International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 06 | June -2017 www.irjet.net p-ISSN: 2395-0072

LOSSLESS ENCRYPTION USING BITPLANE AND EDGEMAP CRYPT ALGORITHMS

R.Pravallika[1]

[1]*Assistant Professor & ECE Dept. Of Lingaya's Institute of Management And Technology*

Abstract - *Cryptography places the major role in information security. It is used in several cases mainly exploded with the arrival and rise of internet. Cryptography has become essential part of today's information system, and it is being exploited in many areas like remote access, online orders and payments, email and messaging security etc. Cryptography is nothing but the encrypt or decrypt the data/image. Its dependent upon the key image technique. The key image size is either same or less than the original image. Using key image of bit plane or edge map generated from another image (hiding image). The key image is selected from the grayscale image or color image for new/existing grayscale image. In this paper I'm considering the color images using lossless encryption. Lossless means without lost any information of image.*

Two types of lossless image encryption algorithms are there

1. Bit plane Crypt algorithm.

2. Edge map Crypt algorithm.

In this process we are sent the images or videos one person/path to another person/path. Those images or videos may contain secured information. For providing high security for these images or videos becomes an important issue for individuals, business, governments as well, automobile, medical, Construction and the Fashion industry require designs, scanned data, building plans and blue-prints to be safe guarded against espionage etc.

***Key Words*: Cryptography, key image, Bit plane slicing.**

1. INTRODUCTION

Visual surveillance systems and networks make remote video monitoring available for homeland security purpose and also easy to transmit and share videos and image data. With the ubiquitous deployment of visual surveillance systems in many important areas such as airports, commercial centres and also military strategic places, large amounts of videos and images with security information are generated, transmitted and stored[3]. Image encryption is an effective approach to protect images or videos by transforming them into completely different formats. Several data encryption algorithms like Data Encryption Standard (DES) and Advanced Encryption standard (AES) are proposed for encrypting images [14]. Image encryption can be accomplished by block-based transformation algorithm which is based on the pixel value rotation of image [6]. A few approaches to exploit the spatial and cross-plane correlation among pixels are discussed, as well as the possibility of exploiting the correlation between colour bands.

Using a concept of a binary "key-image", with the same size of the original image to be encrypted. The bit plane crypt algorithm generates the key-image by extracting a binary bit plane from another new or existing image. The other algorithm is an edge map obtained from a new or existing image using a specific edge detector with a specified threshold [8]. The algorithms decompose the original image into its binary 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 bit planes is inverted. And combine all bit planes. The resulting encrypted image can be obtained by applying a scrambling algorithm to the image/Video. Image security is a major challenge in storage and transmission applications [10]. For example, 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 high security for these images and videos becomes an important issue for individuals, business and governments as well.

2. METHODOLOGY:

In cryptography procedure first of all considers the original image using that generates the key image it's given to encrypt algorithm and its produce the output. Output of encrypt algorithm is considered as a input for decryption technique given to corresponding decryption algorithm and generates the original image.

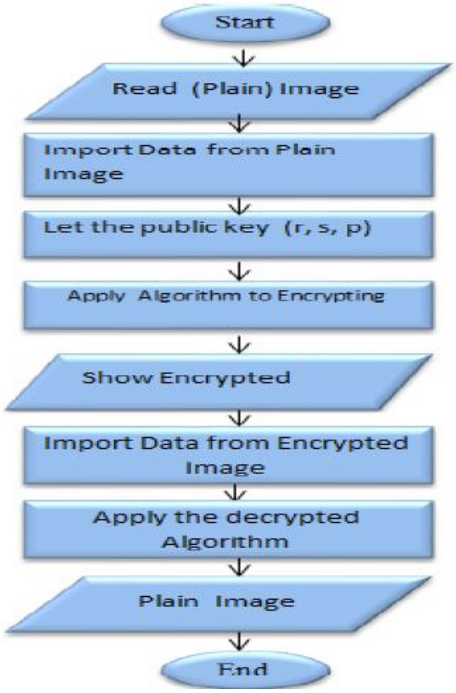

Fig: Flowchart of cryptography

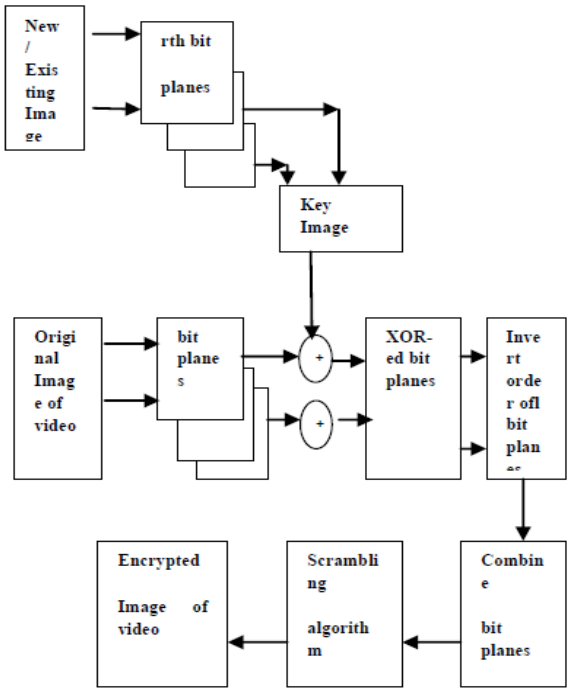

Fig: Bit plane Crypt Encryption algorithm

Input: The original image is to be encrypted.
Step 1: Consider the new image or existing image with the same size of the original image. That new image is converted into bit plane images.
Step 2: Obtain the key image by extract r^{TH} bit plane of the image in Step 1.
Step 3: Consider *i= {1 (R), 2 (G), 3 (B)}.*
Step 4: Decompose the original image i into binary Bit planes.
Step 5: Perform the XOR operation between the key- Image and each bit plane in S
Step 6: Invert the order of all bit planes.
Step 7: Combine all bit planes together to obtain the image.
Step 8: Scramble the resulting image using a selected Scrambling method to generate the resulting Encrypted image.
Output: The encrypted image.
The 8 bit-planes of a gray-scale image (the one on left). There are eight because the original image uses eight bits per pixel. 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. 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 aspect of 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.

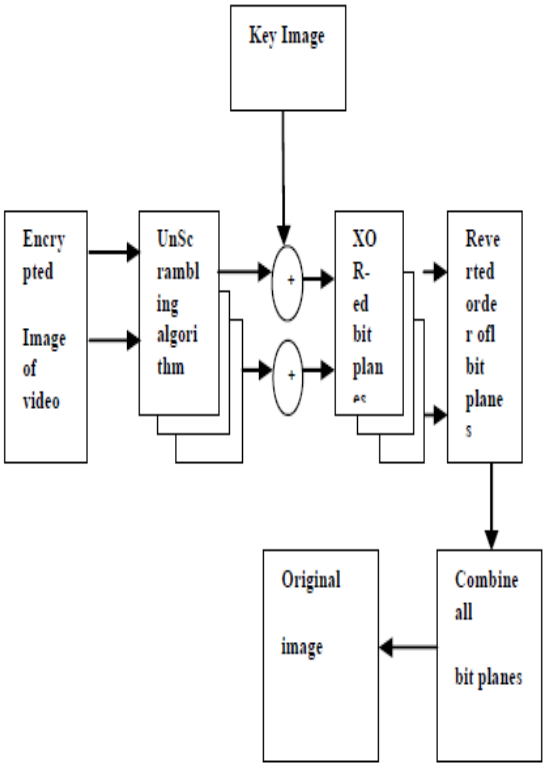

Fig: Bit plane Decrypt Decryption algorithm

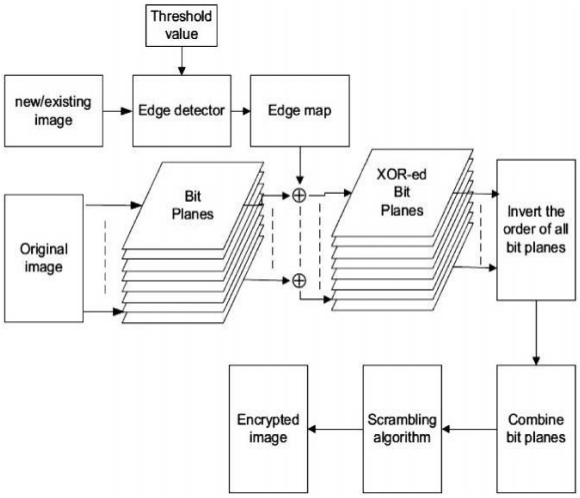

Fig: Edge map Crypt Encryption algorithm

First generate the key-image from another new/ existing image with the same size as the original image using specific edge detector with a selected threshold value. The key image is considered as the edge map. The edge map is frequently used in image enhancement, compression, segmentation and recognition.
Input : The original 2D or 3D image to be encrypted.

Step 1: Choose any or existing image with the same size of the original image.
Step 2 : Obtain the key-image by extract the rth bit plane of the image in Step 1.
Step 3 : Calculate the edge map from the existing image with the same size of the original image.
Step 4 : Decompose the original image or each component of the 3D image into its binary bit planes.
Step 5 : Perform the XOR operation between the edge map of the key-image and each bit plane in Step 4.
Step 6 : Invert the order of all bit planes.
Step 7 : Combine all bit planes together to obtain the image.
Step 8 : Scramble the resulting image or components in Step 7 using a selected scrambling method to generate the resulting encrypted image.
Output : The encrypted edge map image.

ENTROPY:

Entropy is a quantity which is used to describe the `business' of an image, i.e. the amount of information which must be coded for by a compression algorithm. Low entropy images, such as those containing a lot of black sky, have very little contrast and large runs of pixels with the same or similar DN values. An image that is perfectly flat will have an entropy of zero. Consequently, they can be compressed to a relatively small size. On the other hand, high entropy images such as an image of heavily cratered areas on the moon have a great deal of contrast from one pixel to the next and consequently cannot be compressed as much as low entropy images.

$$entropy = -\sum_i p_i \log_2 p_i$$

SIMULATION RESULTS

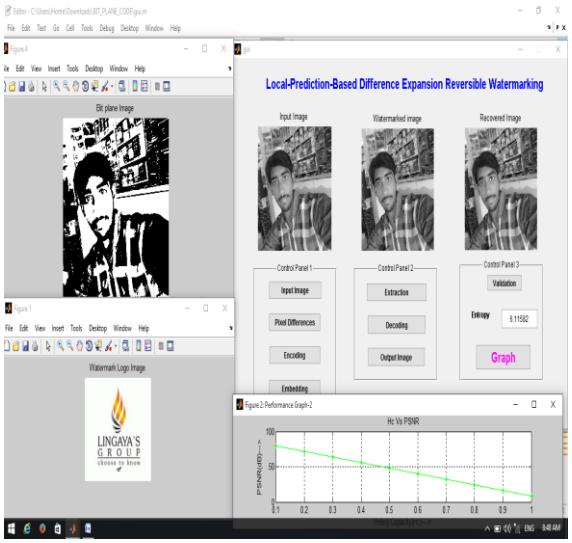

Fig: Result of Bit plane Encryption, Decryption And Entropy Value.

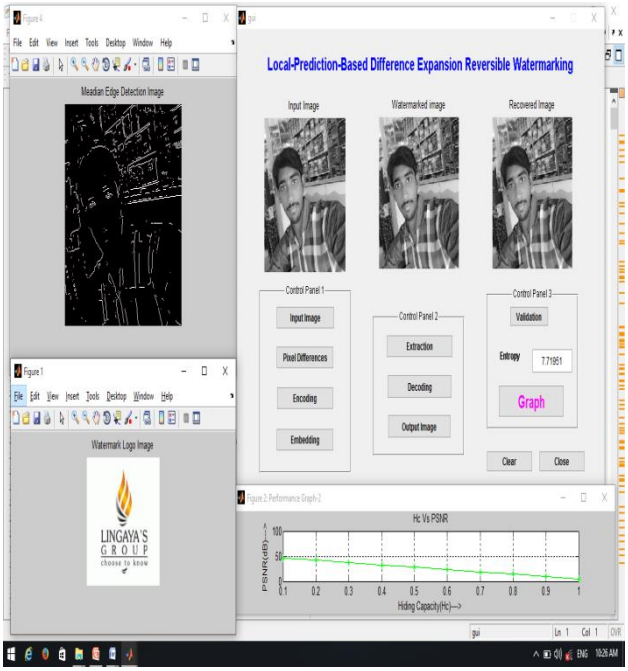

Fig: Result of Edge map encryption, Decryption And Entropy Value

3. CONCLUSION:

In this paper, two algorithms are implemented for lossless encryption. To generate key image an either a Biplane Crypt or an Edge map Crypt algorithm. Both algorithms are easy to implement in software as well as hardware because they operate at the binary levels. In these algorithms we are used

Watermarking and scrambling techniques. Here watermarking technique reduces the noise levels in the original images and simultaneously reconstructs the original image. Finally entropy is calculated to obtain the efficiency.

These two algorithms produced lossless encryption for all type of formats like jpeg, bmp and so on. They are also suitable for multimedia applications and real time application such as mobile phone services and wireless networks etc.

REFERENCES

[1].N. Madhumidha and Dr.S. Chandramathi Bonfring International Journal of Advances in Image Processing, Vol. 2, Special Issue 1, Part 2, February 2012 63 ISSN.
[2]. Abdul Razzaque and Narendra Thakur International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 5, July - 2012 ISSN: 2278-0181
[3]. Koo Kang in IEEE transactions on image processing, vol. 20, no. 1, January 2011 .
[4]. Jayanta Kumar Pal1, J. K. Mandal2 and Kousik Dasgupta3 in (IJNSA), Vol.2, No.4, October 2010.
[5]. Debasish Jena1, Sanjay Kumar Jena2 in 978-0-7695-3516-6/08 $25.00 © 2008 IEEE DOI 10.1109/ICACC.2009.109
[6]. Gonzalez R. C. , Woods R. E. and Eddins S. L. , 2009 . Digital Image processing Using MATLAB. Gatesmark PublishingA Division of Gatesmark, LLC..
[7]. M.J. Wainwright. "Sparse Graph Codes for Side Information and Binning", *IEEE Signal Processing Magazine*, vol. 24 no.5, pp. 47-57, 2007.
[8]. D. Schonberg, S. Draper and K. Ramchandran, "On Compression of Encrypted Images" *Image Processing, 2006 IEEE International Conference on* pp. 269¡272, October 2006.
[9]. Pei, S.C. and Ding, J.J. "Reversible Integer Color Transform with Bit-Constraint" *Image Processing, 2005. ICIP 2005. IEEE Int. Conf. on*, vol. 3, 2005.
[10]. M. Johnson, P. Ishwar, V. Prabhakaran, D. Schonberg and K. Ramchandran, "On Compressing Encrypted Data" *IEEE Tranaction on Signal Processing* vol.52 no.10 pp. 2992¡3006, October 2004.
[11]. John Blesswin, Rema, Jenifer Josel 978-1-4244-9799-71111$26.00 ©20 11 IEEE , in Proc. Eurographics, Saarbrucken, Germany, Sep. 2002, pp. 341-348.
[12]. F.R. Kschischang, B.J. Frey, and H.-A. Loeliger, "Factor graphs and the sum-product algorithm," *IEEE Trans. Inform. Theory*, vol. 47, no. 2, pp. 498-519, Feb. 2001.
[13]. Schnorr, C. P. and Jakobsson, M., 2000. Security of signed ElGamal encryption. Springer Berlin Heidelberg.
[14]. National Institute of Standards and Technology, "Data Encryption Standard (DES),"http://csrc.nist.gov/publications/fips/fips46-3/fips46- 3.pdf, 1999.

Author Details

R.PRAVALLIKA, LIMT-B.Tech, LBRC-M.Tech, working as Assistant Professor in ECE from Lingaya's Institute Of Management And Technology, Via Nunna, Vijayawada, Krishna- District , Andhra Pradesh.