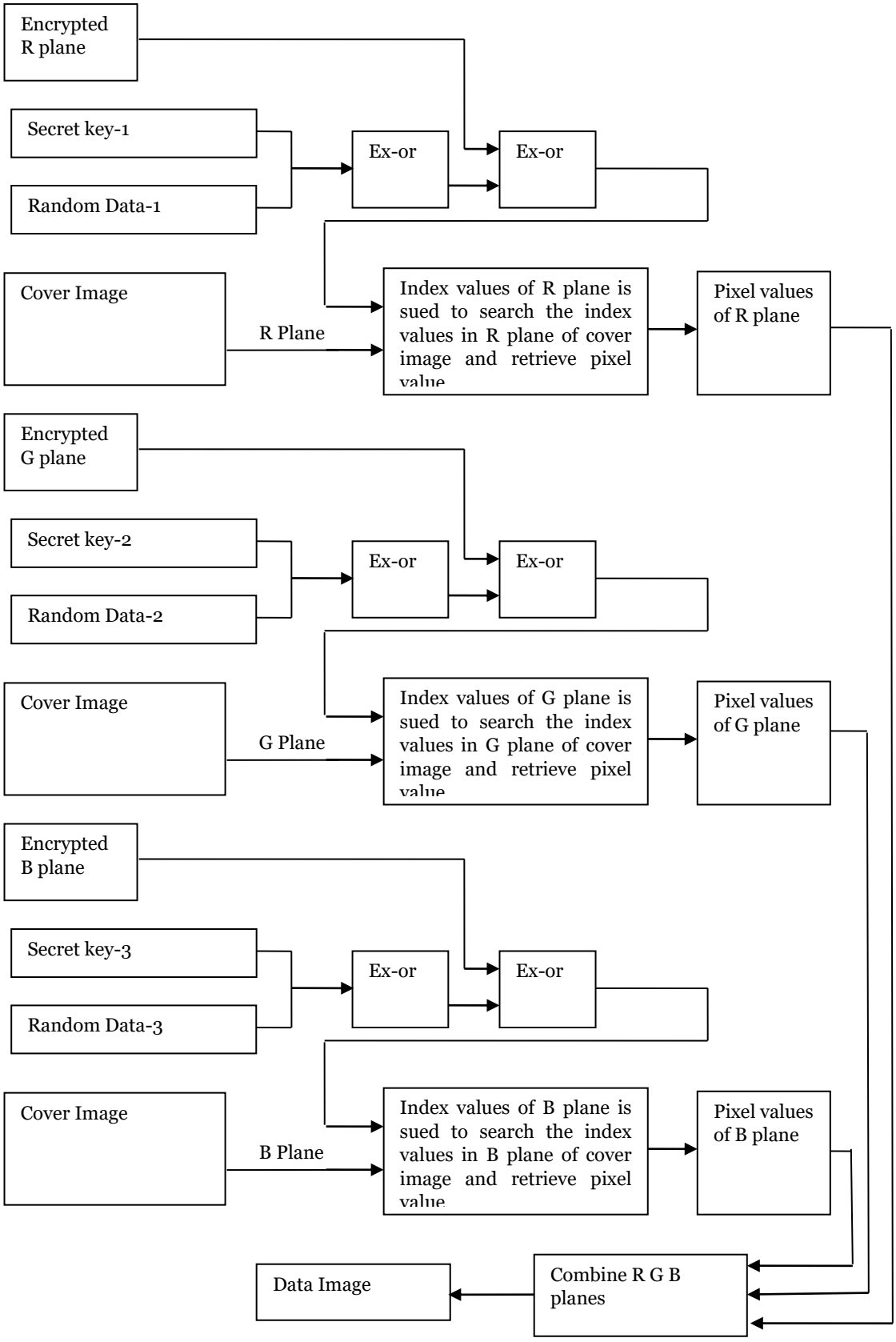

Fig.2: Decryption Block diagram

Fig.2 shows the block diagram for decryption. In this the received encrypted data is being processed and retrieving the RGB planes and combining them to get the data image transferred from the sender side.

The encryption and decryption algorithms are discussed below

Encryption Algorithm:

1. Select the data image(Image to be transferred)
2. Select the cover image.
3. CI=Read the cover image
    (i) r(CI) – Red plane
    (ii) g(CI) – Green plane
    (iii) b(CI) – Blue plane
4. DI=Read the data image
    (i) r(DI) – Red plane
    (ii) g(DI) – Green plane
    (iii) b(DI) – Blue plane
5. do
    locate r(DI) pixel values in r(CI) and store the index value of r(CI)
    repeat for all the pixel values of r(DI)
    lr(DI) – index values of data image pixels of red plane in cover image
    repeat this for g and b planes
    lg(DI) – index values of data image pixels of green plane in cover image
    lb(DI) – index values of data image pixels of blue plane in cover image
   end
6. Generate three random data ran(i), ran(j), ran(k)
7. choose three passwords password(i), password(j), password(k)
8. cipher_r = lr(DI) exor ran(i) exor password(i)
9. cipher_g = lg(DI) exor ran(j) exor password(j)
10. cipher_b = lb(DI) exor ran(k) exor password(k)

Decryption Algorithm:

1. Receive cipher_r, cipher_g, cipher_b
2. Receive three random data ran(i), ran(j), ran(k)
3. With the use of passwords password(i), password(j), password(k)
4. decipher_r = cipher_r exor ran(i) exor password(i)
5. decipher_g = cipher_g exor ran(j) exor password(j)
6. decipher_b = cipher_b exor ran(k) exor password(k)
7. Select the cover image to retrieve the original image
8. CI=Read the cover image
    (i) r(CI) – Red plane

(ii) g(CI) – Green plane

(iii) b(CI) – Blue plane

9. do

locate decipher_r pixel values in r(CI) and store the index value of r(CI)

repeat for all the pixel values of decipher_r

decipher_r – index values of data image pixels of red plane in cover image

repeat this for g and b planes

decipher_g – index values of data image pixels of green plane in cover image

decipher_b – index values of data image pixels of blue plane in cover image

end

10. Original image is recovered

With the help of this image encryption and decryption algorithms, one can provide security for the image and can shared easily. Because of the multi level security for the image, very difficult to retrieve the original image from the encrypted form. The block diagrams of the simulation environment and the corresponding processes involved in encryption and decryption are discussed in the next section.

4. RESULTS AND DISCUSSION

The proposed method is implemented using LabVIEW 2015. Proposed method has provided better security compared with all other existing techniques. This method is highly secured as it requires a cover image and three secret keys to retrieve the original image. Encryption and decryption simulation environments is shown in fig.3 and fig.4.

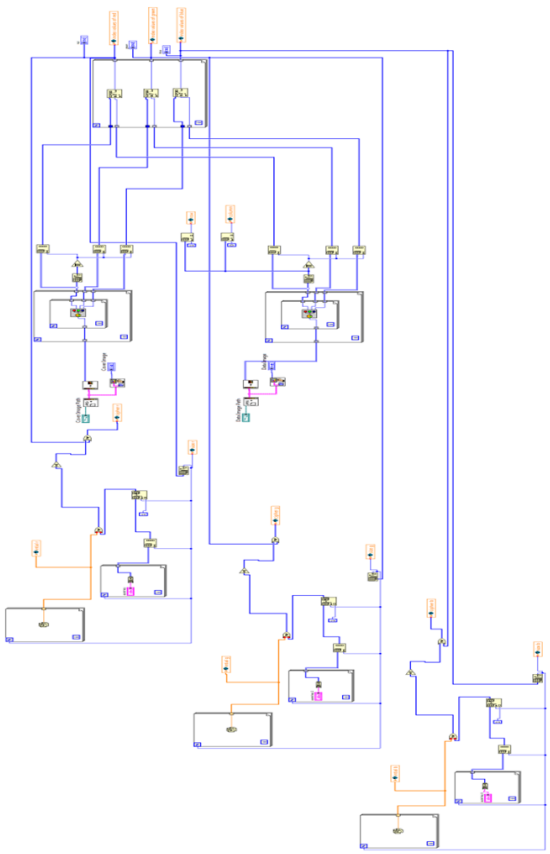

Fig 3: Simulation environment of encryption

The simulation environment of encryption process is shown in fig.3. In the encryption, the image needs to be sent is known as data image and the reference image taken to transfer the data image is known as cover image. In the first phase cover and data images are divided into RGB planes. Ex-or is performed over RGB planes along with secret key, and random data. Here in each plane the pixels values are altered in to index values using cover image. After encryption instead of an image, here values are transmitted and are not being identified by other people. The simulation environment of decryption process is shown in fig.4. The reverse operation is performed here to retrieve the original image.

Image encryption using cover image and three secret keys for RGB planes is shown in fig 5.

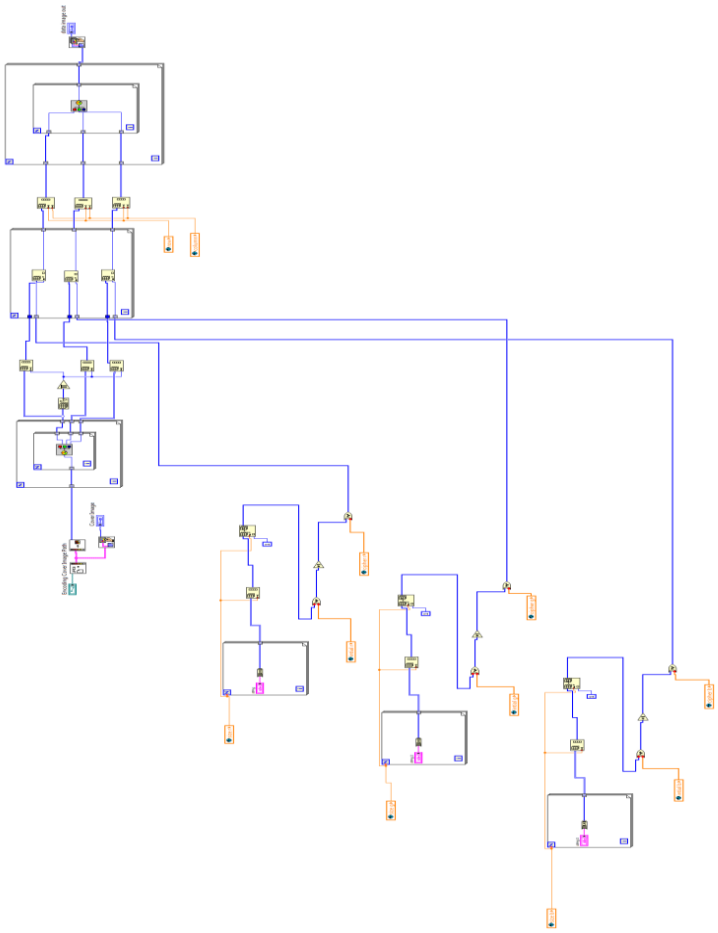

Fig 4: Simulation environment of decryption

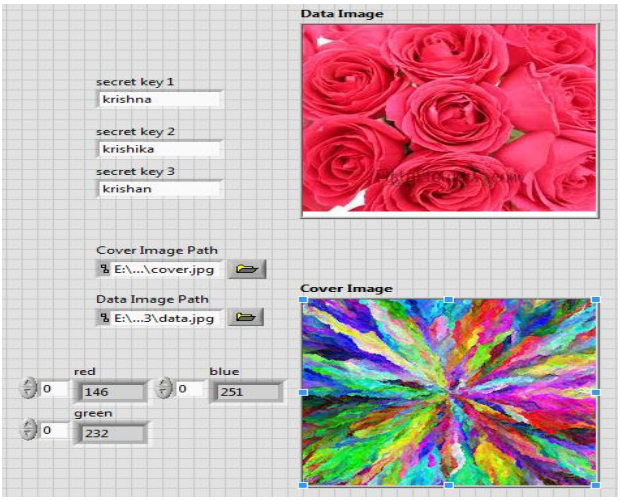

Fig 5: Image encryption

Fig 6 shows the image decryption with wrong password credentials. As it is mentioned the secret key “krishna” is for Red plane, “krishika” for Green plane and “krishan” for Blue plane. If the cover image is correct and if any one of the password is wrong, it is not possible to retrieve the original image from the encrypted one.

It is also not possible to retrieve the original image if the passwords are correct and cover image is wrong. This scenario is shown in fig 7.

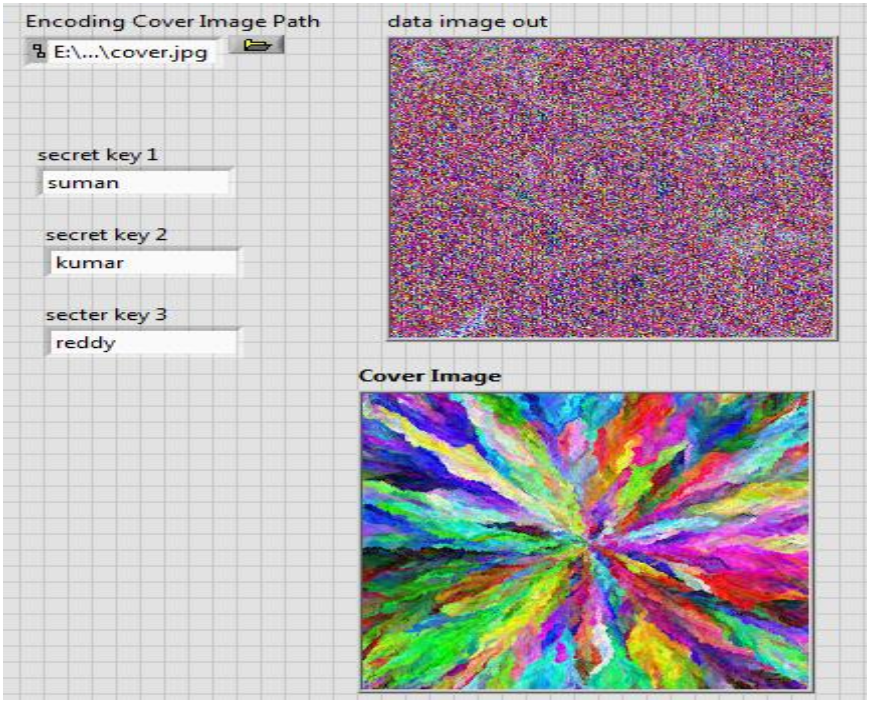

Fig 6: Decryption using correct cover image with wrong passwords

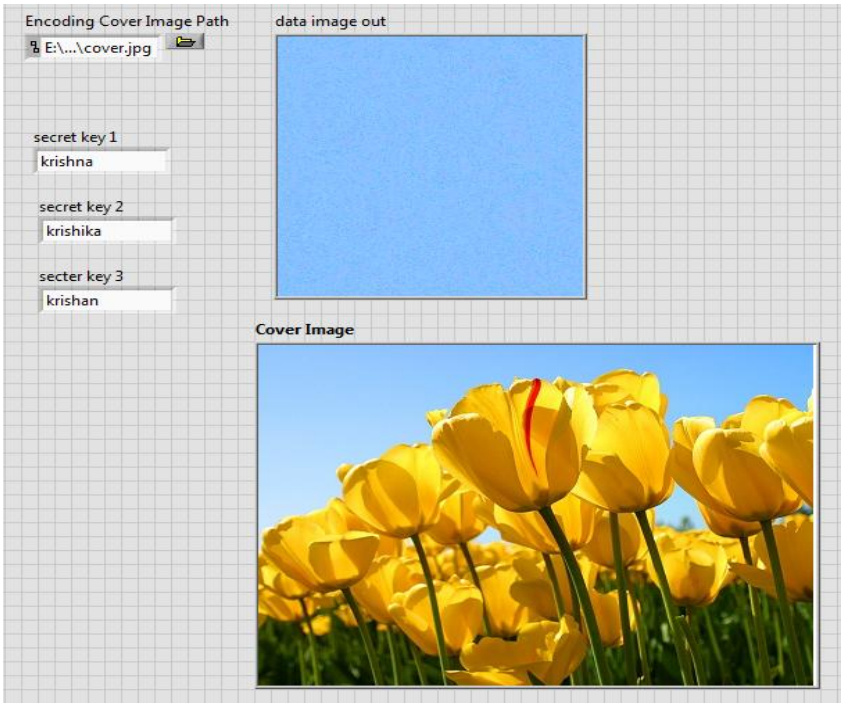

Fig 7: Decryption using correct passwords and with wrong cover image

From the above two cases it is not possible to retrieve the original image. That is why the proposed method is highly secured. The original image retrieved only when cover image and all the three passwords are correct and is shown in fig 8. In order to find the similarity and the quality of the encrypted and decrypted images, MATLAB is used to

find the SSIM and PSNR of the images. The corresponding values of SSIM (Structural Similarity index) and PSNR (Peak Signal to Noise Ratio) have been tabulated in table.1.

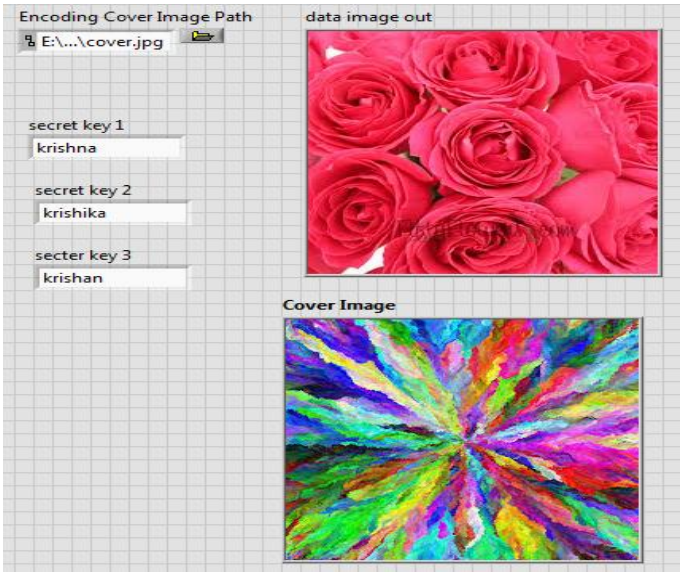

Fig 8: Decryption using correct passwords and cover image

Table.1: Comparison of various scenarios in the simulation

Scenario	SSIM	PSNR
Decryption using correct passwords and with wrong cover image	0.05	2.31
Decryption using correct cover image with wrong passwords	0.29	3.78
Decryption using correct passwords and cover image	0.9786	45.23

Table 2: Attacks on the Proposed Image Encryption Technique and Success Rate

Attack Scenario	**Success Rate (%)**
Brute Force Attack	0%
Known Plaintext Attack	10%
Chosen Plaintext Attack	15%
Chosen Ciphertext Attack	5%
Differential Cryptanalysis Attack	5%
Meet-in-the-Middle Attack	10%
Side Channel Attack	15%
Fault Injection Attack	8%
Social Engineering Attack	15%

From the table.1 it is evident that, the original image has been retrieved only when the cover image and three passwords are correct. In other scenarios it failed to retrieve the image that has been transferred.

Table 2 presents a description of various attacks on the proposed image encryption technique and their estimated success rates. These attacks include Brute Force, Known Plaintext, Chosen Plaintext, Chosen Ciphertext, Frequency Analysis, Differential Cryptanalysis, Meet-in-the-Middle, Side Channel, Fault Injection, and Social Engineering attacks. The success rates provided serve as rough estimates and reflect the likelihood of each attack being successful. It is important to note that the success rates depend on factors such as algorithm complexity, key length, and security measures implemented in the encryption method. Thorough security evaluations and analysis are necessary to accurately assess the resistance of the proposed technique against these attacks.

CONCLUSION

It is very much evident that the above proposed method is a novel one in terms of the security that has been provided for the RGB planes with each secret key and a cover image for the original image retrieval. It is very difficult to identify the length of secret keys used for RGB planes. Though the Ex-or operation looks simple but it provides a great security for image. Along with the keys cover image plays a vital role in image security. With this multi level image security it may not be possible to predict cover image and secret keys for getting the data image.

REFERENCES

[1] Sonka, Milan, Vaclav Hlavac, and Roger Boyle. *Image processing, analysis, and machine vision*. Cengage Learning, 2014.

[2] Masters, Barry R., Rafael C. Gonzalez, and Richard Woods. "Digital image processing." *Journal of biomedical optics* 14.2 (2009): 029901.

[3] Abràmoff, Michael D., Paulo J. Magalhães, and Sunanda J. Ram. "Image processing with ImageJ." *Biophotonics international* 11.7 (2004): 36-42.

[4] Plataniotis, Konstantinos, and Anastasios N. Venetsanopoulos. *Color image processing and applications*. Springer Science & Business Media, 2013.

[5] Singh, Krishna Kant, and Akansha Singh. "A Study Of Image Segmentation Algorithms For Different Types Of Images Different Types Of Images." *International Journal of Computer Science Issues* 7.5 (2010).

[6] Reinhard, E., Adhikhmin, M., Gooch, B., & Shirley, P. (2001). Color transfer between images. *IEEE Computer graphics and applications*, *21*(5), 34-41.

[7] Patel, Komal D., and Sonal Belani. "Image encryption using different techniques: A review." *International Journal of Emerging Technology and Advanced Engineering* 1.1 (2011): 30-34.

[8] Pakshwar, Rinki, Vijay Kumar Trivedi, and Vineet Richhariya. "A survey on different image encryption and decryption techniques." *International journal of computer science and information technologies* 4.1 (2013): 113-116.

[9] Nag, Amitava, et al. "Image encryption using affine transform and XOR operation." *Signal Processing, Communication, Computing and Networking Technologies (ICSCCN), 2011 International Conference on*. IEEE, 2011.

[10] Indrakanti, Sesha Pallavi, and P. S. Avadhani. "Permutation based image encryption technique." *International Journal of Computer Applications (0975–8887) Volume* (2011).

[11] Gadelha, Mikhail YR, Cicero Ferreira Fernandes Costa Filho, and Marly Guimarães Fernandes Costa. "Proposal of a cryptography method using gray scale digital images." *Internet Technology And Secured Transactions, 2012 International Conference for*. IEEE, 2012.

[12] Kumar, Niraj, and Sanjay Agrawal. "An efficient and effective lossless symmetric key cryptography algorithm for an image." *Advances in Engineering and Technology Research (ICAETR), 2014 International Conference on*. IEEE, 2014.

[13] Norouzi, B., Mirzakuchaki, S.: A fast color image encryption algorithm based on hyper-chaotic systems. Nonlinear Dynamics 78, 995–1015 (2014).

[14] N.Krishna Chaitanya, A.Suman kumar reddy, “Simple and efficient data encryption algorithm” International Journal of Scientific & Technology Research Volume 8, Issue 12, December 2019, PP. 2520-2523.

[15] N.Krishna Chaitanya et. al., “Image hiding in an image using Labview” TEST Engineering and Management, Volume 83, June 2020, PP. 18148-18154.

[16] Wang, Xingyuan, Cheng Liu, and Donghua Jiang. "A novel triple-image encryption and hiding algorithm based on chaos, compressive sensing and 3D DCT." *Information Sciences* 574 (2021): 505-527.

[17] Kamal, Sara T., et al. "A new image encryption algorithm for grey and color medical images." *IEEE Access* 9 (2021): 37855-37865.
[18] Pourjabbar Kari, Ahmad, et al. "A new image encryption scheme based on hybrid chaotic maps." *Multimedia Tools and Applications* 80.2 (2021): 2753-2772.
[19] Zhao, Ruoyu, et al. "TPE2: Three-pixel exact thumbnail-preserving image encryption." *Signal Processing* 183 (2021): 108019.
[20] Bouteghrine, Belqassim, Camel Tanougast, and Said Sadoudi. "Novel image encryption algorithm based on new 3-d chaos map." *Multimedia Tools and Applications* 80.17 (2021): 25583-25605.
[21] Li, Chun-Lai, et al. "Image encryption scheme with bit-level scrambling and multiplication diffusion." *Multimedia Tools and Applications* 80.12 (2021): 18479-18501.
[22] Chaitanya, N. Krishna, et al. "IoT-enabled Moving Wheelchair with Obstacle Detection and Continuous Health Monitoring." *2024 Second International Conference on Emerging Trends in Information Technology and Engineering (ICETITE)*. IEEE, 2024.
[23] Talhaoui, Mohamed Zakariya, Xingyuan Wang, and Mohamed Amine Midoun. "Fast image encryption algorithm with high security level using the Bülban chaotic map." *Journal of Real-Time Image Processing* 18.1 (2021): 85-98.
[24] Gupta, Manish, Kamlesh Kumar Gupta, and Piyush Kumar Shukla. "Session key based fast, secure and lightweight image encryption algorithm." *Multimedia Tools and Applications* 80.7 (2021): 10391-10416.
[25] Qu, Lingfeng, Hongjie He, and Fan Chen. "On the security of block permutation and co-XOR in reversible data hiding." *IEEE Transactions on Circuits and Systems for Video Technology* (2021).
[26] Thinnukool, Orawit, Thammarat Panityakul, and Mahwish Bano. "Double Encryption Using Trigonometric Chaotic Map and XOR of an Image." *CMC-COMPUTERS MATERIALS & CONTINUA* 69.3 (2021): 3033-3046.