Mpeg-7 Visual Shape Descriptor Encryption

N.Geetha, K.Mahesh

Abstract: Current issue of multimedia content is managing and securing the millions of data. Metadata is the glue to the millions. In our digital world the multimedia information passed through unsecured channel. In past few years the security of multimedia is a big issue in our digital world. The cryptography technique is suitable for securing the multimedia data. Nowadays transmission of video files are increased in digital transmission. The Surge of Mpeg video is different from other multimedia data like text, image, audio etc. Because of real-time limitations Mpeg video required special encryption algorithm to meet the high security. In this research work a new secure algorithm has been proposed to secure the Mpeg-7 standard. Finally the proposed algorithm has been compared with various parameters like encryption time, size after encryption.

Index Terms: Cryptography, Mpeg-7 Encryption, Visual Shape Descriptors Encryption, Rijndael Algorithm.

1. INTRODUCTION

Roaming of multimedia data have become more popular nowadays. The sensitive information having departments like Government, Hospitals occupy more and more fields like digital data libraries, E-business, Home entertainment, News programs, and Editing in media field[1], especially E-health contains privacy information of patients. The growth of the amount of classified multimedia content is fast and requires fitting methods and strategies to describe and manage the classified multimedia content efficiently and securely. The multimedia standard MPEG-7[2,3,4] is suitable for the requirements of effectively describing multimedia contents.[6] The descriptive tools provided in MPEG-7 do not include the contrivance of encryption, therefore, there is a need to develop security technique that perform encryption and make utilize and extend MPEG-7 Description Tools in order to provide protection for multimedia contents. There is a characters in multimedia contents could meet the security level well. Basically Multimedia contents have taken huge number of elements, There is different security levels for each element. Therefore, the performance of encryption to those elements should be according to the security level of each element, the encryption mechanism should take into account and make full use of the properties of MPEG-7. Section-2 Introduction to Mpeg-7, Section-3 Literature Survey, Section-4 Existing Encryption Method, Section-5 Proposed work, Section-6 Performance Evaluation, Section-7 Conclusion

2. INTRODUCTION TO MPEG-7

The MPEG-7 standard provides tools for effectively and efficiently describing the multimedia contents [1,5]. The classified multimedia is a multimedia that involving some sensitive contents or security information, therefore, the multimedia contents could also be described by MPEG-7 standard tools: Descriptors (Ds), Description Schemes (DSs), and Description Definition Language (DDL) are three main components of the standard. MPEG-7 shape descriptors properties consign the foundation of our encryption scheme.

3. LITERATURE SURVEY

Zheng Xiaojian, In this research work author address the security issues of the classified multimedia contents, a multilevel encryption scheme is presented which support multilevel encryption by introducing the time seed which used for generating time master key and then further generating encryption key. This scheme takes advantage of the properties of MPEG-7 standard to generate the multimedia hierarchy organized into tree structure involving many elements each of which belongs to a security clearance level, the sensitive element or security content can be encrypted with proper key in term of security level and then the entire multimedia encrypted with another appropriate key and the multilevel encryption achieved and introducing the secure user who must be the valid user and passed the identity authentication, secure server which is responsible for key management and identity authentication, secure object involving sensitive or privacy information of classified multimedia, and the comprehensive user identity authentication which considering the environment factors and the fingerprint of secure user, and the time seed which used for generating time master key and then further generating encryption key. This scheme takes advantage of the properties of MPEG-7 standard to generate the multimedia hierarchy organized into tree structure involving many elements each of which belongs to a security clearance level.[8] Jayshri Nehete et.al, In this research author encrypts MPEG video stream is quite different from traditional textual data because inter frame dependencies exists in MPEG video. Author present a real-time MPEG video encryption algorithm based on AES which is fast enough to meet the real-time requirements. Author selectively encrypts a fraction of the whole video. It is faster than encrypting the whole video with AES. Author uses MPEG-1 videos sign-bits. It encrypts at most 128 bits, no matter what type of frame is used. [9] Shujun Li et.al, In this paper, author uses perceptual encryption algorithms of MPEG videos are reviewed and some problems, especially security defects of two recently proposed MPEGVideo perceptual encryption schemes, are pointed out. Then, a simpler and more effective design is suggested, which selectively encrypts fixed-length codewords (FLC) in MPEG-video bitstreams under the control of three perceptibility factors. The proposed design is actually an encryption configuration that can work with any stream cipher or block cipher. The author focuses on the problem of how to realize perceptual encryption of MPEG videos. Based on a comprehensive survey on related work and performance analysis of some existing perceptual video.
encryption schemes. [10] Shujun Li et.al, In this paper author produce the security of a recently proposed MPEG-video encryption scheme based on secret Huffman tables. In this paper author shows that: 1) the key space of the encryption scheme is not sufficiently large against divide-and-conquer (DAC) attack and known-plaintext attack; 2) it is possible to decrypt a cipher-video with a partially known key, thus dramatically reducing the complexity of the DAC brute-force attack in some cases; 3) its security against the chosen-plaintext attack is very weak. As a result, it is found that the scheme is not sufficiently secure against DAC (divide-and-conquer) brute-force attack and known-plaintext attack, and is very weak against the chosen-plaintext attack.[11] Miroslaw Bober, In this paper author describes techniques and tools for shape representation and matching, developed in the context of MPEG7 standardization. The application domains for each descriptor are considered, and the contour-based shape descriptor is presented in some detail. Their performance has been tested, and it has been shown that the descriptors are efficient, concise, and easy to extract and match.[12] Lintian qiao and klara nahrstedt, In this research work author evaluate, and compare representative MPEG encryption algorithms, Naive Algorithm, Selective Algorithm, Zigzag Permutation Algorithm, Video Encryption Algorithm, and Pure Permutation Algorithm, with respect to not only their encryption speed metric, but also their security level and stream size metrics. Finally author conclude that VEA meets the requirements of most multimedia applications because it provides overall high security, size preservation, and relatively fast encryption. Any other algorithms suffers from either low security, or low speed, or stream size increases.[13] Xiang Bai et.al, In this paper author describes shape similarity and shape retrieval are very important topics in computer vision. In this paper, author provide a new perspective to this problem by considering the existing shapes as a group, and study their similarity measures to the query shape in a graph structure. Our method is general and can be built on top of any existing shape similarity measure. Author produces a new similarity is learned through graph transduction. The new similarity is learned iteratively so that the neighbors of a given shape influence its final similarity to the query. In this work, author adapted a graph transductive learning framework to learn new distances with the application to shape retrieval, shape classification, and shape clustering. The key idea is to replace the distances in the original distance space with distances induces by geodesic paths in the shape manifold.[14] Naif Alajlan et.al, In this paper, author adopts geometry-based image retrieval system is developed for multi object images. Author modeled both shape and topology of image objects using a structured representation called curvature tree (CT). The hierarchy of the CT reflects the inclusion relationships between the image objects. To facilitate shape-based matching, triangle-area representation (TAR) of each object is stored at the corresponding node in the CT. The similarity between two multiobject images is measured based on the maximum similarity subtree isomorphism (MSSI) between their CTs. For this purpose, author adopt a recursive algorithm to solve the MSSI problem and a very effective dynamic programming algorithm to measure the similarity between the attributed nodes. medical images and the MPEG7 CE-1 database of 1,400 shape images have shown the effectiveness of the proposed method.[15] Mohammad Reza Daliri and Vincent Torre, In this research work author introduces a new method for shape recognition and retrieval. The suggested algorithm is based on several steps. The algorithm analyzes the contour of pairs of shapes. Their contours are recovered and represented by a pair of N points obtained by linear interpolation. Given two points pi and qj from the two shapes the cost of their matching is evaluated by using the shape context and by using dynamic programming the best matching between the point sets is obtained. After alignment, each contour is transformed into a string of symbols and a modified version of edit distance is used to compute the similarity between strings of symbols. Finally, recognition and retrieval are obtained by a simple nearest-neighbor procedure. The algorithm for shape recognition and retrieval described in the present paper has been tested on a variety of shape databases and for most of them provides better performances than all presently available algorithms. Indeed for the Kimia, natural silhouette, diatom, swedish Leaf, MPEG-7, marine, gesture and ETH-80, the proposed algorithm provides results for both recognition and retrieval superior to almost all previously published algorithms.[16] Zhuowen Tu and Alan L. Yuille, In this work author presents an algorithm for shape matching and recognition based on a generative model for how one shape can be generated by the other. This generative model allows for a class of transformations, such as affine and non-rigid transformations, and induces a similarity measure between shapes. The matching process is formulated in the EM algorithm. The author shows how the EM algorithm can be approximated by using informative features, which have two key properties—invariant and representative. They are also similar to the proposal probabilities used in DD MCMC. Author tests the algorithm on a variety of data sets including MPEG7 CE-Shape-1, Kimia silhouettes, and real images of street scenes. This work is currently limited by the types of representations author used and the transformations author allow.[17]

4. EXISTING ENCRYPTION METHODS
This section describes details about the existing ways and algorithms that have been used for video encryption so far. The Following are existing ways to encrypt the video.

- Fully Layered Encryption
- Scrambling Based Encryption
- Selective Encryption
- Perceptual Encryption
- Chaotic Encryption

4.1 Fully Layered Encryption
First compression can be done in the video to reduce the size of the video and then using algorithms like AES and DES encryption. Because of the heavy computation, it is not suitable for real-time video.

4.2 Scrambling Based Encryption:
The scrambling can be takes place to encrypt the media content. It changes the position of the pixel and does not change its value. Vulnerable to known-plaintext attack.

4.3 Selective Encryption:
The required bytes of the video frames only takes place encryption. The computational speed is fast but the encryption ratio is low.

4.4 Perceptual Encryption:
The video quality is partially degraded in perceptual encryption. The pirated videos contains low quality video due to perceptual encryption. Known-chosen plaintext attack is vulnerable to perceptual encryption.

4.5 Chaotic Encryption:
Chaos based video encryption is best suited for real-time video encryption because of low computational complexity, format-complaint, invariance of compression ratio, real-time, strong transmission error tolerance, multiple levels of security and hence, it is superior over other conventional encryption methods[7].

5. PROPOSED WORK
In this approach, The Mpeg-7 Shape Descriptor can be used for encryption process. The tiff images of Mpeg-7 data set were used for encryption. In this research work, the Rijndael algorithm was tested on the Mpeg-7 Core Experiment shape-1 dataset. First the extracted contour input images are binarized and then used for encryption.

5.1 FLOW OF MPEG-7 SHAPE DESCRIPTOR ENCRYPTION

5.2 FLOW OF MPEG-7 SHAPE DESCRIPTOR DECRYPTION

6. PERFORMANCE EVALUATION
The Simulation results can be done in MATLAB with a configuration of Intel Pentium Inside, Windows 7. The proposed technique can be compared with existing technique is as follows.
Rijndael algorithm. It encrypts at most 128 bits, no matter what type of Mpeg-7 shape descriptors is used. This considerably reduces encryption computations achieving satisfactory encryption results. A software implementation is fast enough to meet the real-time requirements of MPEG-7 decoding. Mpeg-7 applications are Education (e.g., distance learning), Journalism (e.g. searching for speeches by voice or face), Cultural services (history museums, art galleries, etc.), Entertainment (e.g. searching a game, karaoke), Investigation services (human characteristics recognition, forensics), Geographical information systems (GIS), Remote sensing (cartography, ecology, natural resources management, etc.), Surveillance (traffic control, surface transportation), Bio-medical applications, E-commerce and shopping (e.g. searching for clothes/patterns), Architecture, real estate, and interior design, Social (e.g. dating services), Film, video and radio archives. Some Mpeg-7 Applications should have security, for this purpose cryptography technique can be used for Mpeg-7 standards.

8 ACKNOWLEDGMENT
I am thankful for doing this research work has been supported by Alagappa University Research Fellowship (AURF) and RUSA Phase-2.0/Ph.D Fellowship/2019.

REFERENCES
[8]. Shujun Li, Guanrong Chen, Fellow, IEEE, Albert Cheung, Member, IEEE, Bharat Bhargava, Fellow,


[14]. Xiang Bai Student Member, IEEE, Xingwei Yang, Longin Jan Latecki Senior Member, IEEE, Wenyu Liu, and Zhuowen Tu, “Learning Context Sensitive Shape Similarity by Graph Transduction”, IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE.


[16]. Mohammad Reza Daliri, Vincent Torre, “Robust symbolic representation for shape recognition and retrieval”, 0031-3203/$30.00 2007 Elsevier Ltd. All rights reserved. doi:10.1016/j.patcog.2007.10.020.