ISSN (Online) 2249 - 054 X

International Journal of Computing and Corporate Research

Specialized and Refereed Journal for
Research Scholars, Academicians, Engineers and Scientists

http://www.ijccr.com

International Manuscript ID : ISSN2249054X-V3I3M2-052013

VOLUME 3 ISSUE 3 May 2013

IMPLEMENTATION OF IMAGE AND AUDIO DATA USING KUDOS & COMPRESSION TECHNIQUES

Vandana Chandel

M.Tech (CSE) Student

Bahra University, Solan (H.P)

Astt.Prof. Miss Nidhi Sood

Bahra University, Solan (H.P)

ISSN (Online) 2249 - 054 X

International Journal of Computing and Corporate Research

Specialized and Refereed Journal for
Research Scholars, Academicians, Engineers and Scientists

http://www.ijccr.com

International Manuscript ID : ISSN2249054X-V3I3M2-052013

VOLUME 3 ISSUE 3 May 2013

Abstract - Cryptography can be defined as the art or science of altering information or change it to a chaotic state, so that the real information is hard to extract during transfer over any unsecured channel. The prime goal of this paper is applying kudos method to image and audio file data along with the compression technique and will analyze the parameters of algorithm such as encryption time, decryption time and compression time.

***Index Terms*- Cryptography, decryption, encryption, keyless, kudos, sequence counter.**

1. INTRODUCTION

Cryptography can be defined as the art or science of altering information or change it to a chaotic state, so that the real information is hard to extract during transfer over any unsecured channel. Latest advancements in technology and new concepts like quantum cryptography have added a complete new dimension to data security. The cryptography algorithms are categorized into two types on the basis of key management:-

- Key-Oriented Encryption Algorithm.
- Keyless Encryption Algorithm

Key-oriented algorithms are very efficient but they were very bulky to manage as key handling must be done. Due to the great overhead, keyless algorithms seem an attractive option. But what about security by keyless, the solution-KUDOS encryption, which is a keyless security algorithm to provide ultimate security at the one level above of key-oriented. The proposed Algorithm is known as Keyless User Defined Optimal Security (KUDOS). As the name suggests, KUDOS algorithm is keyless because there is no key involved in the encryption process. Only sequence counters are used. The sequence counters

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists

http://www.ijccr.com

International Manuscript ID : ISSN2249054X-V3I3M2-052013

VOLUME 3 ISSUE 3 May 2013

have a definite start point and a particular increment value. The sequences are merged with the actual data at a particular level and encrypted data then replaces original data [1].

2. LITERATURE REVIEW

KaushikAkhil,Satvika,BarnelaManoj,KumarAnant [1] proposed an algorithm in this paper is Keyless User Defined Optimal Security Encryption (KUDOS) is based on the concept of user customization. The algorithm doesn't use the traditional approach of using an encryption key; but defines a series of sequence-counters for encoding. The cryptographic algorithm is based partially on both stream and block encryption, hence the output of same input block over same input sequence-counter is dissimilar and provides enhanced security.

S.S. Maniccam and N.G. Bourbakis [2] have presented a new methodology which performs both lossless compression and encryption of binary and gray-scale images. The compression and encryption schemes are based on SCAN patterns generated by the SCAN methodology. They achieved compression ratio of 1.6353 on Lena Image. The SCAN method takes about 50 seconds to compress-encrypt and about 10 seconds to decompress-decrypt a 512×512 gray scale image.

Nikolaos G. Bourbakis [3] presented an image data compression-encryption scheme by using the words (patterns, or orders) produced by an image processing language called SCAN. The SCAN is a formal language-based two-dimensional spatial-accessing methodology which can efficiently specify and generate a wide range of scanning paths or space filling curves. The proposed methodology can compress

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists

http://www.ijccr.com

International Manuscript ID : ISSN2249054X-V3I3M2-052013

VOLUME 3 ISSUE 3 May 2013

and encrypt both binary and grey level images. Compression is based on Genetic Algorithm approach using fractal based language G-SCAN. Encryption is carried out using transposition cipher based on SCAN. It is based on permutation of N×N image i.e. N×Ni.

D. Maheswari, V. Radha [4] employed lossless compression using a novel layer based compound image compression technique that uses XML compression and JPEG to compress data. The FG layer is compressed using an XML compressor and BG layer is compressed using JPEG 2000. The encryption scheme, called, Shuffle Encryption Algorithm (SEA), proposed by Yahiya and Abdalla (2008), is used. The average total time (compression time + decompression time) taken by XMLCC to compress an image was 0.79 seconds for compression and 0.68 seconds for decompression. But these results are still slower than DjVu. However, the XMLCC technique is superior to JPEG.

Anil Kumar A, Anamitra Makur[5] suggested that compression of encrypted data is possible by using distributed source coding. They considered the encryption, followed by lossless compression of gray scale and color images. They also proposed to apply encryption on the prediction errors instead of directly applying on the images and use distributed source coding for compressing the cipher texts. Decompression and decryption are performed in a single phase. They achieved compression ratios varying from 1.5 to 2.5 despite encryption. On Lena image they obtained the compression result as 5.39 bits per pixel.

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists

http://www.ijccr.com

International Manuscript ID : ISSN2249054X-V3I3M2-052013

VOLUME 3 ISSUE 3 May 2013

3. PROBLEM DEFINITION

This paper will describe a new approach to implement the KUDOS (Keyless User Defined Optimal Security Encryption) method to image or audio file data along with the compression technique.
Encryption at three levels i.e. blocks level, character level and binary level that gives safety three times popular then other algorithms. This algorithm is faster because of optimization techniques employed in the programing. The user can increase or decrease security and speed depending upon his/her needs. Data compression can also be used for in-network processing technique in order to save energy because it reduces the amount of data in order to reduce data transmitted and/or decreases transfer time because the size of data is reduced. Transformation algorithm does not compress data but rearrange or change data to optimize input for the next sequence of transformation or compression algorithm. Most compression methods are physical and logical.

4. OBJECTIVES

The objective of this dissertation is to implement KUDOS method to image or audio file data along with the compression technique and will analyses the parameters of algorithm such as encryption and decryption time, compression time. The objectives are:-

- To make data more securable.
- To encrypt or compress audio and image data.

There is no key involved in the encryption process. Only sequence counter are used.
It used both stream cipher and block cipher to enhance the security.

5. RESEARCH METHODOLOGY

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists

http://www.ijccr.com

International Manuscript ID : ISSN2249054X-V3I3M2-052013

VOLUME 3 ISSUE 3 May 2013

Methodology of constructing the proposed system will consists of various modules. Each module uses different techniques and algorithms to perform its specific tasks. After a particular module completes its task, its output will become input for the next module. In the end the combined effort of each module will be displayed.

Symmetric Key Algorithm:-

The KUDOS cryptographic algorithm falls under the symmetric encryption, i.e. the same key is used at both ends to encrypt and decrypt the data. However, KUDOS actually depends on the sequence counter instead of the encryption key. The major benefit of using KUDOS over other encryption algorithms is its power of customization. The user can manipulate the sequence counter according to his needs; whether he wants it to be simple and faster or hard to crack and secure.

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists

http://www.ijccr.com

International Manuscript ID : ISSN2249054X-V3I3M2-052013

VOLUME 3 ISSUE 3 May 2013

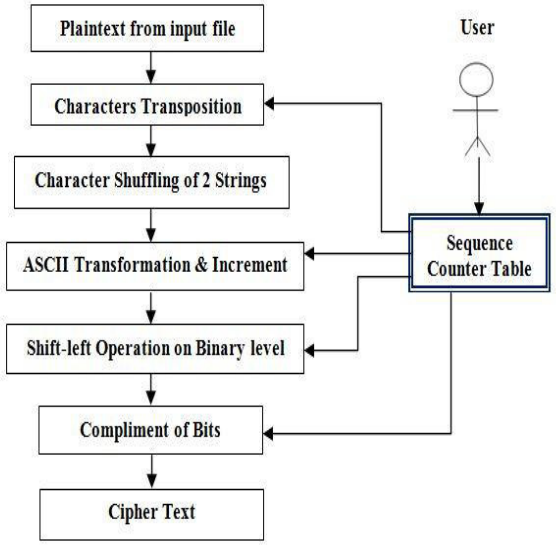

Figure 2. KUDOS Encryption Process

The algorithm is implemented in java programming language. JAVA technology is both a programming language and a platform. The Java programming language is the language in which Java applications, applets, servers, and components are written. The Java platform is the predefined set of Java classes that exist on every Java installation; these classes are available for use by all Java programs. The Java platform is also sometimes referred to as the Java runtime environment or the core Java APIs (application programming interfaces).

Features of Java are follows:

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists

http://www.ijccr.com

International Manuscript ID : ISSN2249054X-V3I3M2-052013

VOLUME 3 ISSUE 3 May 2013

- Simple
- Object Oriented
- Robust
- Security

8. REFERENCES

[1] KaushikAkhil, Satvika, BarnelaManoj, KumarAnant" Keyless User Defined Optimal Security Encryption" International Journal Of Computer And Electrical Engineering Vol.4, No.2.April2012

[2] S. S. Maniccam, and N. G. Bourbakis "SCAN Based Lossless Image Compression and Encryption" IEEE 0-7695-0446-9/99, pp. 490-499, 1999

[3] Nikolaos G. Bourbakis, ―Image Data Compression-Encryption Using G-Scan Patterns‖ *IEEE 0-7803-4053-1/97*, pp. 117-1120, 1997

[4] D. Maheswari, V.Radha,―Secure Layer Based Compound Image Compression using XML Compression‖ *978-1-4244-5967-4/IEEE*, 2010

[5] Anil Kumar A and AnamitraMakur, ―Distributed Source Coding based Encryption and Lossless Compression of Gray Scale and Color Images‖ ,*IEEE978-1-4244-2295-1*, 760 MMSP Singapore, pp. 760-764, 2008