Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, No. 5, July : 2023

AN IMPROVED CRYPTOSYSTEM FOR SECURED IMAGESHARING ON IOT DEVICES

Mrs.T.SRUJANA Assistant professor, Department of ECE, Sree Dattha Institute Of Engineering and Science, Hyderabad

Abstract : Image encryption can be accomplished by scrambling image pixel positions using different techniques in the spatial domain .One example is the recursive sequence based image scrambling approach. It scrambles images using different recursive sequences such as the Fibonacci sequence, Cellular automata and chaotic maps .Image encryption can also be accomplished by scrambling coefficient matrices/blocks in the transform domain. Nevertheless, these approaches have extremely low security levels due to the lack of security keys or the small key space. Furthermore, the permutation-only based encryption schemes areknown to be vulnerable for plaintext attacks. Another approach for image encryption is to change image pixel values based on the combination of image bit plane decomposition and logic operations. The security level of this method is much lower because the results of its decomposition process and logic operations are predictable. It is not immune to plaintext attacks. To achieve higher levels of security, one solution is to change image pixel values while scrambling the positions of image pixels or blocks using different techniques. In this paper, we introduced a new gray/RGB image encryption and decryption algorithm using edgemapped combined key generation (EM-CKG), which is a binary image with the same size as the original image to be encrypted.

IndexTerms **–** Image Encryption, Decryption, Edge mapped Combined key generation(EM-CKG).

I.INTRODUCTION

Network technologies and media services provide ubiquitous conveniences for individuals and organizations to collect, share, or distribute images/videos in multimedia networks and wireless or mobile public channels [1]. Image security is a major challenge in storage and transmission applications [2]. For example, video surveillance systems for homeland security purposes are used to monitor many strategic places such as public transportation, commercial and financial centers. Large amounts of videos and images with private information are generated, transmitted, or restored every day. In addition, medical images with a patient's records may be shared among the doctors in different branches of a health service organization over networks for different clinical purposes. These images and videos may contain private information. Providing security for these images and videos becomes an important issue for individuals, business and governments as well. Moreover, applications in the automobile, medical, construction and fashion industry require designs, scanned data, and blue-prints to be protected against espionage. Considering the long lifetime of image in the afore-mentioned domains, it is imperative to develop and employ techniques which protect the content throughout their lifetime. Image encryption is an effective approach to protect images or videos by transforming them into completely different formats several interesting approaches for image encryption have been developed. One method based on the cryptography concept considers images as data blocks or streams. It encrypts images block byblock or stream by stream using different techniques. Data Encryption Standard (DES) and Advanced Encryption Standard (AES) are two examples of this approach. However, such encryption methods incur large computational costs and show poor error resilience [3].

In the present era of computers and fast communication, one needs to protect communicated information (message or plain text) from unauthorized user, while sending it through any electronic media. So, security of visual data is an important issue in the design ofcommunication systems. Data hiding techniques and visual cryptography are used to introduce confidentiality and security when visual data are transmitted through unsecured communication channels. Data hiding techniques try to embed data in digital media and transmit it in an imperceptible way [4]. The

private-key and the public-key are the two well-known cryptosystems, using these we enable to keep the secret data securely in such a way that that invader cannot able to understand what the secret data means. The data encryption standard (DES) and Rivest, Shamir, Adleman (RSA) and Advanced Encryption Standard (AES) are three representative methods[5].

Steganography is one of the data hiding technique in which Secret communications take place that conceal the very existence of the message [6]. Cryptography in another type of data hiding technique in which message to be hidden is encoded using encryption or coding techniques. Here we know that a message is there but cannot understand it. Watermarking is another technique in which information that is hided is directly related to the item in which it is embedded [7].

On the other hand, in visual cryptography or visual secret sharing (vss), the original input image is shared between a set of participants P by a dealer (secret image holder). Based on the sharing policy, only qualified subsets of participants can recover the original input image.

Two important factor s that used to determine the efficiency of any visual cryptography scheme, namely:

1) The quality of the reconstructed image and
2) The pixel expansion (m).

II.RESEARCH METHODOLOGY

Behrouz Zolfaghar proposed regarding coded caching traditionally adopt a simple network topology consisting of a single server, a single hub, a shared link connecting the server to the hub, and private links which connect the users to the hub [1]. Jawad Ahmad presents a secure real-time scheme for IoT systems by intelligent integration of occupancy monitoring and chaos-based lightweight image encryption. Firstly, the real-time video was usedto extract video frames through the single overhead camera. When people are detectedin a frame, the intelligent system encrypts the current frame and also counts the people in/out and send occupancy count information to the cloud computing platform [2]. Seyed Mohammad a design of the compound one- dimensional chaotic function by coupling piecewise nonlinear chaotic map and nearest-neighboring coupled-map lattices (NCML) suggests self-adaptive color imageencryption. The coupling and nonlinear structure of the compound chaotic function enhances cryptosystem security. The self-adaptive color image encryption is carried out by using one half of the image data for encryption of the other half of the image recursively. The salient features of the proposed image encryption scheme are high security level, high sensitivity, high speed and large key space [3].LEI ZHENG proposed In wireless multicast networks, different users may have quite different link qualities to the server, which will degrade the multicast performance of the coded caching scheme. In order to effectively handle the asymmetric link qualities and fulfill the fairness delivery requirement by a different user, a parallel delivery scheme is proposed to organize the wireless multicast physical channels into multiple logic parallel partially shared links [4].

Takeshi Koshiba proposed acomprehensive survey can highlight existing trends and shed light on less-studied topics in the area of chaotic image encryption [5]. Louis M.pecora proposed The convergence of the two systems to identical trajectories is a surprise. they show how people originally thought about this process and how the concept of synchronization changed over the years to a more geometric view using synchronization manifolds. they also show that building synchronizing systems leads naturally to engineering more complex systems whose constituents are chaotic, but which can be tuned to output various chaotic signals [6]. Li-bo Zhang the shortcomings of TDBMP have been analysed and a chosen plaintext attack has been proposed to break the scheme. After that, they propose an enhanced algorithm to overcome the presented shortcomings in the above original scheme [7]. Shirin Saeedi Bidokhti proposed that improves either on rate or decoding latency over two baseline schemes that are based on standard coded caching [8]. Janan ayad proposed The sharing of information through unsecured networks like the internet has increasedfast recently. This information could be text, audio, image, or video. The

security of data transmission is an essential issue. Encryption is one of the most effective techniques to assure safe data transmission. Videos and Images size are very large andhave a high correlation between neighboring pixels, so the classical encryption techniques such as RSA, DES, AES, etc., cannot be utilized for image encryption while chaotic image encryption schemes, which use a high level of unpredictability in key generation, can solve this problem [9]. chinonso Okereke developed for image viewing applications using the Hill Cipher algorithm. This study aims to evaluate the image encryption quality of the Hill Cipher algorithm. Several traditional metrics are used to evaluate the quality of the encryption scheme. Three of such metrics have been selected for this study. These include, the Color Histogram, the Maximum Deviation (comparing the original image) and the Entropy Analysis of the encrypted image. Encryption quality results from all three schemes using a variety of images show that a plain Hill Cipher approach gives a good result for all kinds of images but is more suited for color dense images [10].

III PROPOSED METHOD

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.

3.1 ENCRYPTION ALGORITHM

Step 1: Select and read a gray/color (RGB) image to be encrypted
Step 2: Now, convert the image into number of bit planes using bit plane algorithm i.e., forgray scale '8' bit planes and for RGB image '24' bit planes
Step 3: Now select and read the two key images with the same size of input image.
Step 4: Apply edge mapping to get the binary information
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.
Step 6: Then do the XOR of bit planes of original gray/RGB 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 tostring and binary to decimal operations.
Step 9: Finally, we had a fully encrypted image with the CKG algorithm.

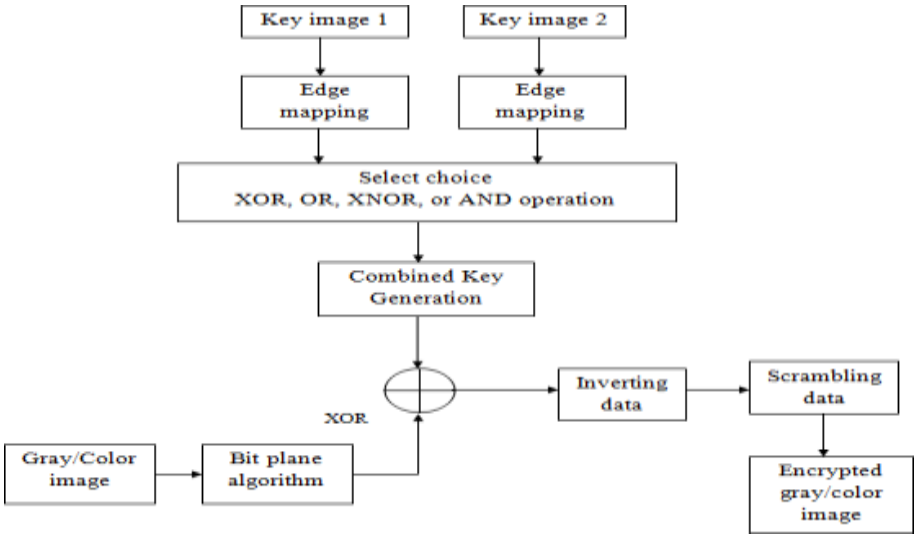

Fig.1 Block diagram of proposed EM-CKG encryption

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, No. 5, July : 2023

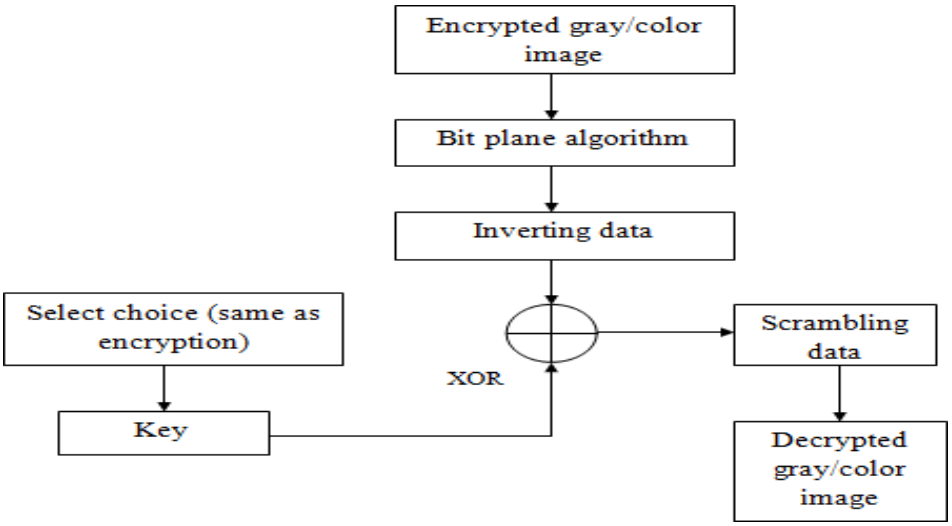

Fig.2 Proposed decryption algorithm.

3.2.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. 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 ofvalues 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. Bit plane 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 aspectof 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

For example, in the 8-bit value 10110101 (181 in decimal) the bit planes work as follows:

Table.1 Bit Plane

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

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, No. 5, July : 2023

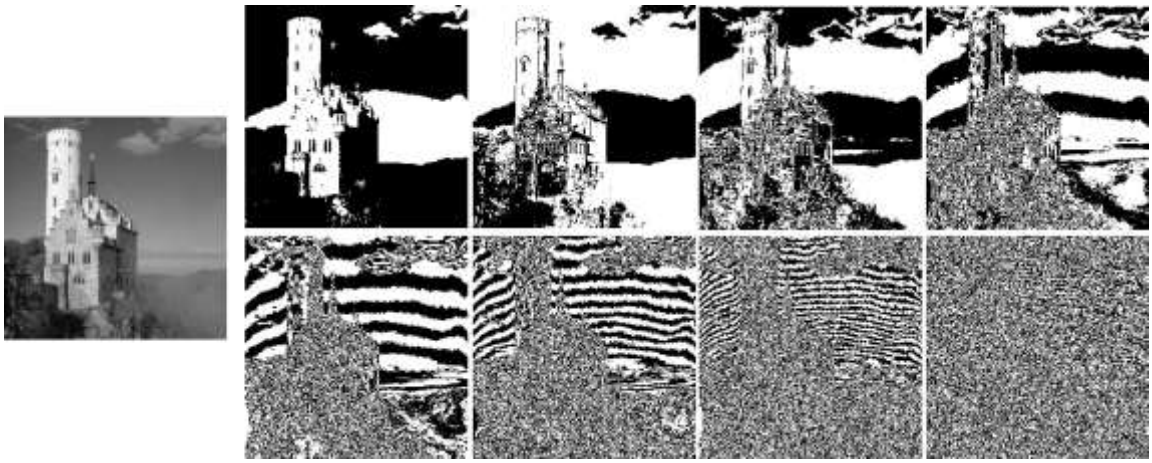

Fig.3 Example Of A Gray Scale Image Bit Planes

3.3 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.

3.4 SCARMBLING ALGORITHM

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

IV.RESULTS AND DISCUSSION

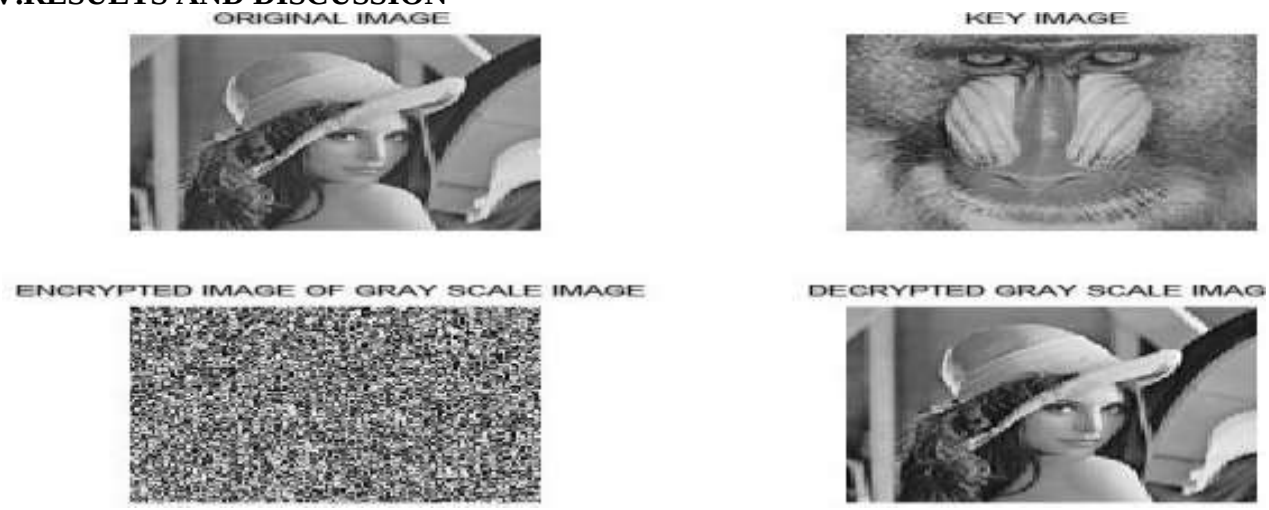

Fig.4 Image Encryption with Gray Scale.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, No. 5, July : 2023

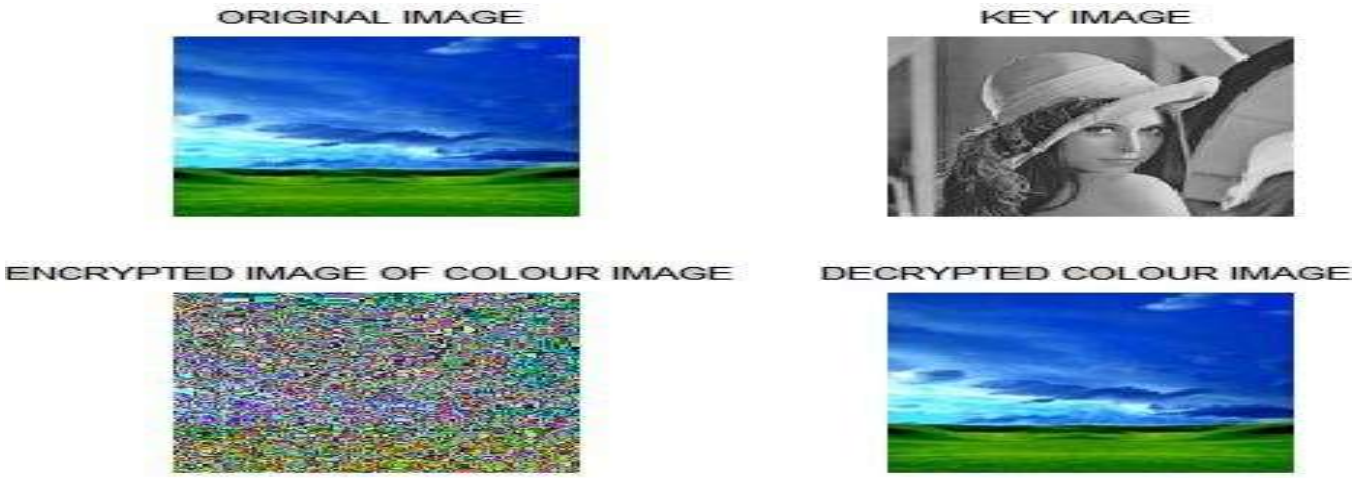

Fig.5 Image Encryption with color images

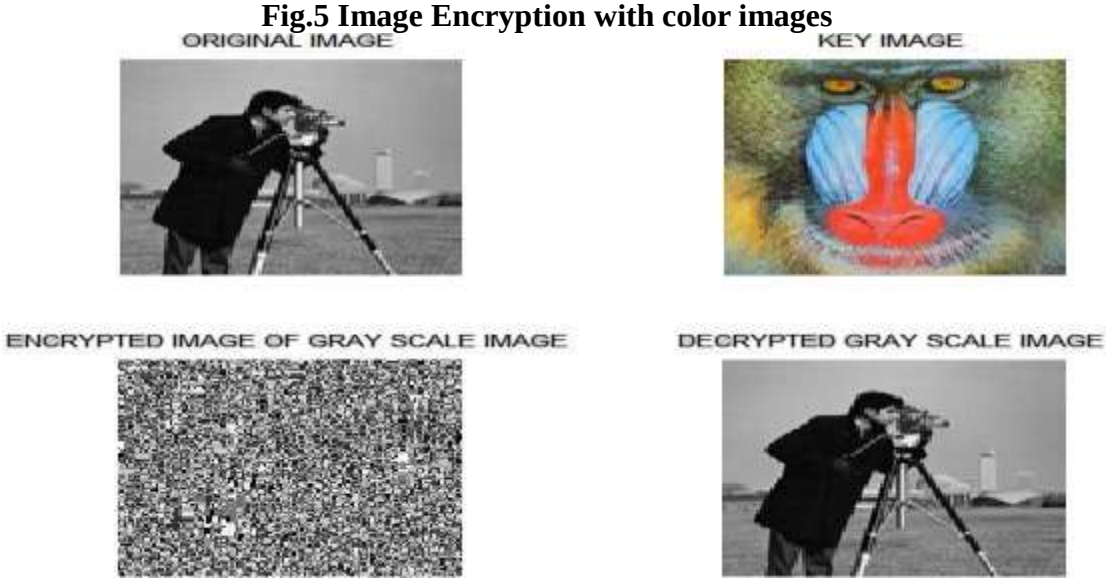

Fig.6 Image Encryption with Secret key image for Gray scale.

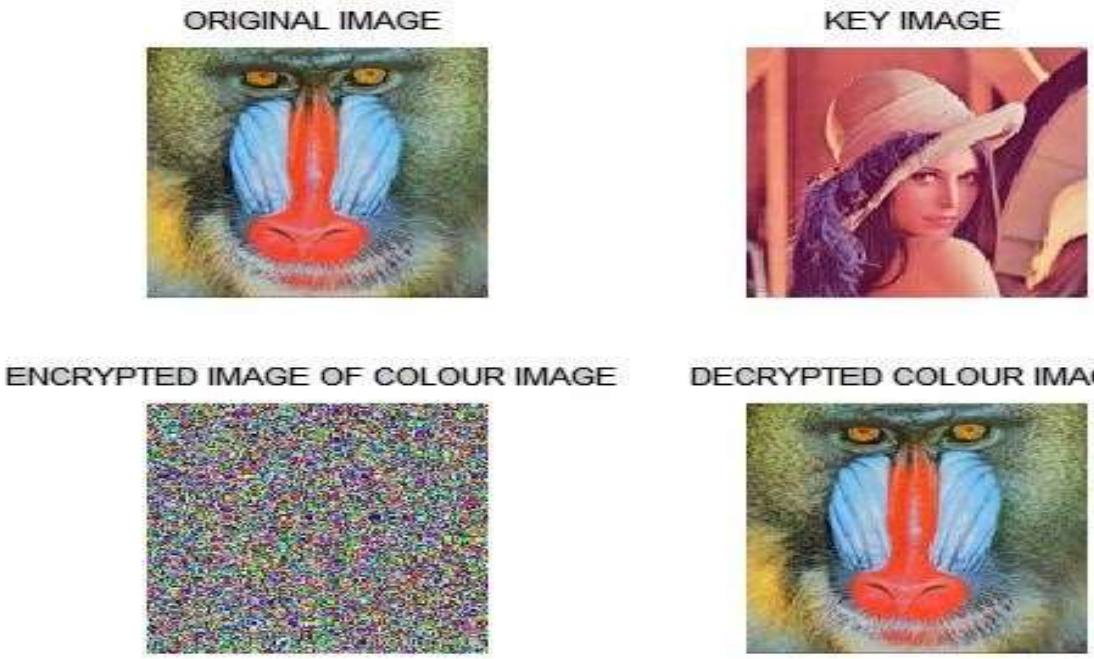

Fig.7 Image Encryption with Secret key image for Color images

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, No. 5, July : 2023

Fig.8 Image Encryption with two Secret Keys

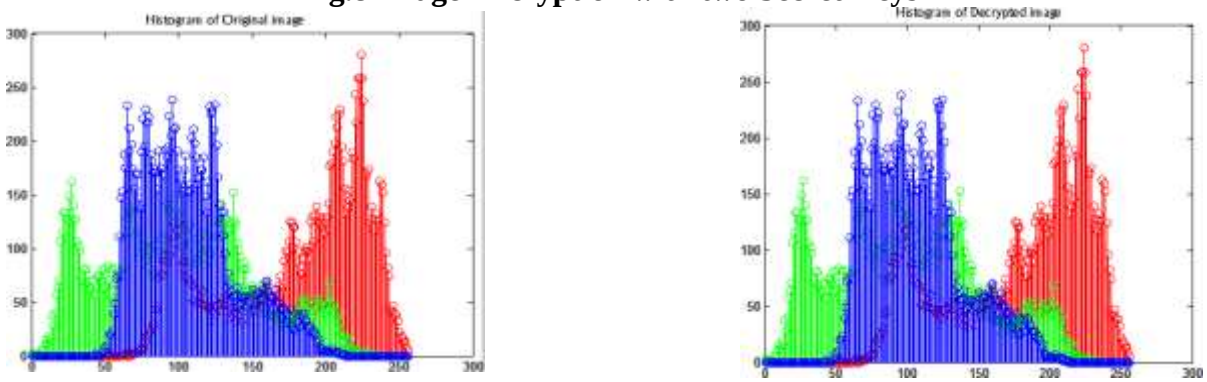

Fig.9 Histogram of original image and Decrypted image.

V.CONCLUSION

In IOT, introduces a new gray/RGB image encryption and decryption algorithm using edge mapped combined key generation (EM-CKG) with logical operations and scrambling approaches. The proposed algorithm has many advantages over existing single key image algorithms such as bit plane crypt and edge map crypt algorithms. 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].Cryptography in Hierarchical Coded Caching: System Model and Cost Analysis.AUTHOR: Behrouz Zolfaghari , Vikrant Singh , Brijesh Kumar Rai , Khodakhast Bibakand Takeshi Koshiba
[2].Secure Occupancy Monitoring System for IoT Using Lightweight Intertwining Logistic Map.AUTHOR: Jawad Ahmad , Hadi Larijani , Rohinton Emmanuel , Mike Mannion ,and Ayyaz-Ul-Haq Qureshi
[3].Using self-adaptive coupled piecewise nonlinear chaotic map for color imageencryption scheme.: Seyed Mohammad seyedzadeh,Seyyed Mohammad sadegh moosavi
[4].Delivery Design for Coded Caching Over Wireless Multicast Networks.AUTHOR: LEI ZHENG1,3, QIFA YAN2 , (Member, IEEE), QINGCHUN CHEN 3
[5].Chaotic Image Encryption: State-of-the-Art, Ecosystem, and Future Roadmap.AUTHOR: Behrouz Zolfaghari ,and Takeshi Koshiba .
[6].Synchronization in chaotic system.AUTHOR: Louis M.pecora,T.L carroll
[7].Cryptanalysis and Enhancements of Image Encryption Based on Three-dimensional Bit Matrix Permutation.AUTHOR: Li-bo Zhang, Zhi-liang Zhu, Ben-qiang Yang
[8]. State-Adaptive Coded Caching for Symmetric Broadcast Channels. AUTHOR: Shirin Saeedi Bidokhti Mich`ele Wigger, Aylin Yener, and Abbas ElGamal.
[9].Image Encryption using Chaotic Techniques: A Survey Study.AUTHOR : Janan ayad.
[10].Evaluation of the quality of an image encrytion scheme.AUTHOR: omoruyi Osemwegie, chinonso Okereke.