International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
ISSN: 2457-0362
www.ijarst.in

Colour image High Level encryption and decryption using chaotic maps

R Premananda, Shridhar H, Kabballi Prashanth

[1,2] Assistant Professor, Dept. of E&CE, Government Engineering College, Haveri, Karnataka, India

[3]Assistant Professor ,Government Engineering College Huvinahadagali

rpremananda@gmail.com, shridhar47@gmail.com, kabs.prashanth@gmail.com

Abstract

In this paper we have proposed a scheme which incorporates the concept of modular arithmetic and chaotic theory, for high level image encryption and decryption, which is useful for many applications. In the proposed scheme, we have used chaos theory to generate LSB of input image with MSB of secret image and used the same for Image encryption process. For Decryption, we have used Extract LSB of cipher image for decryption of an encrypted image. Our proposed scheme seems to be robust against various attacks.

Keywords: encryption, decryption, cipher image, chaotic maps, attacks.

1. Introduction

With the fascinating development in multimedia, communication and internet technology, security plays an important role while transfer and storage of sensitive information related to military, medical, science, engineering and forensic science. Security of the medical images is biggest challenge as it has sensitive information of patient. If any unauthorized access of patient image or alteration of the image may leads to wrong decision. Cryptography is basic method used for security of multimedia data such as text, audio, image and video etc. In cryptography there are some legacy encryption schemes such as Advanced Encryption Standard (AES), Data Encryption Standard (DES), and International Data Encryption Standard (IDES) and RSA etc given in techniques lead to high computational cost, high correlation between pixels and consume high computing power for image of large data capacity. Hence it may not be suitable for images applications, so we are using the chaos based cryptographic method.Cryptography is a basic method of storing and transferring of data or image in particular form so that only for whom it is intended can read.

Chaos is one of the emerging research directions in the multimedia encryption and decryption. Chaos means it is a state of confusion or disorder. Chaos is discovered by Edward Lorenz in 1963. Chaos system is dynamically nonlinear, aperiodic, and sensitive to initial condition, ergodic and deterministic in nature.Encryption will be defined as the conversion of plain imageinto a form called a cipher image that cannot be read by any people without decrypting the encrypted image.

Encryption is the most effective way to achieve data security. The process of encryption hides thecontents of a message in a way that the original information is recovered only through a decryption process. The purpose of Encryption is to prevent unauthorized parties fromviewing or modifying the data. Encryption occurs when the data is passed through somesubstitute technique, shifting technique, table references or mathematical operations. All thoseprocesses generate a different form of that data. The unencrypted data is referred to as theplaintext and the encrypted data as the ciphertext, which is representation of the original data in a different form.

Key-based algorithms use an Encryption key to encrypt the message. There are two generalcategories for key-based Encryption: Symmetric Encryption which uses a single key to encryptand decrypt the message and Asymmetric Encryption which uses two different keys – a publickey to encrypt the message, and a private key to decrypt it. Currently, there are several types ofkey based Encryption algorithms such as: DES, RSA, PGP, Elliptic curve, and others but all ofthese algorithms depend on high mathematical manipulations.

Decryption is the reverse process of encryption which is the process of converting encrypted image into its original plain image so that it can be read.

2. Literature survey

Mohammed Jawad1, developed based onImage encryption plays an important role to ensure confidential transmission and storage of image over internet. However, areal–time image encryption faces a greater challenge due to large amount of data involved. This paper presents a review on image encryption techniques of both full encryption and partial encryption schemes in spatial, frequency and hybrid domains.

. Rinki Pakshwar, Vijay Kumar Trivedi, Vineet Richhariya Rinki Pakshwar et al,mainly focuses mainly on the different kinds ofimage encryption and decryption techniques. In additionfocuses on image encryption techniques, As the use digitaltechniques for transmitting and storing images are increasing,it becomes an important issue that how to protect theconfidentiality, integrity and authenticity of images. There arevarious techniques which are discovered from time to time toencrypt the images to make images more secure. This paperpresents a survey of over 25 research papers dealing withimage encryption techniques scrambled the pixels of the imageand decrease the correlation among the pixels, so that we willget lower correlation among the pixel and get the encryptedimage. In this paper a Survey of Different Image Encryptionand encryption techniques that are existing is given. Itadditionally focuses on the functionality of Image encryptionand decryption techniques.

Lini Abraham1, Neenu Daniel2,developed the transmission of multimedia data including image and video is growing in telecommunications. Security is one of themain issues in transferring such sensitive information. Powerful image encryption algorithm is the solution for this problem. Thispaper is an implementation of a color image encryption algorithm based on Rubik's cube technique. The Rubik's cube techniqueis used for pixel permutation and a bit substitution method based on DNA sequences are used to change the value of each pixel onthe image. Then the time-stamp is appended with encrypted image, which can be used to identify the replay attack. For evaluatingthe performance of the algorithm a series of tests are performed. These tests include information entropy analysis, correlationanalysis, analysis of NPCR and UACI values etc.

B.V.Santhosh Krishna,are projected on image encryption algorithmshave been increasingly based on chaotic systems, but thedrawbacks of small key space and weak security in onedimensionalchaotic cryptosystems are obvious. This paper, anew image encryption scheme which employs one of the threedynamic chaotic systems (Lorenz or Chen or LU chaoticsystem selected based on 16-byte key) to shuffle the position ofthe image pixels (pixel position permutation) and uses anotherone of the same three chaotic maps to confuse the relationshipbetween the cipher image and the plain-image (pixel valuediffusion), thereby significantly increasing the resistance toattacks. The proposed system has the advantage of bigger keyspace, smaller iteration times and high security analysis such askey space analysis, statistical analysis and sensitivity analysiswere carried out. The results demonstrate that the proposedsystem is highly efficient and a robust system.

3. Methodology of work

In our proposed method we embed the secret image in the input image and we retrieve the secret image along with the input image. For embedding image in the image there are many algorithms available. In this paper we propose LSB Shifting to embed secret image in the input image. The embedded image along with the input image is retrieved by the shifting operations. In the previous works the input images were not completely restored. LSB shifting (LSBS) is a useful technique for image hiding. With LSB-based algorithm, high capacity and low distortion can be achieved efficiently. For image embedding, certain pixel values are shifted to create vacant spaces whereas some others are manipulated to carry hidden data by filling the created vacant spaces. A general framework to construct LSB algorithm is presented. According to the proposed general framework, one can get a LSB algorithm by simply designing the so called shifting and embedding functions.

Image data hiding methods have many applications. Image data hiding represents a class of processes used to embed data into cover images. Robustness is one of the basic requirements for image data hiding. In most cases, the cover image cannot be inverted back to the original image after the hidden data are retrieved. We propose a framework to the data along with the cover image. For most image data hiding methods, the host image is permanently distorted and it cannot be restored from the marked content. But in some applications such as medical image sharing, multimedia archive management, and image trans-coding, any distortion due to data embedding is intolerable and the availability of the original image is in high demand. To this end, a solution called “reversible data hiding” (RDH) is proposed, in which the host image can be fully restored after data embedding. RDH is a hybrid method which combines various techniques to ensure the reversibility. Its feasibility is mainly due to the lossless compressibility of natural images. Many RDH methods have been proposed in recent years, e.g., the methods based on lossless compression difference expansion (DE), histogram shifting (HS), and integer transform, etc. All these methods aim at increasing the embedding capacity (EC) as high as possible while keeping the distortion low.

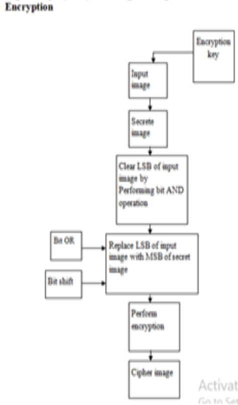

Encryption
Encryption key
Input image
Secrete image
Clear LSB of input image by Performing bit AND operation
Bit OR
Bit shift
Replace LSB of input image with MSB of secret image
Perform encryption
Cipher image

Figure 1: encryption process

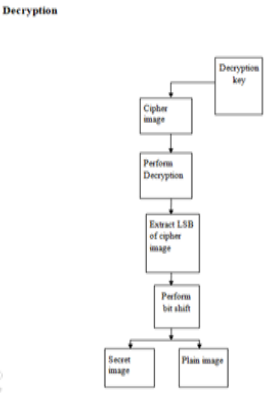
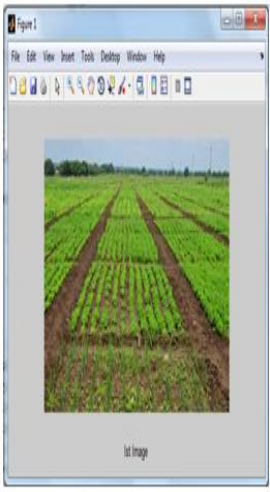


Figure 2: decryption process

4. Results and discussions

The proposed chaotic algorithm is quite simple and compact .The result shows that using this algorithm in image encryption results in accuracy and faster than traditional algorithm this work is also extended to colour images.



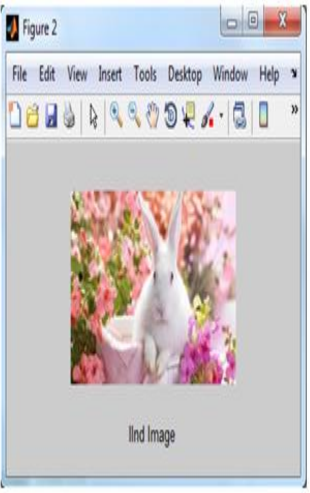
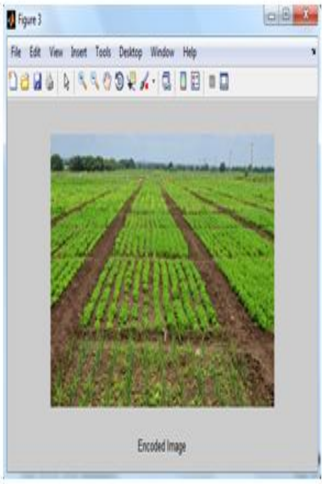


Figure 3: input imageFigure 4: The secret image

The above figure is taken as input image for the process and the size of the image is 212X320X3, the format of the image is JPG.

The above figure is taken as a secret image for the process and the size of the image is 118X210x3, the format of the image is JPG.



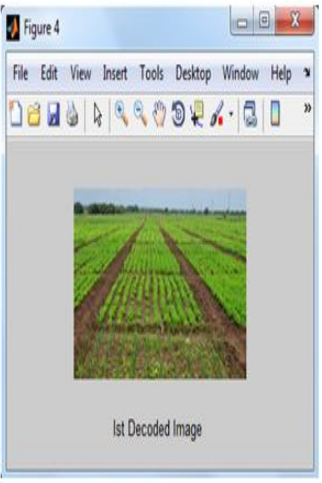


Figure 5: The encrypted imageFigure 6: First decoded image

The output of the encryption process as shown in the above figure, in which the secret image is hidden in the input image. The size of the encrypted image is 236X420X3. The Image format is JPG. The decoded image is as shown in figure. The size of the image is 212X320X3 and the Image format is JPG.

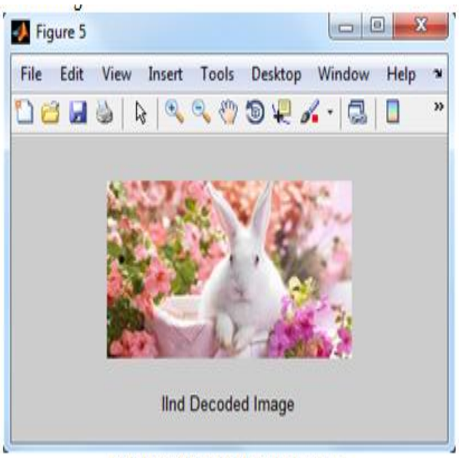


Figure 7: Second decoded image

The second decoded image is as shown in figure and the image size is 118X210X3. The Image format is JPG.

Conclusion

Based on the design rules discussed earlier, the newimage encryption scheme was designed. A suitable chaoticmap preserving the properties of chaos after discretizationwas chosen. By choosing a high dimensional chaotic system,the key space is increased. Complex non-linearity waspreserved by choosing suitable chaotic maps. Repeatedpermutations are avoided but pixel values are changed bythe diffusion function. By incorporating all these features,the proposed cryptosystem avoids all the crypto graphicalweaknesses of earlier chaos-based encryption systems.Number of security analysis were carried out on the newalgorithm and simulation results show that encryption anddecryption are good and the algorithm has good security androbustness.In this paper, we reviewed a wide-range of image encryption algorithms and classified them on the basis offull and partial image encryption schemes under spatial domain, frequency domain and hybrid domain categories.In the course of this review, some observations were made,which are that full encryption scheme ensures high level ofsecurity of encrypted data due to the fact that they encrypt the entire image, though much time is spent in such aprocess. In the case of partial encryption, only a region or some part of the image is encrypted. In other words, thetime spent in encrypting the region of interest is less in comparison to the full encryption schemes. For this reason,the partial encryption scheme is more appropriate for realtime applications.

References

[1]. Rinki Pakshwar et al,/(IJCSIT) International journal of computer science and

Technology,Vol.4 (1), 2013, 113-116

[2].Journal of Information Engineering and Applications, ISSN 2224-5782, Vol

3, No.6, 2013

[3].IJCSI International Journal of computer science issues, Vol 10,No.1,Nov 2013

[4].International journal of advanced research in software engineering Vol3,Issue 9,Sept

2013.

[5].International Journal of Information and Education Technology Vol 1,No 2,June

2011.