Asian Journal of Computer Science and Technology
ISSN: 2249-0701 (P) Vol.4 No.2, 2015, pp.13-17
© The Research Publication, www.trp.org.in
DOI: https://doi.org/10.51983/ajcst-2015.4.2.1750

A Novel Approach to Encrypt and Decrypt Color Images

V. S. Giridhar Akula
Professor and Principal
Methodist College of Engineering and Technology, Hyderabad, India
E-mail: akulagiri2002@yahoo.com

(Received 7 July 2015; Revised 22 July 2015; Accepted 18 August 2015; Available online 25 August 2015)

Abstract - **The proposed cryptosystem avoids all the crypto graphical weaknesses of earlier chaos-based encryption systems. Number of security analysis were carried out on the new algorithm and simulation results show that encryption and decryption are good and the proposed chaotic algorithm is proven to be the good procedure in terms of robustness.**

Keywords: **Image Encryption, Data Hiding, Chaotic Maps, Secret Image Holder, Pixel, Visual Cryptography, diffusion function.**

I.INTRODUCTION

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 are known 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 introduce two new lossless image encryption algorithms using a new concept “key-image” which is a binary image with the same size as the original image to be encrypted. One algorithm, called the Bitplane Crypt, generates the key-image by extracting a binary bit plane from another new or existing image. The key image of the other algorithm, called Edge map Crypt, is an edge map obtained from a new or existing image using a specific edge detector with a specified threshold. The algorithms decompose the original image into its binary bit planes. The bit planes are encrypted by performing an XOR operation with the key-image one by one. And then the order of all the bit planes is inverted. The resulting encrypted image can be obtained by applying a scrambling algorithm to the image from a combination of all bit planes.

Steganography is one of the data hiding technique in which Secret communications take place that conceal the very existence of the message. 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.

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).

Any loss of information during the reconstruction phase leads to reduction in the quality of the recovered image. On the other hand pixel expansion refers to the number of sub pixels in the generated shares that represents a pixel of the original input image. For bandwidth constrained communication channels it is desirable to keep m as small as possible. For color images, reducing pixel expansion is of paramount importance since they occupy more space and consume more bandwidth compared to grayscale and binary images. Most of the previous works in this area try to optimize pixel expansion or obtain perfect reconstruction.

II.METHODS AND MATERIALS

Cryptography is, the study of means of converting information from its normal, comprehensible form into an incomprehensible format, rendering it unreadable without secret knowledge the art of encryption. In the past, cryptography helped ensure secrecy in important communications, such as those of spies, military leaders, and diplomats. In recent decades, the field of cryptography has expanded its remit in two ways. Firstly, it provides mechanisms for more than just keeping secrets: schemes like digital signatures and digital cash, for example. Secondly, cryptography has come to be in widespread use by many civilians who do not have extraordinary needs for secrecy, although typically it is transparently built into the infrastructure for computing and telecommunications, and users are not aware of it.

Cryptography has had a long and colorful history. Generally speaking the earliest forms of secret writing required only pen and paper, and are now collectively termed classical cryptography. The two main categories are transposition ciphers, which rearrange the order of letters in a message, and substitution ciphers, which systematically replace groups of letters with others. Classical ciphers tend to leak varying amounts of information about the statistics of the plaintext, and because of this they are easily broken, for example by frequency analysis. Classical ciphers still enjoy popularity today, though mostly as puzzles .

Various devices and aids have been used for encryption. Early in the 20th century, several mechanical devices were invented for performing encryption, including rotor machines - most famously the Enigma cipher used in World War II. The ciphers implemented by these machines brought about a significant increase in the complexity of cryptanalysis. The various attacks on Enigma, for example, succeeded only after considerable effort. Occasionally, these devices have featured in films, such as in the James Bond adventure From Russia with Love.

With the advent of digital computers and electronics, very complex ciphers could be implemented. A characteristic of computer ciphers is that they operate on binary strings unlike classical and mechanical schemes, which use an alphabet of around 26 letters, depending on the language. Computer ciphers are also much more resistant to cryptanalysis; few are susceptible to a cipher text-only attack.

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that the decryption can be performed by humans (without computers).

The first visual cryptographic technique was pioneered by Moni Naor and Ad Shamir in1994. It involved breaking up the image into n shares so that only someone with all n shares could decrypt the image by overlaying each of the shares over each other. Practically this can be done by printing each share on a separate transparency and then placing all of the transparencies on top of each other. In their technique n-1 shares revealed no information about the original image.

Visual Cryptography is a graphical form of information concealing. It can be seen as a cryptographic primitive, since it offers methods and technologies for building more complex information security systems.

The techniques of visual cryptography are inspired from the general secret sharing schemes as presented by Adi Shamir and G.R. Blakley. The main difference between the visual and the general secret sharing schemes is that for the first ones the secret will be visually reconstructed in the decryption phase.

Novelty contributions are provided in implementing general k–out–of–n visual cryptography schemes. In such schemes the secret information can be reconstructed if and only if a minimum of k participants in a set of n participants will superimpose the shares they own. An adversary analyzing less then k shares can obtain no information (from the theory of information point of view) considering the secret message, no matter her computing power and analysis method used.

On special interest are the extended visual cryptography schemes for “natural images” – continuous tone gay images. In a two–out–of–two extended visual cryptography scheme, the two shares the secret image is split into are “innocent” images hiding the very intention of sending a secret message.

Further contributions are made considering the applications of visual cryptography in e-commerce, especially for scenarios that involve the presence of a corrupt Post of Sale (POS)[7].

Steganography is the art and science of hiding the fact that communication is taking place. Using steganography, you can embed a secret message inside a piece of unsuspicious information and send it without anyone knowing of the existence of the secret message. Steganography and cryptography are closely related. Cryptography scrambles messages so they cannot be understood. Steganography on the other hand, will hide the message so there is no knowledge of the existence of the message in the first place. In some situations, sending an encrypted message will arouse suspicion while an “invisible” message will not do so. Both sciences can be combined to produce better protection of the message. In this case, when the steganography fails and the message can be detected, it is still of no use as it is encrypted using cryptography techniques.

The chaos-based image cryptosystem[3] mainly consists of two stages [2]. The plain image is given at its input. There are two stages in the chaos- based image cryptosystem. The confusion stage is the pixel permutation where the position of the pixels is scrambled over the entire image without disturbing the value of the pixels and the image becomes unrecognizable. The pixel permutation is carried out by a chaotic system [1,2]. The chaotic behavior is controlled by the initial conditions and control parameters which are derived from the 16-character key. To improve the security, the second stage of the encryption process aims at changing the value of each pixel in the whole image an important tool to protect image from attackers. The basic idea of encryption[5,6] is to modify the message in the diffusion stage, the pixel values are modified sequentially by the sequence generated from one of the three chaotic systems selected by external key. The whole confusion-diffusion round repeats for a number of times to achieve a satisfactory level of security. The randomness property inherent in chaotic maps makes it more suitable for image encryption.

III.PROPOSED METHOD

1. First input original image s taken and then to get the cipher image we used chaotic algorithm in which should pixels positions are change for high security
2. In the decryption we use reverse process of the encryption means input is cipher image and result image is plain image

A.The Edge Map Crypt Algorithm

The edge map is frequently used in image enhancement, compression, segmentation and recognition. The application of edge maps can also be extended to image encryption. In this section, we introduce a new image encryption algorithm using an edge map which is called the Edge map Crypt algorithm. An edge map is considered as the key-image in this algorithm. Such edge map is generated from another different image with the same size as the original image using a specific edge detector with a selected threshold value.

The Edge map Crypt algorithm first decomposes the original image into its binary bit planes. Each of them is encrypted by performing an XOR operation with the key-image, which is an edge map created from another image. Next, the algorithm inverts the order of all XORed bit planes and combines them together. The resulting image is scrambled by using a selected scrambling algorithm to generate the final resulting encrypted image. The Edge map [4] Crypt algorithm is illustrated in Fig. 1. Similar to the Bitplane Crypt algorithm, a 3D image can be encrypted by applying the Edge map Crypt algorithm to all its 2D components individually. Any new or existing image with the same size of the original image can be used to generate the edge map, the key image.

It could be an image in the public online database or a new image generate by the users. The edge map can be obtained by using any existing edge detector such as Canny, Sobel, Prewitt, or any other edge detector. The users have flexibility to choose any existing image or any existing edge detector or any threshold value to generate the edge map used as a key-image. They also have flexibility to use any existing image scrambling method for the Edge map Crypt algorithm. Therefore, the security keys for this algorithm consist of the image or its location which is used to generate the edge map, the type of the edge detector, the edge detector’s threshold, and the security keys of the scrambling algorithm. To reconstruct the original image, the users should be provided the security keys which help them to obtain the correct edge map. The decryption process first generates the edge map from the selected image using the security keys. It then unscrambles the encrypted image using the selected scrambling algorithm. Next, it decomposes the unscrambled image into its binary bit planes and performs XOR operation between the edge map and each bit plane. The order of all bit planes is restored to the original order. The reconstructed 2D image/component can be obtained by combining all bit planes.

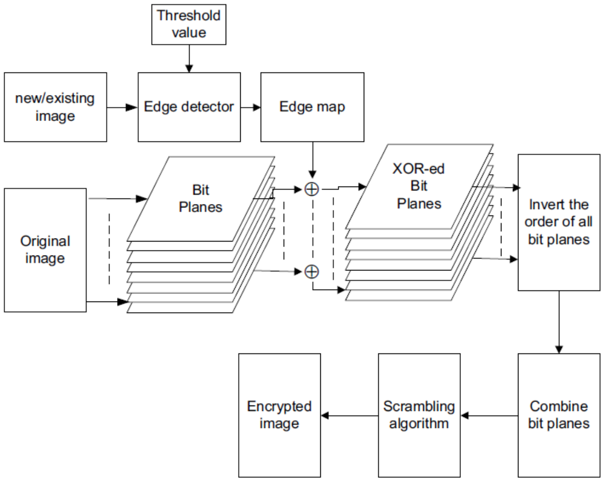

Fig.1 The Edge map Crypt algorithm

IV. RESULTS AND DISCUSSION

The proposed image encryption system uses any one of the chaotic system for pixel position permutation and one of the same chaotic system for pixel value modification. Several simulation results are provided to show the performance of the algorithms for 2D and 3D image encryption. In all experimental results of this paper, both algorithms utilize the image scrambling algorithm based on the Generalized P-Gray Code in with the security keys: *n*=*2*=2, *p* = 0 .

Fig. 2 shows several 2D images to be used as test images or images to generate the key-image.

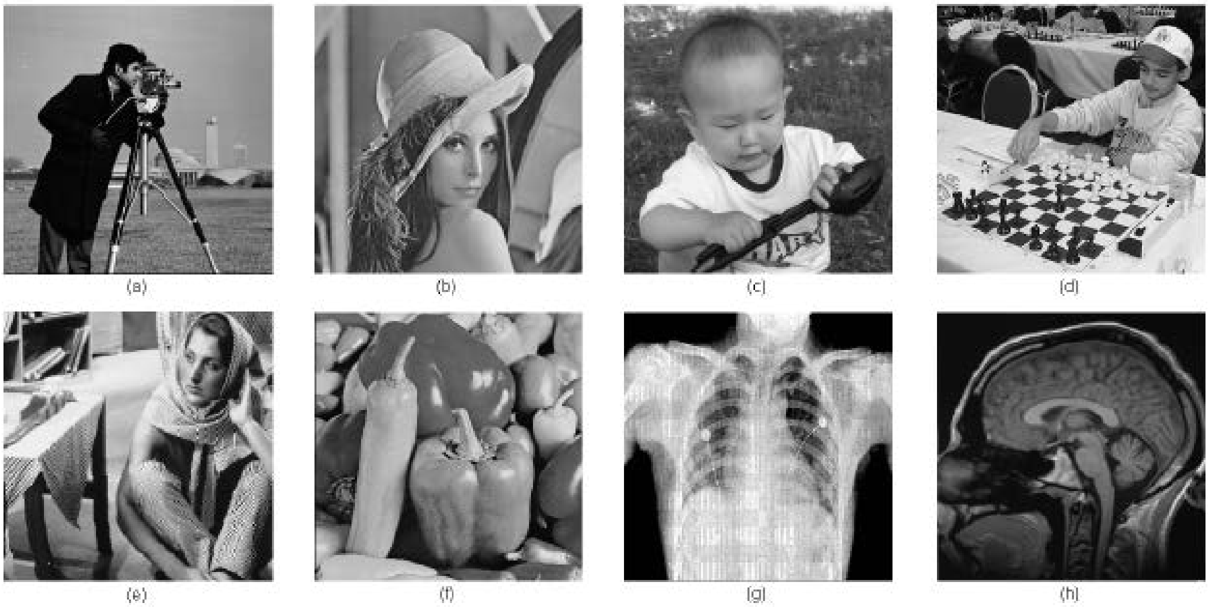

Fig. 2 Test images. (a) 256×256 Cameraman; (b) 256×256 Lena; (c) 256×256 Baby; (d) 256×256 Chessplayer; (e) 512×512 Barbara; (f) 512×512 Peppers; (g) 512×512 CT ribs image; (h) 512×512 MRI brain image

A. 2D IMAGE ENCRYPTION

There are several types of 2D images such as grayscale images, medical images and biometrics. The 2D image can be decomposed into several binary bit planes and encrypted one by one. Figure 3 shows the Grayscale image encryption using the Edge map Crypt algorithm, Color image encryption using the Edge map Crypt algorithm.

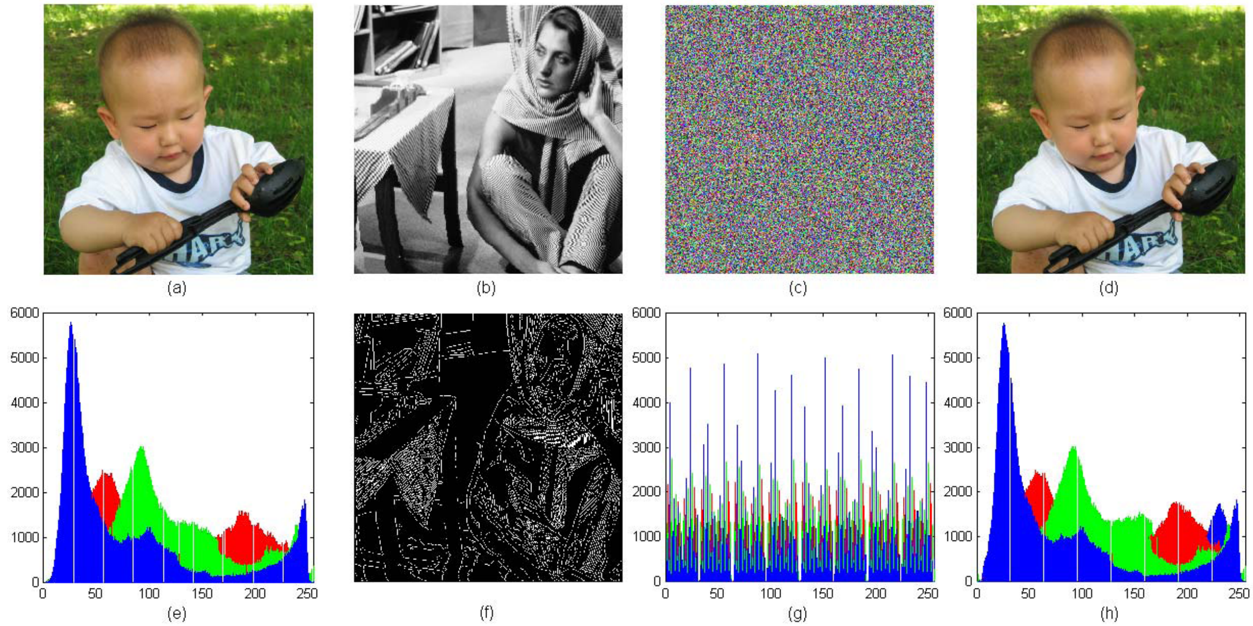

Fig.3 Color image encryption using the EdgemapCrypt algorithm.
(a) The original 512×512 color image; (b) A 512×512 grayscale Barbara image; (c) The encrypted color image; (d) The reconstructed color image;(e) Histogram of the original image in (a); (f) The edge map of the Barbara image in (b), Canny, 0.1; (g) Histogram of the encrypted image in (c); (h) Histogram of the recontructed image in (d).

V. CONCLUSION

Based on the design rules discussed earlier, the new image encryption scheme was designed. A suitable chaotic map preserving the properties of chaos after discretization was chosen. By choosing a high dimensional chaotic system, the key space is increased. Complex non-linearity was preserved by choosing suitable chaotic maps. Repeated permutations are avoided but pixel values are changed by the diffusion function. By incorporating all these features, the proposed cryptosystem avoids all the crypto graphical weaknesses of earlier chaos-based encryption systems. Number of security analysis were carried out on the new algorithm and simulation results show that encryption and decryption are good and the algorithm has good security and robustness.

REFERENCES

[1] Xiping He Qionghua Zhang , “Image Encryption Based on Chaotic Modulation of Wavelet Coefficients”, Congress on IEEE Image and Signal Processing (CISP'08), Sanya, Hainan, Vol.1, pp.622-626, 27- 30 May 2008.

[2] Xin Zhang, Weibin Chen, “A New Chaotic Algorithm For Image Encryption”, pp 889-892 IEEE ICALIP2008

[3] Dong enxeng, Chen Zengqiang, Yuan zhuzhi, Chen zaiping, “A Chaotic Images Encryption Algorithm with The Key Mixing Proportion Factor”,pp 169-174 Computer Society IEEE 2008.

[4] Chong Fu, Zhen-chuan Zhang, Ying-yu Cao, “An Improved Image Encryption Algorithm Based on Chaotic Maps”, Computer Society, IEEE 2007

[5] Huang Yuanshi, Xu Rongcong, Lin Weiqiang, “An Algorithm for JPEG Compressing with Chaotic Encrypting”, Proceedings of the International Conference on Computer Graphics, Imaging and Visualisation (CGIV’06), 2006

[6] Peng Fei, Shui-Sheng Qui, Long Min, “An Image Encryption Algorithm based on Mixed Chaotic Dynamic Systems and External Keys”, Proceedings of 2005 International Conference on Communications, Circuits and Systems,,Vol. 2, pp.1139, 27-30 May 2005.

[7] Guang ZH, Huang FJ, Guan WJ, “Chaos-based Image Encryption Algorithm”, Physics Letters A, Vol.346, pp.153 – 157, 2005.