Volume 3, Issue 5, May 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Issues and Challenges in Symmetric Key based Cryptographic Algorithm for Videos and Images

Niraj Kumar[1], Prof. Sanjay Agrawal[2]
Department of Computer Engineering and Application,
National Institute of Technical Teachers' Training and Research, Shyamla Hills,
Bhopal , India

Abstract : - ***Modern era is fully dependent on internet communication. Through internet we can transfer data anywhere in the world. Through these various activities can be done such as online bill payment, shopping. The network is currently used for carrying personal information as well as financial data. Thus, it is necessary to secure the network, in order that unauthorized person cannot access personal information. Cryptography is used for protecting data in network channel on the move. Encrypting information in transit helps to secure it from hacker, because it is difficult to physically secure all access to networks. Standards cryptographic software and hardware is used to perform encryption. There are many cryptographic algorithms which are being used to secure data including images and video, but all of them have some advantages and disadvantages. So there is need to develop a strong cryptography algorithm for securing the image and video while transferring. Graphical data is complicated in comparison with other data like text, so the method of securing them will also be complicated.***

Keyword: ***Digital Rights Management (DRM), Data Encryption Standard (DES), elliptic curve cryptography (ECC), Video Object Plane (VOP), cryptography, encryption, decryption.***

I. INTRODUCTION:

Modern era is fully dependent on network. We are using the internet for many purposes. Peoples can also perform various tasks such as bill payment, online shopping and internet banking over a computer network. This implies that the PC network is currently every day terribly helpful for carrying personnel likewise as personal monetary information. Thus, it becomes necessary to secure the network, in order that unauthorized folks cannot access such sensitive data. However we tend to don't seem to be safe in information transfer through the network. Many people have tried to hack our personal or confidential information from the network during transfer of data. They are searching our confidential data in a network. For example if a hacker knows our bank account, user name and password from the network then they can withdraw our money from my account without our permission and information. In network communication there is a lot of security and safety approaches are used during communication.

We can divide video and audio services into three broad categories. That is streaming storing video/audio, streaming live video/audio and interactive video/audio. When we can send multimedia data on the internet, then we need to digitize of multimedia data. The development of multimedia digitization and networking technology has made in many useful applications like telecommunication, internet etc, such as video broadcast, video on demand. According to the Nyquist theorem, if the best frequency of the signal is 'f', we want to sample the signal '2f' times per second. There are unit alternative strategies for digitizing an audio signal however the principle is that the same [1].

II. TECHNICAL REVIEW:

According to M. Abomhara, Omar Zakaria , the rapid development of various multimedia technologies and more multimedia data are generated and transmitted in network for commercial and military purposes. This may include some sensitive information which should not be accessed by unauthorized users. Therefore, security and privacy have become an important for securing data. Over the last few years several encryption algorithms have developed for the purposes of securing video data over the network channels. There are many multimedia and text based cryptography algorithm have been developed for security of multimedia and text data, but every algorithm has some weaknesses. While a large number of new multimedia encryption schemes have been proposed day by day. In this paper, the author discuses four algorithms that are Naive Algorithm, Pure Permutation Algorithm, Zig-Zag Permutation Algorithm and Video Encryption Algorithm. The encryption algorithms for video are working in the compressed domain. A description and comparison between encryption methods and representative video algorithms were presented. The Author had achieved efficiency, flexibility and security through this algorithm [2]. To construct a public key cryptosystem, it is essential to seek out a unidirectional trap-door operate. This is also focus by the author in propose of a new one-way trapdoor function, and presents the corresponding encrypt - system and entity authentication scheme. Author use hyperbolic function for encryption and decryption method. This process is more secure under the condition of the nearly similar

efficiency. The Author has proposed a trapdoor one-way function based on the improved hyperbolic functions. This process is more secure and practically implemented [3].

Through is paper, the author concludes following result

(i) Any algebraic polynomials, which have semi-group property of equations (a) and recursion property like equation (b) over the real field may be wanting to construct a trap door unidirectional operate. (ii) The proposed function can be used to construct a public key encryption algorithm, entity authentication, key agreement algorithm and digital signature algorithm [3].

According to Joyshree Nath, Suvadeep Dasgupta, Asoke Nath, Dripto Chatterjee, a new symmetric key cryptographic method for encryption and decryption of any file which contain characters, numbers, and symbols. The Author has developed an algorithm know as DJSA symmetric key algorithm. This algorithm is modified version of the MSA algorithm for encryption and decryption of any file using a random key square matrix containing 256 elements. In MSA algorithm if a hacker wants to hack the key of MSA algorithm then it is not impossible to hack, because now a day it is possible to calculate factorial of 256 (256!). To get rid of this problem here the authors suggest a better algorithm than MSA because MSA has some drawback. The Author has removed drawback of MSA algorithm and develop a new cryptographic algorithm. In the present method the authors considered the size of the key matrix to be 65536 and in each cell Author store 2 character pattern instead of 1 character unlike MSA method. If someone wants to want know the key then hacker must trial a factorial of 65536 (65536!) which is not easily possible now a day. If hacker gives a brute force method to find our actual key then one has to give a trial for factorial 65536!. It is not easily possible in theoretical, this is an intractable problem. Author use 2 dimensional matrix of size 256 by 256 and each calls capacity of 2 character pattern, it means ASCII code 0-255. The total number of words possible is 65536. The user has choose and enter some secret text-key of most key length is sixteen characters long. To calculate the randomization variety and also the variety of coding to be done is calculated from the text-key employing a technique planned by Nath (9). This is suitable for a file of size less than 2MB. If the file size is large then Author suggests choosing small encryption number to speed up the system [4].

According to the Changgui Shi and Bharat Bhargava, multimedia data security that is important for multimedia commerce. There are many cryptographic algorithms for focused on text data. The cryptographic algorithms for secure text message and data are not suitable for images, video and audio data applications because of large data sizes and real time constraint. There are lightweight encryption algorithms are attractive for multimedia applications. The Author presents an efficient MPEG video encryption algorithm. This algorithm author uses the binary secret key of size 'm' bits. It is more difficult to identify the value of the key. There is '2m' possibility for searching key. There is also a facility for randomly changing the sign bits of encoded differential values of DC coefficients of I pictures and a different value for motion vectors of P and B pictures. The encryption effects are achieved by the IDCT during MPEG video decompression processing. This algorithm is very efficiently and fast [5].

These are purposed two experiments:

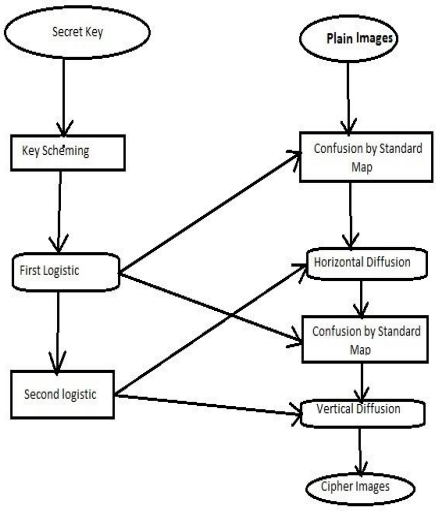
1. To test the encryption results;
2. To find the overheads added to MPEG codes.

These are three kinds of experiments conducted by the author:

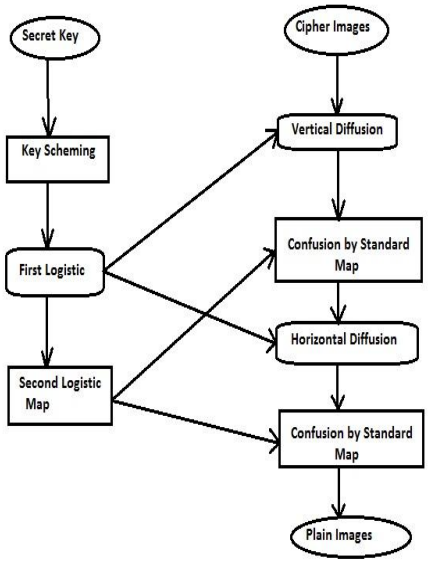
1. Encrypting all motion vectors of B and P frames. The video image is blurred, but still comprehensible.
2. Encrypting all DC coefficients of I frames. The image is obscured, but one can still tell the object motion directions.
3. Encrypting all DC coefficients of I frame and motion vectors of B and P frames. The image is incomprehensible [5].

III. CRYPTOGRAPHY ALGORITHM FOR IMAGES

Encryption of images is somehow different from text encrypted due to some inherent features of the images. Images have bulk information capability feature and the high correlation between pixels, that square measure typically tough to handle like a text message. The exceptionally fascinating properties of the chaotic maps such as sensitivity to initial conditions and random-like behavior have attracted the attention of cryptographers to develop new encryption algorithms. The Author has proposed a new symmetric key cryptography for images. This algorithm use 128 bits of secret key. This algorithm widely used confusingly–diffusion architecture which utilizes the concept of chaotic 2 dimensions (2D) Standard map and 1 dimension (1D) Logistic map. This algorithm is specifically designed for the color images, which are 3D arrays of RGB data stream. This algorithm is specially designed for color images, which is a 3D array of the data stream. Author like a chaotic common place map to Baker and Cat maps as a result of the key area taken from the chaotic Standard map is additional as compared to the Baker and Cat maps that make the brute-force attack impossible. The initial conditions and system parameters of the chaotic maps constitute the secret key of the algorithm. The control parameters used in the confusion stage for further enhancement of the security and in diffusion stage the key stream employed distinct in different rounds and related to the plain-image. The Author had used to tend map for generating variable control parameters for confusion and diffusion rounds. There are two types of diffusion processes that are horizontal and vertical divisions. This algorithm used mixing properties of horizontally and vertically adjacent pixels using a Logistic map, for getting higher security and complexity. Author had gotten results of many experiments, together with the foremost vital ones like key area analysis, key sensitivity take a look at, applied math analysis, and visual take a look at by histograms of encrypted pictures, the correlation coefficients of adjacent pixels, and differential analysis, demonstrate the satisfactory security and potency of projected image coding theme for periodic image coding and transmission [6].



The diagram represents an encryption scheme [6].



The diagram represents Decryption Process [6].

Issues of images: when the cipher text is created, cipher text must be decrypted into original plain text without any loss. However, the cipher images may be decrypted to plain images in some lossy manner because image size is much larger than the text message, so traditional cryptosystems need much time to directly encrypt the image data.

IV. CRYPTOGRAPHY ALGORITHM FOR VIDEO

According to Habib Mir M. Hosseini, Pong Mee Tan, the security issue is very important for video streaming applications. Unauthorized access and duplication of proprietary content is nearly inevitable. Authorized persons and service providers are worried about hacking of digital multimedia content by unauthorized persons. Encryption provides a security to video and image data for transmission over the network. In this paper, the author has proposed a framework for secure MPEG video streaming. This algorithm provides a security of MPEG video data during transferred in network channel. The system will support multiple communication modes [7].

The options of the projected system for secure MPEG video streaming system are as follows:
(1) It supports multiple communication modes like multi-unicast, multicast and broadcast for various application wants.
(2) It might adopt several MPEG video coding algorithms. Through performance analysis, we've complete that these algorithms bring home the an appropriate quality of service and are suitable for various security levels of video and obtainable computing resource.
(3) The object-oriented style strategy facilitates incorporating new MPEG video security algorithm into the system.
(4) It makes use of a secure key management team. We've conjointly introduced a VLC permutation coding rules that are extremely quick rule [7].

In this paper author is highlighted a new symmetric key cryptography algorithm for a video file. The MPEG-4 video streaming service is being regarded as a de facto standard service for current mobile multimedia video streaming services

such as video conferencing, voice over IP, and even progressive digital multimedia system broadcasting technology. There are several illegal users have used proprietary material while not obtaining permission and/or paying for its use. Therefore, abundant attention has been procured DRM for digital media. Author created a protection theme for MPEG-4 video file format, which may be applied, for the video services that area unit exploiting the MPEG-4 customary. During this protection theme, minimum segments of each Video Object Plane in an every MPEG-4 video file may well be encrypted with a symmetric cryptography system like DES, so people that have not received permission and/or paid to use the contents wouldn't be able to read and view them. Author applied this scheme to all kinds of MPEG-4 VOP types that is I-, P- and B vop's severally. The image system was developed for proving the feasibility of this scheme for handheld devices and for VOP , MMS environment [8].

In this research work's author has an emphasis on the development of a novel lossless digital encryption system for multimedia. This system uses the orthogonal transforms for the encryption of all types of multimedia data formats. The Author has used the symmetry properties of the orthogonal transforms to calculate the inverse of the orthogonal matrices during the execution of the decryption process to speed up the operations and reduce the cost of performance. In this paper author has used several classical image encryption approaches such as Discrete Cosine Transform (DCT), Hadamard Transform (HT) as well as Malakooti Transform (MT). The Author has additionally projected, a replacement Malakooti-Raeisi (MR) Key generation formula that may be wanting to inscribe and decode the voice signals by applying the XOR operation over the voice signals and Key information Sequences. The projected Key information formula beside higher than orthogonal transforms are wanting to increase the amount of security in addition because the hardness of formula throughout the image encryption/decryption method. The Author has encrypted/decrypted pictures with solely the M-R Key information values to indicate the power of the formula. This formula incorporates a big selection of applications like real time voice transmission, secure voice chat, and secure video cryptography [10].

Table Mean square Error for DCT, MT and HT [10].

Transform/ MSE	N=32	N=64	N=128
DCT	5.079 E-9	5.640 E-9	6.249 E-9
MT	0	0	5.749 E-17
HT	0	0	0

Table Correlation Coefficient Analysis [12].

Image Name	Vertical Pixels		Horizontal Pixels		Diagonal Pixels	
	Plain Images	Cipher Image	Plain Images	Cipher Image	Plain Images	Cipher Image
Boat	0.9704	0.0015	0.9400	0.0045	0.9223	0.0021
Bridge	0.9275	0.0013	0.9404	0.0016	0.8975	-0.0007
Clock	0.9938	-0.0114	0.9894	-0.0080	0.9840	-0.0116
Elaine	0.9730	-0.0026	0.9757	0.0037	0.9692	-0.0013

According to J. –C. Bajard, L. Imbert Plantard, C. Negre and T, a new multiplication algorithm for the implementation of ECC over the finite extension fields $GF(P^K)$ where P is a prime number greater than 2K. In the context of error correction code Author will assume that P could be a 7-to-10-bit range, and simply notice values for K that satisfy: P> 2K, and for security reasons $\log_2(P) * K \simeq 160$. All the computations are performed inside associate degree alternate polynomial illustration of the sphere components that is directly obtained from the inputs. No conversion step is required. Author describes a formula in terms of matrix operations and imply some properties of the matrices which will be want to improve the look. The projected formula is extremely parallelizable and appears well custom-made to hardware implementation of elliptic curve cryptosystems [11].

Issues in videos: Video data is not directly encrypted or decrypted. First video data is converted into a number of image frames and then cryptography algorithm is applied on individual image frames. DFS, AES, RES are not suitable for video as well as color images.

V. CONCLUSION:

Following conclusions:

1. There is a need of new version of Video Encryption Algorithm (VEA) is developed, which required less computation than the old version and achieve the same encryption results. That algorithm can be used to secure many MPEG video applications.
2. Some algorithm can achieve an acceptable quality of service and suitable for different security level of the video.

3. Some encryption model based on the orthogonal transforms for images. Symmetric encryption method use malakooti Raeisi (M-R) transform algorithm for key generation of DCT, HT and MT.

4. Cryptography algorithm for multimedia (that is images and video) is not so easy. DES, AES, RES are not suitable for color images and video, which are 3D arrays of data.

5. Chaotic maps, tent map, standard map, logistic map and Baker and Cat map techniques are used for multimedia cryptography. A lossless digital encryption system for multimedia used orthogonal transforms matrix and XOR operations are used for the improved cryptography algorithm. Naive Algorithm, Pure Permutation Algorithm, Zig-Zag Permutation Algorithm and Video Encryption Algorithm are also used for cryptography techniques.

REFERENCES :

[1] TCP/IP Protocol Suite 4th Edition Behrouz A. Forouzan.

[2] An Overview of Video Encryption Techniques, M. Abomhara, Omar Zakaria, Othman International Journal of Computer Theory and Engineering, Vol. 2, No. 1 February, 2010 1793-8201

[3] A Public-key Cryptography and Entity Authentication Scheme Based on Improved Hyperbolic Function Dahu Wang, Heyuan Bai, Qunpo Liu, Zhaojing Tong School of Electrical Engineering & automation, Henan Polytechnic University, Jiaozuo Henan, China 978-1-4244-2013-1/2008 IEEE.

[4] A new Symmetric Key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm Dripto Chatterjee, Joyshree Nath, Suvadeep Dasgupta, Asoke Nath Department of Computer Science St. Xavier's College (Autonomous), Kolkata Kolkata, India.978-07695-4437-3/11 2011 IEEE

[5] An Efficient MPEG Video Encryption Algorithm Changgui Shi and Bharat Bhargava Department of Computer Sciences Purdue University West Lafayette, IN 47906, USA.

[6] Color Image Cryptosystem using Chaotic Maps Sahar Mazloom, Amir-Masud Eftekhari –Moghadam Faculty of Electrical, Computer and IT Engineering, 978-1- 4244-9915-1/2011 IEEE

[7] Encryption of MPEG Video Streams Habib Mir M. Hosseini, Pong Mee Tan School of Electrical and Electronic Engineering, Nanyang Technological University Singapore 639798 1-4244-0549-1/2006 IEEE.

[8] Intellectual Property Management on MPEG-4 Video for Hand-Held Device and Mobile Video Streaming Service Gunhee Kim, Dongkyoo Shin, IEEE, and Dongil Shin 0098 3063/2005 IEEE

[9] Symmetric key cryptography using random gnerator, A. Nath, S.S. Ghosh, M.A Mallik Proceedings of International conference on SAM -2010 held at Las Vegas(USA) 12-15 July,2010, Vol-2,P 239-244.

[10] A Lossless Digital Encryption System for Multimedia Using Orthogonal Transforms Dr. Mohammad V. Malakooti, Mojtaba Raeisi Nejad Dobun 978-1-4673-0734-5 2012 IEEE

[11] Efficient Multiplication in GF(P^K) for Elliptic Curve Cryptography J.-C.Bajard, L. Imbert, C. Negre and T. Plantard Laboratoire d'Informatique de Robotique et de Microelectronique de Montpellier LIRMM, 161 rue Ada, 34392Montpellier cedex 5-France proceedings Of 16th IEEE Symposium on Computer Arithmetic, (ARITH'03).

[12] Confusion and Diffusion of Grayscale Images Using Multiple Chaotic Maps Sukalyam Som, Atanu Kotal Department of Computer Science Barrackpore Rastraguru Surendranath College and Techno India College of Technology respectively Kolkata, W.B., India, 978-1-4673-1953-9/2012 IEEE

