ISSN: 0975-3583,0976-2833 VOL12,ISSUE03,2021

A Robust and Secure Cryptanalysis Using Logical Scrambling with Histogram Matching

B. Bharathi[1], P. Suresh Kumar[1], Srikanth A[1]

[1]*Dept. of ECE, Sree Dattha Institute of Engineering and Science, Hyderabad, Telangana*

Abstract

Transmitting an image is an important and challenging task with higher security. The process of secure data transmission with scrambling and jumbling is known as cryptanalysis. This can be used inmany applications for confidentiality such as military, medical, satellite and web etc. Here, we introduced a new and novel cryptanalysis scheme with improved security using logical scrambling and histogram matching. The proposed algorithm can be easily adapted for real time application due to its ease of access and less storage capacity. Experimental analysis has been done on various test images such as medical, satellite and few of real images, also compared the original and decrypted images with histogram matching and subtraction approach.

Index terms: Cryptanalysis, bit planes, logical scrambling, histogram and bound map.

I. INTRODUCTION

Many wireless network technologies and media services were rendering ubiquitous conveniences for collecting, distributing and sharing of images, data sheets, files or videos over mobile networks or social media such as whatsapp, wechat, hike messenger and facebook etc, due to the rapid increase in sharing of digital information in almost each and every field. Among those most of them need to transmit the data securely in such a way that any unauthorized persons or parties were unable to see or detect the original data. For example, many places like commercial centers, financial centers and public transportations will be monitored by digital video surveillance systems for the purpose of homeland security. We need to restore, generate and transmit the large amount of data with higher security that cannot be seen by unauthorized persons. In addition to this, secure data transmission plays a vital role in medical field for sending or receiving the patient's information such as x-ray reports, magnetic resonance tomography (MRT) images, electro cardiogram (ECG) or electro encephalogram (EEG) among the many doctors from different centers of health service organizations (HSO) over cellular mobile or wireless networks for the purpose of diagnosis. All the above shared data may contain some private information, which is more confidential and could not be shown.Hence, secure data transmission is a highly challenging scenario in present years. Developing and hiring such schemes is very important to increase the lifetime of images, files or videos, which protects the content of original data for many yearsfrom hackers or unauthorized people [1]. Protecting images or videos is an effective approach [1], which transforms them into a different manner or format that cannot be detected by the third party.There are so many algorithm have been developed to provide more security, enhanced quality with easy implementation and faster calculations. Among them all of the techniques have their own drawbacks like computational complexity, time consumption, not suitable for 3D images etc., To overcome all the drawbacks, we introduced a novel and robustcryptanalysiswith logical scrambling and histogram matching, which will provide more security by generating two secret keys.

II. RELATED WORK

From the past decades there are so many image cryptographic algorithms have been developed to protect the images from unauthorized parties, which were looking to destroy the information sent by transmitter. In 1995 the first image and video encryption: from digital rights management to secured personal communication published by pommer andreas and uhl andreas. In [1] the authors said that an incorporated overview of schemes for encryption of images and videos will be provided by image and video encryption. This ranges from few commercial applications like digital video broadcasting

ISSN: 0975-3583,0976-2833 VOL12,ISSUE03,2021

(DVB) or digital audio broadcasting (DAB)to more research oriented topics and published content.The concept in [2] was published by B. Schineir, in which the theorital and practical knowledge of a cryptosystem has been provided to secure the multimedia.It was introduced in 1995 and very soon it became the standard text book for cryptography courses in all over the world.The author in [3] proposed a new invertible 2D map, called Line map, for encryption and decryption of image, which maps an image into an array of pixels and then maps it back to the original image. This approach shows the better performance than the previously existed 2D maps, in which only permutation was used. Another approach for image encryption in [4], which is proposed by kuang tsan lin, this approach utilized the both magic matrix scrambling and binary coding method to form a hybrid encoding method to encrypt an image. This will not provide any sort of distortion in decoding process, which means that the exact original image will be recovered at the receiver end. Anil kumar *et. al.* in [5] introduced a new image encryption technique based on chaotic standard map which uses extended substitution-diffusion scheme. This method uses linear feedback shift register to overcome the drawbacks of existing techniques by adding non-linearity. This approach is highly secured and faster than the conventional methods.

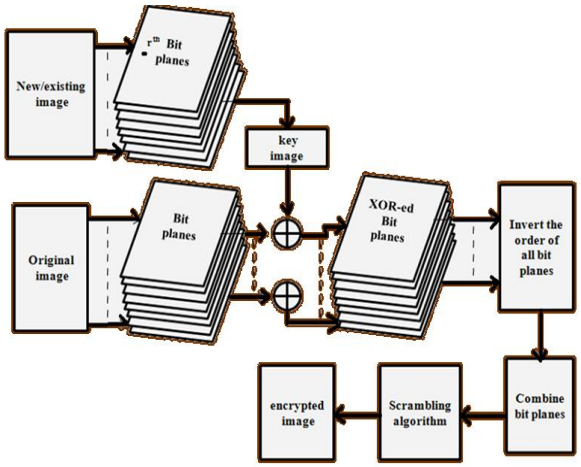


Fig. 1: Existing bit plane crypt algorithm.

Zhi liang zhu *et. al.* [6] introduced a chaos based symmetric image encryption using a bit level permutation, in which the Arnold cat map for bit level permutation proposed for an image cryptosystem to provide more security and faster simulations. An effective, secured, fast and cost effective image transmission scheme proposed in [7] employs encryption, compression and secured key exchanging along with the image transmission.

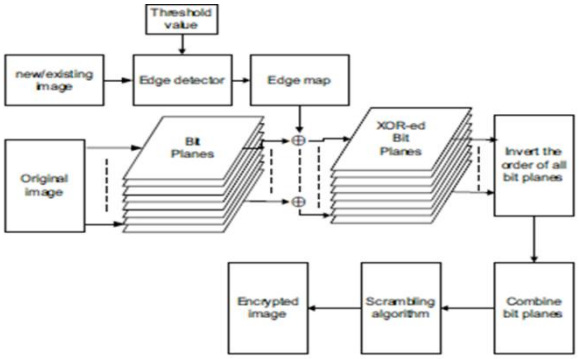


Fig. 2: Existing edge map crypt algorithm.

ISSN: 0975-3583,0976-2833 VOL12,ISSUE03,2021

Recently, an image encryption scheme based on fractional Fourier transform (FRFT), singular value decomposition and Arnold transform has been proposed in [10] to improve the security to enhance the quality of decrypted image. Image encryption technique using bit plane decomposition and scrambling was proposed by qiudong sun [8], which aims at the pixels positions interchanging and changing the gray values of pixels at the same time. This approach has better efficiency and properties than the random scrambling methods and it has more stability degree than the classical methods such as Arnold transform.

III. PROPOSED TECHNIQUE

Here in this, we proposed two lossless image crypto systems to provide higher security and lossless recovery of encrypted image at the receiver end. Those two algorithms are as follows:

1. Combined Bit plane(CBP)
2. Combined Bound map(CBM)

The proposed algorithm included with inverting and scrambling of data after doing the XOR operation for the combined key and input image bitplanes. Scrambling is done by converting the decimal or binary numbers into the strings and then converting them into binary to decimal values afterwards the values will be reshaped into the number of rows and number of columns of input image.

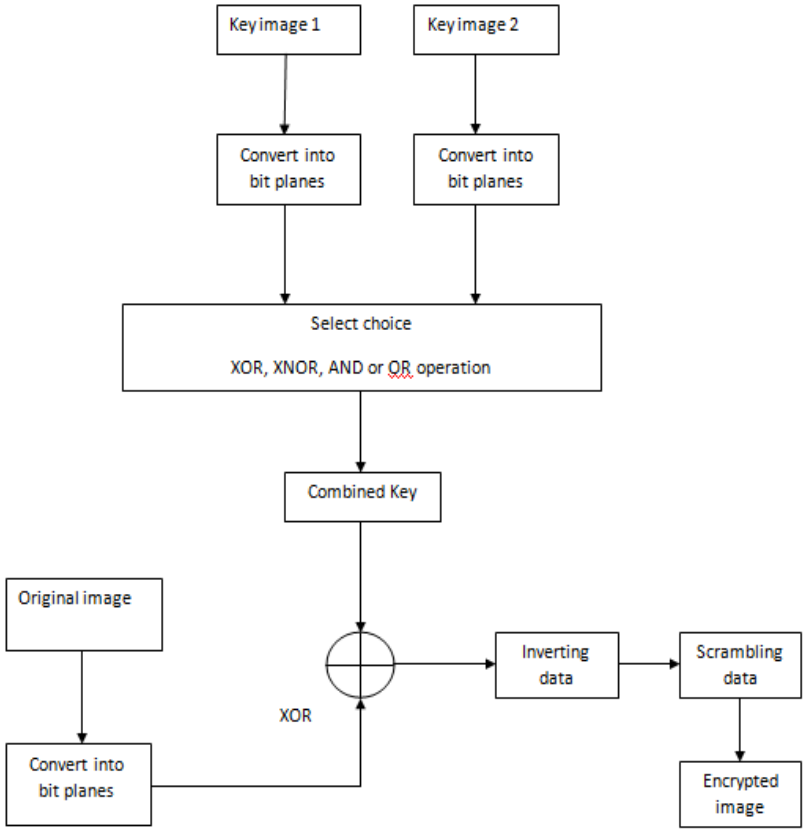


Fig. 3: Proposed CBP scheme with two key images

A. CBPScheme

Here are the steps involved in image encryption using BPC algorithm:

Step1: Select and read an input 2D or 3D image.

ISSN: 0975-3583,0976-2833 VOL12,ISSUE03,2021

Step2: Convert the input image into the number of bit planes. There are 8-bit planes for grayscale image and 24-bit planes for 3D or true color image.

Step3: Now, select and read the two key images with the same size of input imagei.e., both gray scale images, gray and color, color and gray or else both color images.

Step4: Convert both key matrices into number of bit planes and then do the logical XOR, OR, AND or XNOR operation to get the combined key from the two key matrices.

Step5: Do the XOR for the 8^{th} bit plane of input image with the combined key matrix bit planes.

Step6: Now, invert or shuffle the order of the bit planes to the output of step5.

Step7: Scramble the data obtained in step6 to get the encrypted grayscale or color image.

B. CBM Scheme

The following steps are used for the image crypto system which is based on BMC algorithm.

Step1: Select and read an input 2D or 3D image.

Step2: Convert the input image into the number of bit planes. There are 8-bit planes for grayscale image and 24-bit planes for 3D or true color image.

Step3: Now, select and read the two key images with the same size of input image i.e., both gray scale images, gray and color, color and gray or else both color images.

Step4: Convert the two key matrices into bound mapped matrices, then do the logical XOR, OR, AND or XNOR operation to get the combined key from the two key matrices.

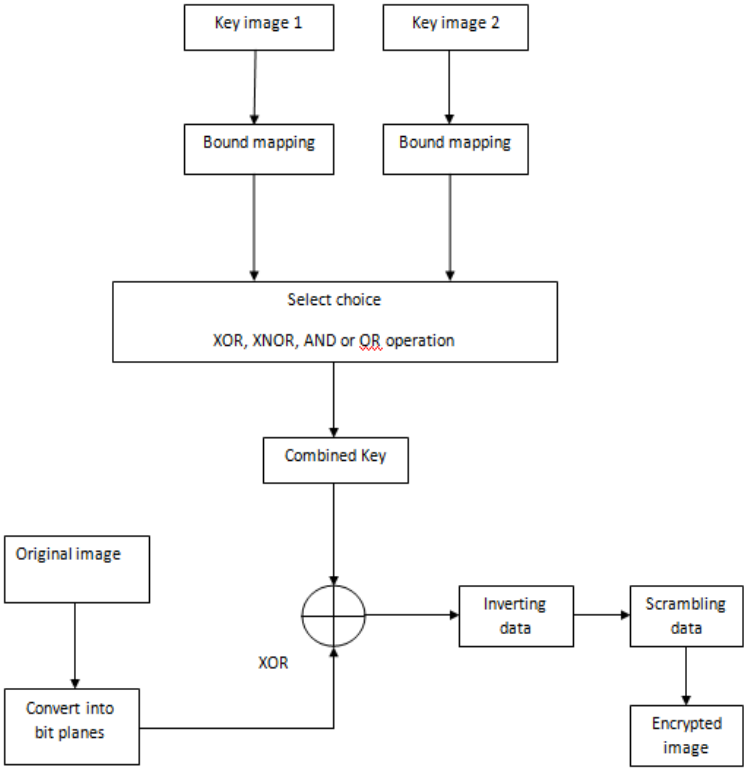


Fig. 4: Proposed CBM scheme with two key images

Step5: Do the XOR for eachbit plane of input image with the combined key matrix bit planes.

Step6: Now, invert or shuffle the order of the bit planes to the output of step5.

ISSN: 0975-3583,0976-2833 VOL12,ISSUE03,2021

Step7: Scramble the data obtained in step6 to get the encrypted grayscale or color image.

IV. EXPERIMENT RESULTS

In this section we are going to discuss the performance analysis of two proposed algorithms for both gray scale and true color images. Experiments have been done in MATLAB 2014a with 4.0 GB RAM and i3 processor, on multiple images taken from the web, various sitesand from textbooks. Fig.3 show that the original lena.jpg image has been encrypted with the two key matrices i.e., images baboon.jpg, which is a true color image and cameraman.jpg, which is a gray scale image, we can see that the encrypted image will not be decrypted if any one of the key matrices is not available. The decrypted image is almost equal to the original image which has been encrypted by using CBP algorithm.Histogram of the original and decrypted color images has been shown in fig.4, and the difference image showed in fig.5. By observing the fig.4 and 5, we can conclude that the proposed CBP algorithm is a lossless cryptography. In fig.6 we displayed the CBM results, which used bound mapping for the encrypting the key matrix with the original image. Here in CBM algorithm also we had shown the histograms and difference image in fig.7 and 8.

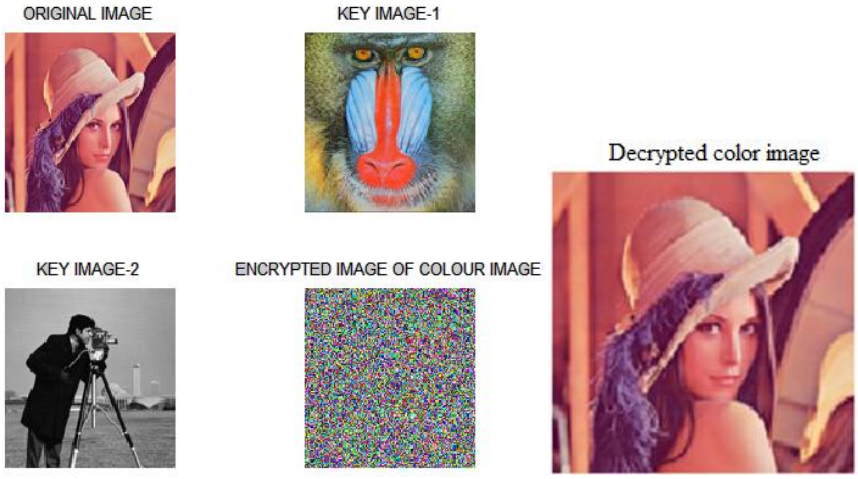
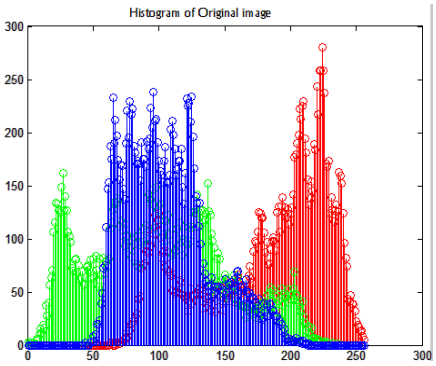
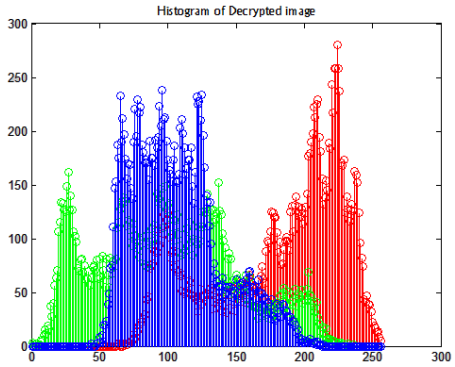


Fig.3: Proposed cryptanalysis for CBP algorithm.



(a)

ISSN: 0975-3583,0976-2833 VOL12,ISSUE03,2021



(b)

Fig. 4:(a) Original and (b) decrypted image histograms.

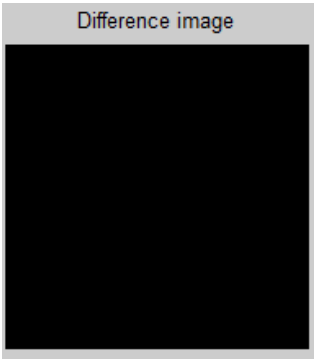
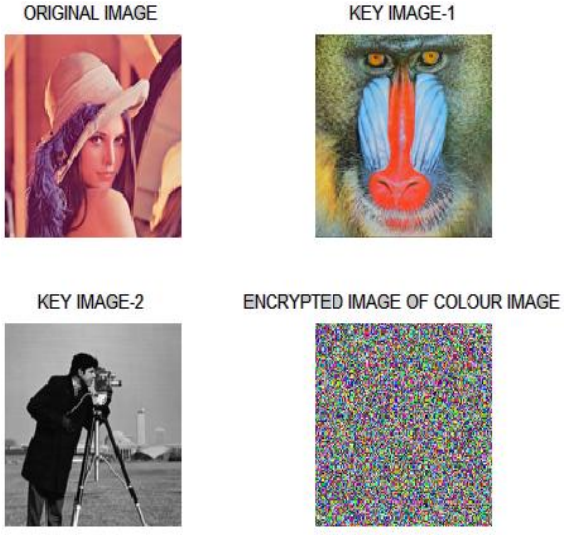


Fig. 5: Difference image of original and decrypted images.



ISSN: 0975-3583,0976-2833 VOL12,ISSUE03,2021

Fig.6: Proposed CBM algorithm.

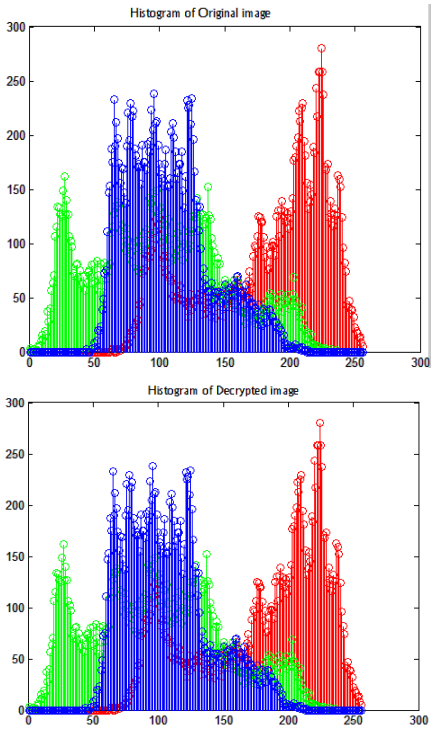


Fig. 7: Original and decrypted image histograms.

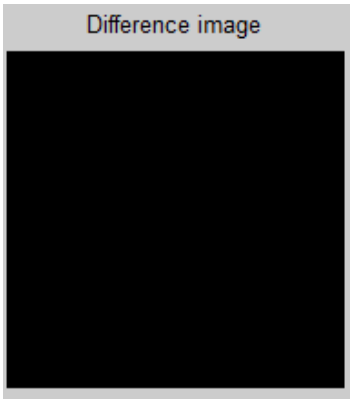


Fig. 8: Difference image of original and decrypted images.

V. CONCLUSION

ISSN: 0975-3583,0976-2833 VOL12,ISSUE03,2021

In this letter, we had implemented a new image cryptanalysis for improving the security to digital information based on the two powerful image encryption algorithms, which uses a binary key matrix for encrypting and decrypting the data. Here we had used two binary keys for improving the security and robustness. The proposed method has two methods CBP and CBM, which can be applied to any sort of image like real time, satellite, medical, bio-medical, remote sensing etc., Simulation results shows that both algorithms have shown the excellent performance.

REFERENCES

1. A. Pommer, A. Uhl, "Image and video encryption: from digital rights management to secured personal communication", Advances in Information Security, Vol. 15, 161p., 2005
2. B. Schneier.: Cryptography: Theory and Practice, CRC Press, Boca Raton, 1995.
3. Yong Feng, Xinghuo Yu, "A Novel symmetric image encryption approach based on an invertible two dimensional map".*35th Annual Conference on Industrial Electronics*,pp.1973-1978, 2009.
4. Kuang Tsan Lin, "*Hybrid encoding method by assembling the magic-matrix scrambling method and the binary encoding method in image hiding*", Optics Communications, Vol. 284, pp. 1778-1784, 2011.
5. Anil Kumar and M. K. Ghose, "*Extended substitution-diffusion based image cipher using chaotic standard map*", Communication in Nonlinear Science and Numerical Simulation, Vol.16, Issue 1, pp. 372-382, 2011.
6. Zhi-liang Zhu, Wei Zhang, Kwok-wo Wong and Hai Yu, "*A chaos-based symmetric image encryption scheme using a bit-level permutation*", Information Sciences, Vol. 181, pp. 1171-1186, 2011.
7. Kamlesh Gupta and Sanjay Silakari, "*Novel Approach for fast Compressed Hybrid color image Cryptosystem*", Advances in Engineering Software, Vol.49, pp. 29-42, 2012.
8. Qiudong Sun, Wenying Yan, Jiangwei Huang and Wenxin Ma, "Image encryption based on bit-plane decomposition and random scrambling".*2nd International Conference on Consumer Electronics, Communications and Network*, pp. 2630-2633, 2012.
9. Y. Zhou, K. Panetta, S. Agaian and C. L. Philip Chen, *"Image encryption using P-Fibonacci transform and decomposition"*, Optics Communications, Vol. 285, pp. 594-608, 2012.
10. A Linfei Chen, Daomu Zhao and Fan Ge, "*Image encryption based on singular value decomposition and Arnold transform in fractional domain*", Optics Communications, Vol.291, pp. 98-103, 2013.