Advances in Engineering Software 49 (2012) 29–42

Contents lists available at SciVerse ScienceDirect

Advances in Engineering Software

journal homepage: www.elsevier.com/locate/advengsoft

# Novel Approach for fast Compressed Hybrid color image Cryptosystem

Kamlesh Gupta [a,*], Sanjay Silakari [b]

[a] Dept. of Computer Science & Eng., Jaypee University of Engineering and Technology, A.B. Road, Guna, MP, India
[b] Dept. of Computer Science & Eng., University Institute of Technology, RGPV, Bhopal, MP, India

ARTICLE INFO

*Article history:*
Received 25 January 2012
Received in revised form 29 February 2012
Accepted 4 March 2012
Available online 25 April 2012

*Keywords:*
Chaotic map
Cat map
Standard map
Elliptic Curve Cryptography
Curvelet transform
ECDLP

ABSTRACT

In this Paper, the issues pertaining with efficient, fast, cost effective and secured image transmission are addressed in totality. The proposed model employs Compressed Hybrid Cryptosystem constitutes compression, encryption and secured session key exchange along with the transmission of image. In the proposed work, an algorithm has been designed to generate diffusion template using 3D Standard map. The image is rotated vertically and horizontally followed by a shuffle using 3D Cat map and Standard map. The image is then encrypted by performing XOR operation on the shuffled image and diffusion template. Proposed method takes lesser time and is found to be safe from any of the existing cryptanalytic attack. Further Elliptic Curve Cryptography is used for secure transfer of private key, which has resulted in significant reduction in the key size without compromising its security strength. To reduce bandwidth requirement and power consumption, a compression technique is proposed based on curvelet transform before image encryption, with special technique of coefficient elimination by which a higher compression ratio can be obtained without much loss in image information. Even though the coefficients neglected are large, the higher PSNR values show that curvelet has better reconstruction performance.

The model has been rigorously examined over the prevalent standard test and has encouragingly succeeded to pass most of them like key sensitivity analysis, key space analysis, statistical analysis, differential analysis, entropy analysis, randomness analysis, PSNR analysis, MSE analysis, for fast, cost effective and secured image transmission. Which was the key problem statement for this research work.

## 1. Introduction

With the advent of Internet and World Wide Web, the amount of digital information to be stored and communicated has grown exponentially beyond imagination. This digital information not only comprises text, but also has large volume of image, audio/video and multimedia data, which comparatively is very bulky than the textual information.

The images as on date have become an integral and vital component of any useful data and are widely used in several important applications. Few of these crucial applications include Military Image Database & Message Communication, Confidential Video Conferencing, Medical Imaging System & Telemedicine, Online Personal Photograph Albums, Natural Disaster or Catastrophe Alarming Systems, Online Image Identification and Authentication, Reflection Seismology, Electronic Surveillance Systems, Document Imaging, Image 'CAPTCHA', Image Registration, Geographic Information System, etc.

The use of images in most these applications has given rise to several problems as follows:

1. Traffic on the internet has increased tremendously resulting in longer delays and higher communication cost.
2. An image being bulky amount of data requires larger bandwidth for the transmission.
3. High space requirements for intermediate and final storage.
4. Security and integrity of the transmitted images.

All these applications not only require faster communication but also require that image transmission must be cost effective and secured.

Encryption of images is different from that of textual data, as images are intrinsically bulky and have high correlation among pixels and higher redundancy which is difficult to be handled by the traditional encryption schemes. Hence the DES, AES, IDEA, Blowfish, RC6 and RSA, etc., do not suite for modern image transmission requirements. Many researchers have tried to innovate better solutions for secured image transmission. In particular, application of chaos theory in multimedia encryption is one of the important research directions.

* Corresponding author. Tel.: +91 94257 57684.
*E-mail addresses:* Kamlesh_rjitbsf@yahoo.co.in (K. Gupta), ssilakari@yahoo.com (S. Silakari).

0965-9978/$ - see front matter © 2012 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.advengsoft.2012.03.001

The aim of this research is to fix the following problems for efficient, fast, cost effective and secured image transmission.

- Asymmetric cryptography doesn't suite for secured transmission of images because of the bulk data, strong pixel correlation and high redundancy. Moreover encryption at the source and decryption at the destination lowers the encryption performance.
- Symmetric encryption is fit for image encryption, but the security of symmetric encryption depends on the private key so it is needed to transmit this key by asymmetric method but the key used in that is itself bulky, hence, it is needed to transfer the key by secured channel with a significant reduction in key size.
- An image is the bulky amount of data and requires larger bandwidth for the transmission, hence efficient compression is required.

To view the basic ingredients, speed, cost effectiveness and security of image transmission in totality.

In this paper, we propose the following solutions to the above mentioned problems by proposed Compressed Hybrid Cryptosystem, which are described below:

The algorithm has been designed to generate diffusion template using 3D standard map. The image is rotated vertically and horizontally followed by a shuffle using 3D cat map and standard map. The image is then encrypted by performing XOR operation on the shuffled image and diffusion template. Proposed method takes lesser time and is found to be safe from any of the existing cryptanalytic attack. Further Elliptic Curve Cryptography is used for secure transfer of private key, which has resulted in significant reduction in the key size without compromising its security strength.

To reduce bandwidth requirement and power consumption, a compression technique is proposed based on curvelet transform, with special technique of coefficient elimination by which a higher compression ratio can be obtained without much loss in image information. Even though the coefficients neglected are large, the higher PSNR values show that curvelet has better reconstruction performance.

## 2. Performance evaluation metrics

The basic objective of image compression is the reduction of size for transmission or storage while maintaining suitable quality of reconstructed images. Good compression schemes having a lower MSE and high PSNR.

With the application of an encryption algorithm to an image, its pixels values change when compared with the original image. A good encryption algorithm must make these changes in an irregular manner and also maximize the difference in pixels values between the original and the encrypted images. Also, to get a good encrypted image, it must be composed of totally random patterns that do not reveal any of the features of the original image. The encrypted image has to be independent of the original image. It should have a low correlation with the original image [21,2,10,16].

### 2.1. The image compression evaluation metrics

The reconstruction quality of the compressed image can be measured in PSNR and MSE in dB.

$$\mathrm{PSNR} = 10\log_{10}\frac{255^2}{MSE} \tag{1}$$

where

$$\mathrm{MSE} = \frac{\sum_{i-1}^{W}\sum_{j-i}^{H}(x_{ij} - \widetilde{x_{ij}})}{W \times H} \tag{2}$$

where $x_{ij}$ and $\widetilde{x_{ij}}$ denotes the original and reconstructed pixel, respectively, and the images are of size $W \times H$. A lower value for MSE means lesser error, and as seen from the inverse relation between the MSE and PSNR, this translates to a high value of PSNR. Logically, a higher value of PSNR is good because it means that the ratio of Signal to Noise is higher. Here, the 'signal' is the original image, and the 'noise' is the error in reconstruction. So, a compression scheme having a lower MSE and higher PSNR can be recognized as a better one.

### 2.2. The image encryption evaluation metrics

In this section, we evaluate the ability of the encryption algorithm to substitute the original image with uncorrelated encrypted image. Theoretical analyses for the secured image encryption on the basis of key space analysis, statistical analysis, histogram analysis, information entropy analysis, correlation analysis and differential analysis confirm that to minimize the possibility of brute force attack for decryption.

#### 2.2.1. Key space analysis

The key space should also be suitably large to make brute-force attack not feasible.

#### 2.2.2. Statistical analysis

An ideal cipher should be strong against any statistical attack, so statistical analysis on cipher-text is of crucial importance for a cryptosystem. In order to prove the security of the proposed image encryption scheme, the following statistical tests are performed.

*2.2.2.1. Histogram analysis.* To prevent the access of information to attackers, it is important to ensure that encrypted and original images do not have any statistical similarities. The histogram analysis clarifies that pixel values of image [4] are distributed.

The histogram of original image contains great sharp rises followed by sharp declines and the histograms of the encrypted images for different round have uniform distribution which is significantly different from original image and has no statistical similarity in appearance. Therefore, it does not provide any clue for statistical attack.

*2.2.2.2. Correlation analysis.* The correlation between two vertically adjacent pixels, two horizontally adjacent pixels and two diagonally adjacent pixels in plain-image and cipher image respectively [4]. Then, calculate their correlation coefficient using the following two formulas:

$$co\,v(x,y) = E(x - E(x))(y - E(y)) \tag{3}$$

$$r_{xy} = \frac{co\,v(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{4}$$

where $x$ and $y$ are the values of two adjacent pixels in the image. In numerical computations, the following discrete formulas were used:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N}x_i \tag{5}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y - E(y)) \tag{6}$$

$$co\,v(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - (E(y)) \tag{7}$$