*International Journal of Current Research and Modern Education (IJCRME)*
*ISSN (Online): 2455 - 5428*
*(www.rdmodernresearch.com) Volume I, Issue I, 2016*

# DATA HIDING IN CRYPTOGRAPHY PROCESS USING KEYLESS ENCRYPTED ALGORITHM

**M. Vasumathi* & M. Rajakumar****

* PG Scholar, Department of Master of Computer Applications, Dhanalakshmi Srinivasan Engineering College, Perambalur, Tamilnadu

** Associate Professor & Head, Department of Master of Computer Applications, Dhanalakshmi Srinivasan Engineering College, Perambalur, Tamilnadu

**Abstract:**

*Securing data is a challenging issue in today's technology. Most of the data travel over the internet and it becomes difficult to make data secure. The information security has become one of the most significant problems in data communication. So it becomes an inseparable part of data communication. In order to address this problem, cryptography technique is used for data transmission to making data secure. There arises a need of data hiding. So here using a combination of stegnography and cryptography for improving the security. All previous methods embed data by random vacating room from the encrypted images, which may be subject to some errors on data extraction and image restoration. In this project, propose a novel method by shuffling room in image pixels process before encryption with a traditional Keyless algorithm, and thus it is easy for the data hider to shuffling embed data in the encrypted image. The proposed method can achieve real data hidden in the image process, and it will take less time if the file size is large. The cryptography method can be applied for data encryption and decryption for sending confidential data.*

**Index Terms:** Keyless algorithm, Cryptography, Stegnography, Encryption & Decryption

## 1. Introduction:

The information security has become one of the most significant problems in data communication. So it becomes an inseparable part of data communication. In order to address this problem, cryptography technique is used for data transmission to making data secure. So here we are using a combination of stegnography and cryptography for improving the security. In this project I propose a novel method by shuffling room in image pixels process before encryption with a traditional Keyless algorithm, and thus it is easy for the data hider to shuffling embed data in the encrypted image. The proposed method can achieve real data hidden in the image process, and it will take less time if the file size is large. The cryptography method can be applied for data encryption and decryption for sending confidential data .

### 1.1. Problem and Discussion:

Using a cryptography technique is used for data transmission to making data secure. So here we are using a combination of stegnography and cryptography for improving the security.

## 2. Related Works:

"Keyless Cryptography in Grid Computing Cyclic Shift Transposition Algorithms**",** Gomathi. Grid computing is a distributed computing model in which new kind of systems are combined to form a heterogeneous computational resources such as computers, storage space, sensors, and experimental data. The grid can seamlessly, transparently and dynamically supply the computing and data resources when a user wants to request them. In recent years, a security issue has become an important concern for grid computing. A strong mutually encrypted and decrypted methodology is

needed for user and to prevent the grid resources from being illegally visited In this paper, we proposed a keyless Cyclic Shift Transposition Algorithm (CSTA) which uses a combination of shifting and transposition without public or private key to secure the data in the grid computing system.

"Proposed System for data hiding using Cryptography and Steganography", Dipti Kapoor Sarmah. Steganography and Cryptography are two popular ways of sending vital information in a secret way. One hides the existence of the message and the other distorts the message itself. There are many cryptography techniques available; among them AES is one of the most powerful techniques. In this project we are developing a system where we develop a new technique in which Cryptography and Steganography are used as integrated part along with newly developed enhanced security module. In Cryptography we are using AES algorithm to encrypt a message and a part of the message is hidden in DCT of an image; remaining part of the message is used to generate two secret keys which make this system highly secured.

**3. Proposed Work:**

Cryptography is the art of achieving security by encoding the data into unreadable form. Data that can be unreadable and not understood with difficulty is called encryption cryptography. Proposed process shuffling he data image pixels from the encrypted images is relatively difficult and sometimes inefficient, If we shuffling the order of encryption and vacating room prior to image encryption at content owner side with a traditional Keyless algorithm, and thus it is easy for the data hider to shuffling embed data in the encrypted image. Encrypted images would be more natural and much easier which leads us to the novel framework for secure data transmission.

**3.1 Advantages:**

- ✓ In this system it uses traditional keyless algorithm, and thus it is easy for the data hider to shuffling embed data in the encrypted image.
- ✓ Using this system data extraction and image recovery are free of any error.
- ✓ Security enhancement in the cryptography.

**3.2 Modules:**

- ✓ Registration and authentication
- ✓ Owner side Encryption the data using keyless Algorithm
- ✓ Cryptography User Data to image Conversation
- ✓ Client Decryption the Data with secure process

**3.3 System Architecture:**

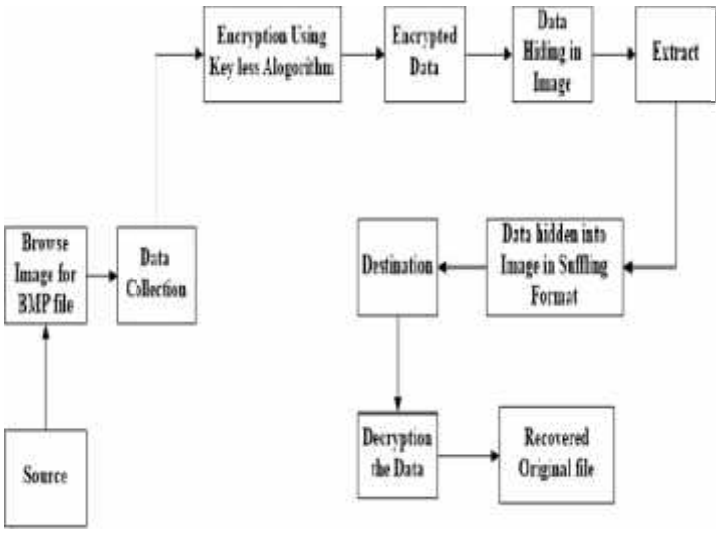


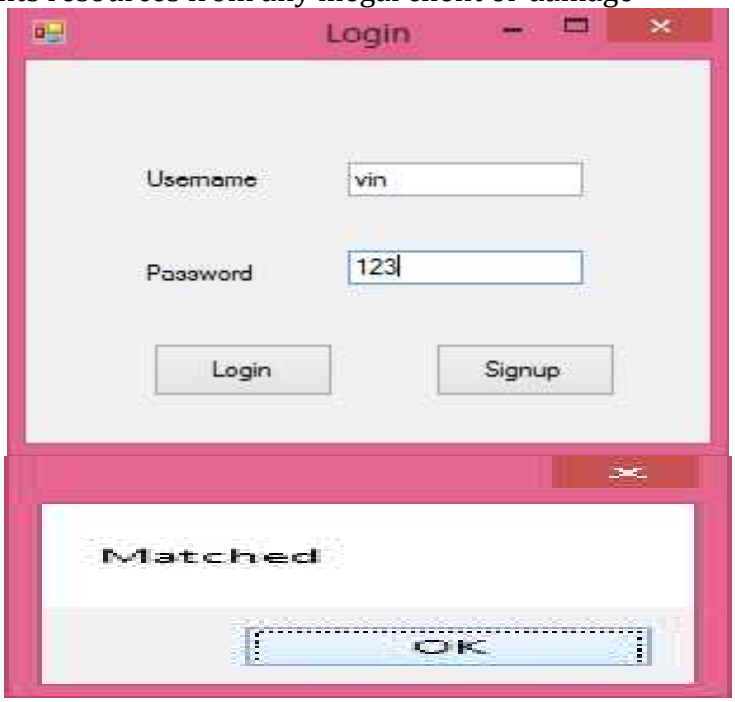

Figure 1: Shows the System Architecture

**3.4 Used Algorithm:**

The keyless algorithm is used for the data encryption. This Keyless Algorithm is a Feistel Network, iterating a simple encryption function 3 times. The block size is 64 bits, and the key can be any length up to 448 bits. Although there is a complex initialization phase required before any encryption can take place, the actual encryption of data is very efficient for secure data encryptions. It is suitable for applications where the key does not change often, like a communications link or an automatic file encryption

**4. Experimental Analysis and Results:**

In this framework it allows user to enter the user name and password in order to restrict the user to access the system. Then it validates the entered user name and password, if it is correct it will allow the user to access the application. Access users only to have authentication process before registration, Authentication process is always occurred prior to mobility management process included location registrations and service delivery, and it also ensures network resources are accessed by authorized clients and prevents resources from any illegal client or damage



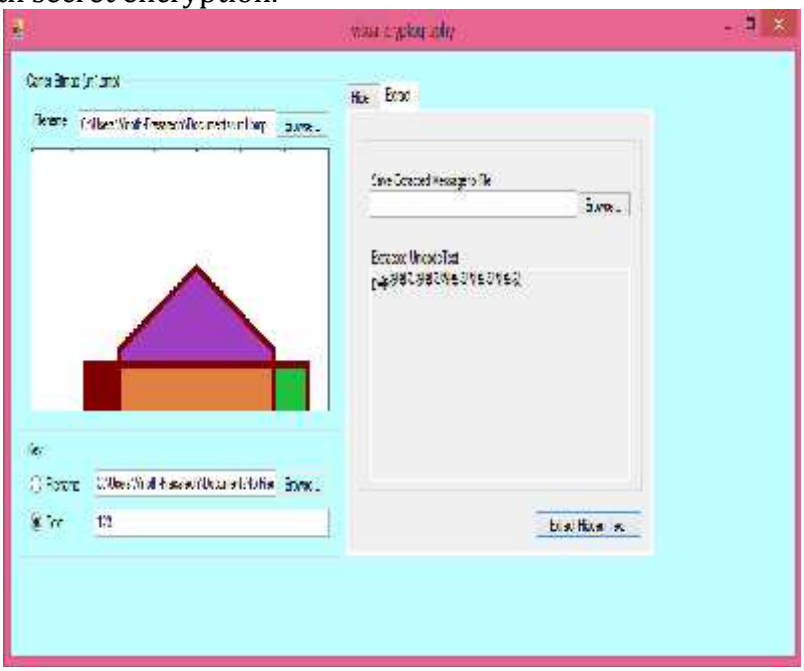

**4.1 Owner Side Encryption the Data Using Keyless Algorithm:**

In this module it allows to pick the message and then to enter the password key for encryption after that has to enter the message, that have to be encrypted. Once this all over, encryption is carried out. The keyless algorithm is used for the data encryption. This Keyless Algorithm is a Feistel Network, iterating a simple encryption function 3 times. The block size is 64 bits, and the key can be any length up to 448 bits. Although there is a complex initialization phase required before any encryption can take place, the actual encryption of data is very efficient for secure encryptions.

**4.2 Cryptography User Data to Image Conversion:**

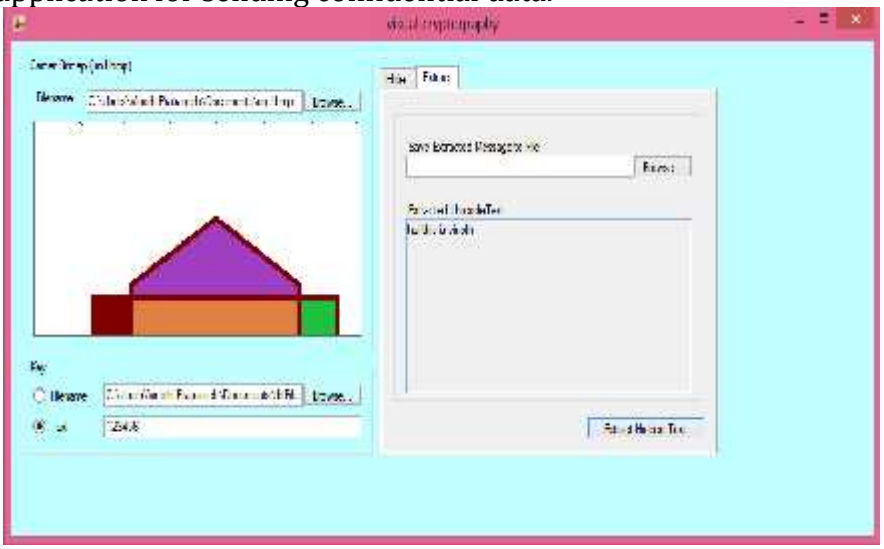
Cryptography is that branch of science which is concerned with the mathematical techniques for keeping message secure and free from attacks. Cryptography is the art of achieving security by encoding the data into unreadable form. Data that can be read and understood without any difficulty is called plain text or clear text. The method of encoding Plain text in such a way as to hide its content is called encryption. Technique is used to shuffling room in voice pixels process before

encryption. The data are hidden in the every Shuffling pixels of the voice. The voice having data with secret encryption.



**4.3 Client Decryption with the Secure Data Process:**

In this module it allows to pick the encrypted image received from the owner Side Encrypting Data and then to enter the password key to decrypt. If the image and the key is correct then the corresponding message will be displayed. To decrypt any file one has to know exactly what is the key matrix and to find the random matrix theoretically one has to decrypt the cryptography data. The Decryption Key is send by the owner. The keyless method can be applied for data encryption and decryption in any type of application for sending confidential data.



**5. Conclusion:**

Security in the Internet is improving. The increasing use of the Internet for commerce is improving the deployed technology to protect the financial transactions. Extension of the basic technologies to protect multicast communications is possible and can be expected to be deployed as multicast becomes more widespread. Control over routing remains the basic tool for controlling access based on the keyless algorithm

**6. Future Enhancement:**

Implementing particular policies will be possible as multicast routing protocols improve. Cryptography is a tool which may alleviate many of the perceived problems of using the Internet for communication

**7. References:**

1. Handramouli, R., Kharrazi, M. & Memon, N., "Image Steganography and steganalysis: Concepts and Practice", Proceedings of the 2nd International Workshop on Digital Watermarking, October 2010
2. Stefan Katznbeisser, Fabien.A., P.Petitcolas editors, Information Hiding Technique for Steganography and Digital Watermarking, Artech House, Boston. London, 2011.
3. Wang, H & Wang, S, "Cyber warfare: Steganography vs. Steganalysis", Communications of the ACM, 47:10, October 2004
4. Marvel, L.M., Boncelet Jr., C.G. & Retter, C., "Spread Spectrum Steganography", IEEE Transactions on image processing, 8:08,2010
5. Dunbar, B., "Steganography techniques and their use in an Open-Systems environment", SANS Institute, January 200219th National Information Systems Security Conference, 1G., Derrick, (2001), Data watermarking Steganography and watermarking of digital data, Computer Law & Security Report, 17 (2), 101-104.
6. Ross J. Anderson, Fabien A.P. Petitcolas, "On the Limits of Steganography", IEEE Journal of Selected Areas in Communications,