ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

A Robust and Efficient Image Cryptography by Using Private Key Matrices and Logical Scrambling

Sai Mounika Bolla
M.Tech Student
RVR & JC College of Engineering, Guntur, Andhrapradesh, India

Ranga Babu Tummala
Guide
RVR & JC College of Engineering, Guntur, Andhrapradesh, India

ABSTRACT

Recent years there is a rapid growth in wireless technologies, every day G-bytes of information has been exchanging between the parties. Secure transmission of information is a highly challenging task for confidential applications such as military, civil, medical and web applications. Here in this thesis a new color image cryptanalysis scheme is proposed, which is based on the logical data scrambling and two binary key matrices. Two lossless color image cryptanalysis algorithms for secure transmission of a grayscale/color image by encrypting with the two binary key matrices are proposed. Simulation results show that the proposed schemes provide improved performance than the conventional techniques.

INTRODUCTION

Most of the media services and wireless network technologies were providing omnipresent conveniences for sharing, collecting or distributing images or videos over cellular mobile networks, social networks such as wechat, whatsapp, facebook etc., wireless public channels and multimedia networks for many organizations and individuals. Recent years there is a rapid growth in digital information sharing such as digital images or digital videos. Digital information sharing will be done in various applications, each of them need to transmit the information securely without knowing to the unauthorized person or party. For the applications like storage and transmission securing an image is a challenging task. For example, many strategic places like commercial centers, financial centers and public transportations will be monitored by digital video surveillance systems for the purpose of homeland security. Every day there is a large amount of images and videos with secure information, which does not known by unauthorized persons have been generated, transmitted or restored. In addition to this, patient's records in medical images such as Magnetic Resonance (MR) or Computed Tomography (CT) and medical signal reports such as electro cardiogram (ECG) or electro encephalogram (EEG) will be shared among the most of the doctors from different branches of health service organizations (HSO) over wireless networks for diagnosis purpose. All these medical images, signals and digital videos may contain some private information, which is more confidential. Hence, it is an important task to provide security for thissort of images and videos. Many applications such as medical, military, construction industries, fashion design industries and automobile industries require scanned information, blue prints and designs to be protected against espionage. Developing and employing schemes to enhance the lifetime of digital images or videos is an important, imperative and challenging task, which protects the content of original data for many years [1]. To protect an image or video encryption is an effective approach [1], which transforms the image or video into different format. In recent years 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 color images etc., To overcome all the drawbacks here in the proposed system we introduced a new technique called an improved color image cryptanalysis using two secret key image and logical operation, which will provide more security by generating two secret keys.

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 pommerandreas and uhlandreas. 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 (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 kuangtsanlin, 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.Zhiliangzhu*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. 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.

PROPOSED TECHNIQUE

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

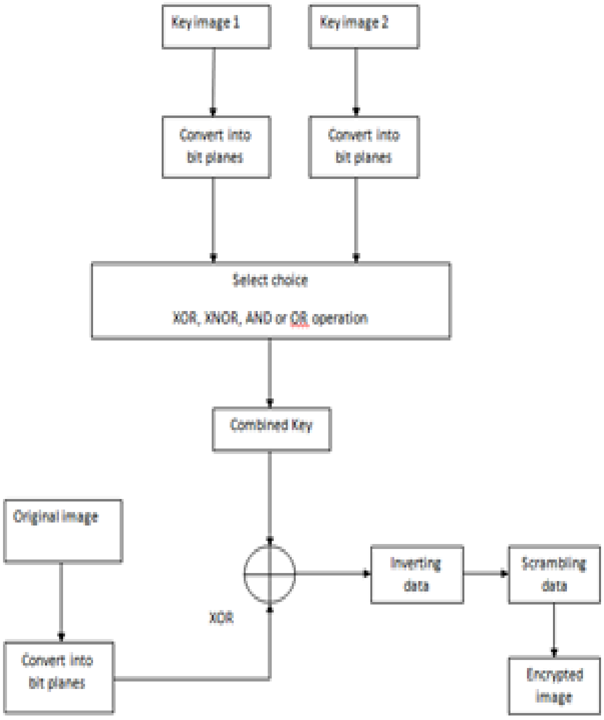

Fig.1 Proposed block diagram for Bitplane Crypt algorithm

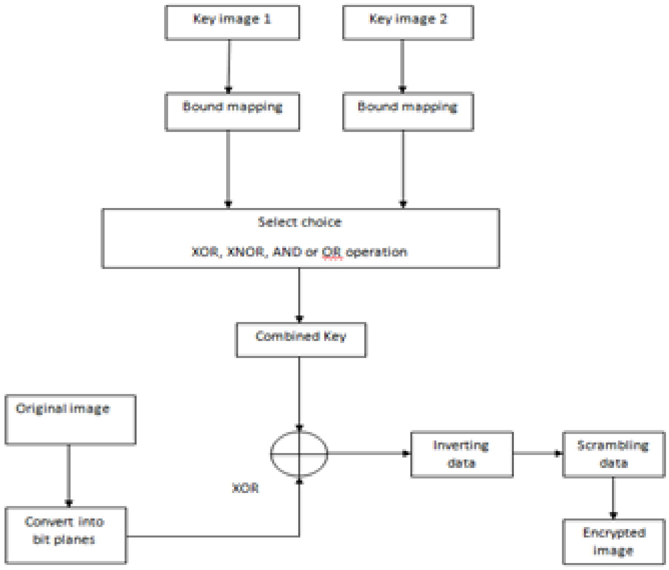

Fig.2 Proposed block diagram for Boundmap Crypt algorithm

1. Bitplane Crypt (BPC) algorithm
2. Boundmap Crypt (BMC) algorithm

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.

A. BPC Algorithm

Here are the steps involved in image encryption using BPC algorithm:
Step1: Select and read an input 2D 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 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 the 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 8th 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. BMC Algorithm

The following steps are used for the image crypto system which is based on BMC algorithm.
Step1: Select and read an input 2D 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 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
Step5: Do the XOR for the each 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

EXPERIMENTAL ANALYSIS

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 text books. 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 matrix is not available. The decrypted image is almost equal to the original image which has been encrypted by using BPC algorithm.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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 BPC algorithm is a lossless cryptography. In fig.6 we displayed the BMC results, which used bound mapping for the encrypting the key matrix with the original image. Here in BMC algorithm also we had shown the histograms and difference image in fig.7 and 8.

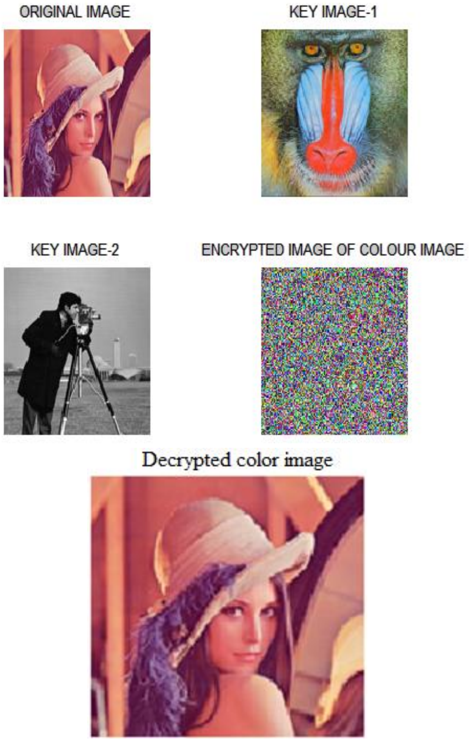

Fig.3. Proposed cryptanalysis for BPC algorithm

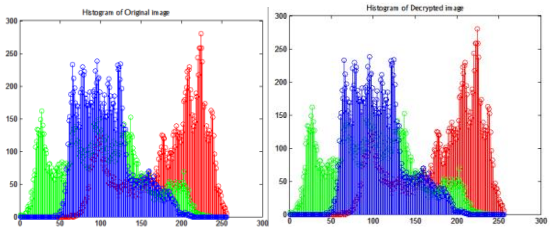

Fig4. Original and decrypted image histograms

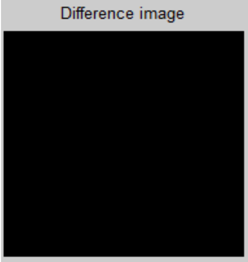

Fig5. Difference image of original and decrypted images

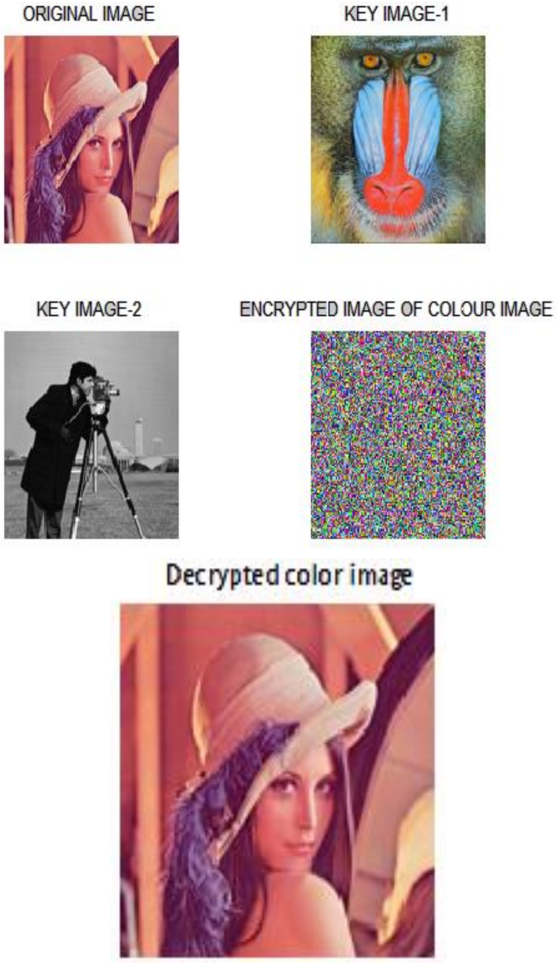

Fig.6. Proposed BMC algorithm

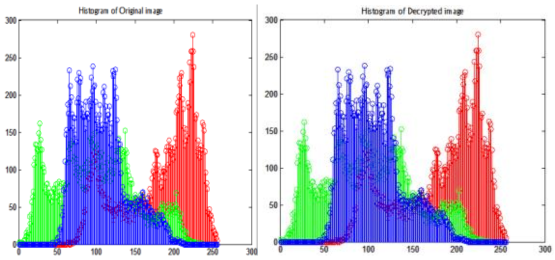

Fig7. Original and decrypted image histograms

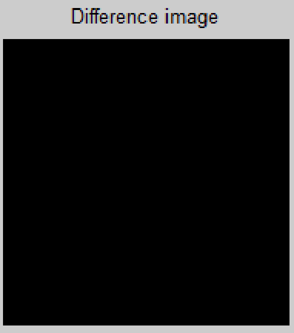

Fig8. Difference image of original and decrypted images

CONCLUSION

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 is implimented. Here we had used two binary keys for improving the security and robustness. The proposed method has two methods BPC and BMC, which can be applied to any sort of image like real time, satellite, medical, bio-medical, remote sensing etc., Simulation results shows that the 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. KuangTsan 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.