NOVATEUR PUBLICATIONS
INTERNATIONAL JOURNAL OF INNOVATIONS IN ENGINEERING RESEARCH AND TECHNOLOGY
[IJIERT] ISSN: 2394-3696 Website: ijiert.org
VOLUME 8, ISSUE 6, June. -2021

CHAOTIC IMAGE ENCRYPTION TECHNIQUE

Raghav Gupta
Department of Information Technology,
AKGEC, Ghaziabad, India.

Shushant Malik
Department of Information Technology,
AKGEC, Ghaziabad, India.

Pradeep Kumar
Department of Information Technology,
AKGEC, Ghaziabad, India.

Vaibhav Lakhmani
Department of Information Technology,
AKGEC, Ghaziabad, India.

ABSTRACT
In this paper, we will provide an overview of the mechanisms used in image protection, especially Chaos-based encryption techniques available today. We will see how previously proposed methods such as Data Encryption Standard (DES), Triple Data Encryption Standard (Triple-DES), and International Data Encryption Algorithm (IDEA) have been applied in image protection domain and how new concepts of Chaos-based encryption techniques are superior to traditional methods.
The chaotic system is rich in significance and in implication because of sensitivity to change initial conditions, control parameters, ergodicity, random-like behaviour, repeated processing and very high diffusion and confusion properties that are desirable for cryptography.

INTRODUCTION
Advances in space science, data analysis, and communication technologies present new opportunities for users
✓To increase productivity
✓Reduce costs
✓Facilitate innovation and
✓Create virtual collaborative environments for addressing the new challenges.

➤ The chaotic system was a new innovation because it can change
✓Initial conditions
✓Control parameters
✓ Ergodicity
✓Very high diffusion
✓Confusion properties that are desirable for Cryptograpy

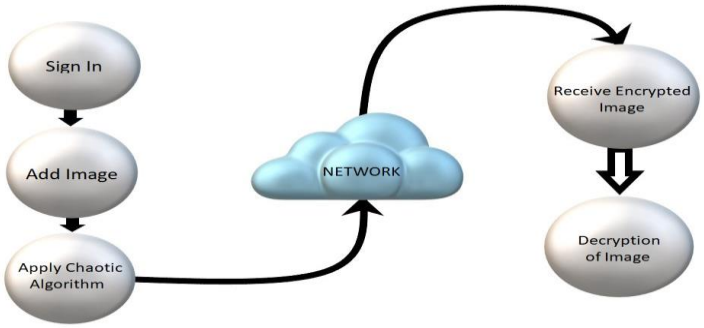


Fig. Chaotic Image Encryption Mechanism

Project Background

In this paper, we will provide an overview of the mechanisms used in image protection, especially Chaos-based encryption techniques available today. We will see how previously proposed methods such as Data Encryption Standard (DES), Triple Data Encryption Standard (Triple-DES), and International Data Encryption Algorithm (IDEA) have been applied in image protection domain and how new concepts of Chaos-based encryption techniques are superior to traditional methods.

The chaotic system is rich in significance and in implication because of sensitivity to change initial conditions, control parameters, ergodicity, random-like behaviour, repeated processing and very high diffusion and confusion properties that are desirable for cryptograpgy.

PURPOSE

The development of the Space Science and Technology has recently attracted a growing interest from researchers and industrial communities, mainly because of large number of possible applications capable to exploit remotely sensed data and satellite images. Advances in space science, data analysis, and communication technologies present new opportunities for users to increase productivity, reduce costs, facilitate innovation and create virtual collaborative environments for addressing the new challenges. GIS and Remote sensing technologies, along with related geospatial technologies, contribute powerful tools for preserving and protecting the nation‟s critical infrastructure.

In such systems, a space borne platform collects scientific data and transmits them to a ground station and at the ground segment, a series of image products are created that can be made available to research or commercial organizations for exploitation. The data delivery and sharing process, usually based on CD/DVD-ROM or on shared network environment (Internet, LAN, WAN etc), provides the user with a digital version of the remote sensing data and images. In the same way as for multimedia contents, the digital format implies an inherent risk of unauthorized copy or use of the product.

Similarly many digital services, such as Medical, Military, and Space imaging systems require reliable security in storage and transmission of digital images. The rapid progress of Internet in the digital world today, the security of digital images has become more and more important. The prevalence of multimedia technology in our society has promoted digital images to play a more significant role, which demands a serious protection of users‟ privacy. To fulfill such security and privacy needs in various applications, encryption of images is very important to minimize malicious attacks from unauthorized parties.

EXISTING SYSTEM

- There are traditional image encryption techniques like DES, Triple-DES and IDEA.

➤ Limitations

. Requires large data size
. Long computational time
. High computing power.
• Not suitable for practical image encryption and for online communications

3.1. Proposed System

A. The conventional cryptographic algorithms are mainly based on discrete mathematics.
B. chaos-based cryptography is relied on the complex dynamics of nonlinear systems
C. The image encryption algorithm includes two steps:

1. Firstly, the image fusion is completed between the original-image and the key-image.
2. the pixel values of the fusion image are encrypted by Henon chaotic system.

3.2. Security Analysis

1. A good encryption scheme should be sensitive to the secret keys, and the key space should be large enough to make brute-force attacks infeasible.
2. In our encryption algorithm, the key-image and the initial values of Henon Chaotic map are used as secret keys.

3. The key space is large enough to resist all kinds of brute-force attacks. The Experimental results also demonstrate that our scheme is very sensitive to the Secret key mismatch.

OBJECTIVE AND SCOPE OF THE PROJECT

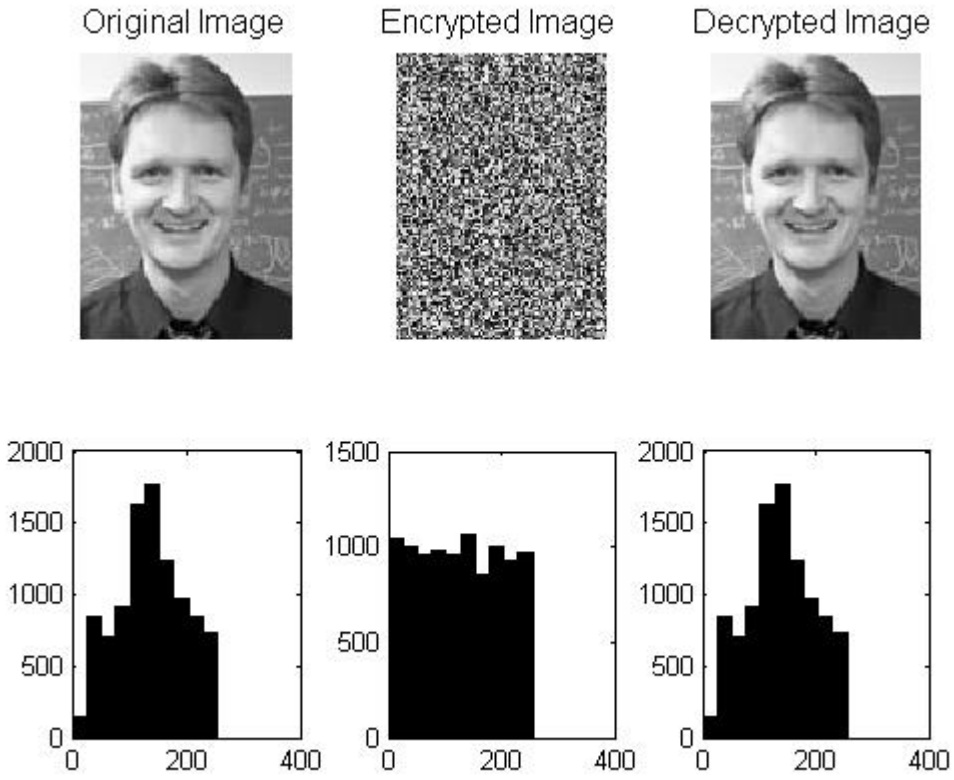
Objective

The main Objective was to provide an Image encryption mechanism which provides high security level, less computational time and power in reliable and efficient way to deal with balky, difficult and intractable data.

Scope

Although there are many image encryption techniques but none of them are suitable for the networking systems. So, the main scope of our project was to provide security for the images in the networking systems. Our project provides safe ways of means to transfer images between the networking systems confidentially.

Example Image Encryption



This figure shows original, encrypted, and decrypted images using the shuffle and mask process. We can see from the histograms of gray values in the encrypted case that diffusion objectives have been achieved, since information about the gray values of the original have been disguised so that an attacker with just the encrypted image stands little chance of recovering any information about the original. The procedure is still vulnerable to other attacks, as the report discusses.

Feasibility Study

The mentioned description of the system which is about to be developed can be implemented using the latest technologies which include:

○ Java- Java is a class based, object-oriented programming language that is designed to have a few implementation dependencies as possible.

○ Servlets- Servlets are the Java programs that runs on the Java-enabled web server or application server. They are used to handle the request obtained from the web server, process the request, produce the response, then send response back to the web server.
○ JSP- (Java Server pages) JSP not only enjoys cross-platform and cross-Web-server support, but effectively melds the power of server-side Java technology with features of static HTML pages.
○ Oracle 10g XE - Oracle Database 10g Express Edition (Oracle Database XE) is a free version of the world's most capable relational database
○ Rational Rose - The Rational Rose family of products is a set of UML modeling tools for software design. The Unified Modelling Language (UML) is the industry-standard language for specifying, visualizing, constructing, and documenting the artifacts of software systems. It simplifies the complex process of software design, creating a "blueprint" for construction of software systems..

METHODOLOGY

It is intended to the people who need privacy for their confidential images. It was most suitable in the networking Systems, so it was more eligible in Space Science research centers.
The user can have membership by concerning the administrator. The system dynamically generates member id on presenting the user details. The user can have transactions by having their member id. The user adds the image for encryption and encrypts it for confidential images.
Chaotic Image Encryption Techniques Project Users:
1. Administrator.
2. User.
3. Other (Guests).

Administrator:
Administrator is having all the rights to access this portal. Admin can view all the images, and the status of the encrypting and decrypting process. He will have control over the network whether to accept the server's request for receiving image. He will provide all the benefits for image encryption and decryption.

User:
The people who use this system for providing security for confidential images are users. There may be different set of users for this system. The users just load an image to encrypt and encrypt it and enter the destination systems IP address to transfer the image and he can view the status of the network for the sent image.

Guests:
Guest or the new user can only view the functionalities in the portal and they have no access permissions unless they are registered.
In Chaotic Image Encryption Techniques, there are mainly three modules:
1) Administrative
2) User
3) Encryption Module
4) Decryption Module
5) File Transfer Module
Administrative Module
o Maintains the user accountability
o Controls the user activities
User Module
The people who use this system for providing security for confidential images are users.
There may be different set of users for this system.
o The users just load an image to encrypt.
o Enter the destination systems IP address to transfer the image.
o User can view the status of the network for the sent image.

Encryption Module
o Selects the image
o Providing key for Encryption
Decryption Module
o Enter the key for Decryption
File Transfer Module
o Provide the view of the entering IP address for file transfer module

Proposed system provides a solution to existing system by extending its facilities. The proposed study aims to explore the possibility of using chaotic or chaos-based encryption techniques to protect remote sensing satellite images and provides high level of security in efficient and reliable way. Chaos based cryptographic scheme provides high security level, less computational time and power in reliable and efficient way to deal with balky, difficult and intractable data that why many researchers recommends that it is more suitable for multimedia data, especially for images. Chaos-based system has many properties to achieve high security level, such as sensitivity to change initial conditions and parameters, periodicity (a system that tends in probability to a limiting form that is independent of the initial conditions), random behavior and unstable periodic orbits with long periods. It has very high diffusion and confusion properties that are desirable for cryptosystem.

REQUIREMENT ANALYSIS

Software and Hardware Requirements

Software Requirements

The minimum software requirement specifications for developing this project are as follows:

Operating System	:	Windows XP
Presentation Layer	:	Java, Servlets, JSP
Web Server	:	Apache Tomcat 6.0
Database	:	Oracle 10g XE
IDE	:	Eclipse 3.3
Database Layer	:	JDBC
Documentation Tool	:	MS Office
UML Tools	:	Rational Rose

7.1. Hardware Requirements

The minimum hardware requirement specifications for developing this project are as follows:

Processor	:	Standard processor with a speed of 1.6GHz
RAM	:	256MB RAM or higher
Hard Disk	:	20GB or more
Monitor	:	Standard color monitor
Keyboard	:	Standard keyboard
Mouse	:	Standard mouse

INDUSTRY IMPACT

The development of the Space Science and Technology has recently attracted a growing interest from researchers and industrial communities, mainly because of large number of possible applications capable to exploit remotely sensed data and satellite images. Advances in space science, data analysis, and communication technologies present new opportunities for users to increase productivity, reduce costs, facilitate innovation and create virtual collaborative environments for addressing the new challenges. GIS and Remote sensing technologies, along with related geospatial technologies, contribute powerful tools for preserving and protecting the nation's critical infrastructure. In such systems, a space borne platform collects scientific data and transmits them to a ground station and at the ground segment, a series of image products are created that can be made available to research or commercial organizations for exploitation. The data delivery and sharing process, usually based on CD/DVD-ROM or on shared network environment (Internet, LAN, WAN etc.), provides the user with a digital version of the remote sensing data and images. In the same way as for multimedia contents, the digital format implies an inherent risk of unauthorized copy or use of the product. Similarly, many digital services, such as Medical, Military, and Space imaging systems require reliable security in storage and transmission of digital images. The rapid progress of Internet in the digital world today, the security of digital images has become more and more important. The prevalence of multimedia technology in our society has promoted digital images to play a more significant role, which demands a serious protection of users‟ privacy. To fulfill such security and privacy needs in various applications, encryption of images is very important to minimize malicious attacks from unauthorized parties. This project is intended to the people who need privacy for their confidential images. It was most suitable in the networking Systems, so it was more eligible in Space Science research centers.

CONCLUSION

A. The proposed algorithm has six merits:

1. The algorithm has a large enough key space to resist all kinds of brute force attack.

2. The cipher-image has a good statistical property

3. The encryption algorithm is very sensitive to the secret keys.

4. provides high security level

5. less computational time

6. Both reliable and efficient way to deal with balky, difficult and intractable data

B. The only disadvantage is that the application should be at both the sender and receiver in network system

REFERENCES

F. Belkhouche, U. Qidwai, I. Gokcen, and D. Joachim. "Binary Image Transformation Using Two-Dimensional Chaotic Maps." Proc. International Conf. on Pattern Recognition 4 (2004).
L. Kocarev and G. Jakimoski. "Logistic map as a block encryption algorithm." Physics Letters A 289, pp. 199-206. (2001).
G. Chen , Y. Mao , and C. K. Chui. "A symmetric image encryption scheme based on 3D chaotic cat maps." Chaos, Solitons and Fractals 21 pp 749-761. (2004).
M. Usama, M. K. Khana, K. Alghathbara, and C. Leeb. "Chaos-based secure satellite imagery cryptosystem." Computers & Mathematics with Applications, in press (2010).
N.K. Pareek, Vinod Patidar, K.K. Sud. "Image encryption using chaotic logistic map." Image and Vision Computing 24 pp. 926-934. (2006).
C. Cokal and E. Solak. "Cryptanalysis of a chaos-based image encryption algorithm." Physics Letters 373 15 pp. 1357-1360. (2009).