ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Designing of Energy Efficient Security Techniques for Multimedia Applications

Anshula Bardak[*1], Sunita Sangwan[2], Darshana Hooda[3]

[*1] Depatment of CSE, P.G. Student, P.D.M. College of Engineering, Bahadurgarh, Maharshi Dayanand University, Rohtak 120001, India

[2] Assistant Prof. in Computer Science Dept., P.D.M. College of Engineering, Bahadurgarh, Haryana 124507, India

[3] System Analyst and Head UCC, Deenbandhu Chhotu Ram University of Science & Technology, Murthal-131039 India

anshula30@yahoo.com

Abstract

In current scenario due to convenience and technological advancement more and more users and businesses use smart phones as effective communication tool to discuss their business plans/activities or to share personal matters/affairs. All users have the right to maintain their privacy and confidentiality of communication, while it is travelling over communication channels. To boost faith of users in technology enhanced communication tools security mechanisms were evolved to protect the information from unauthorized access. Since the 1990s a lot of research efforts have been made for the development of specific video encryption algorithm keeping in the view peculiar requirements of video services. This paper presents the overview of existing video encryption algorithms.

Keywords: Security Techniques.

Introduction

This 21st century is known as the age of Information where information has become important strategic resource. In this digital era, nearly all the govt. agencies, companies, educational institutes and home users depend on computer systems and communication systems. Evolution of digital advancement have lead towards new information sources, which were not so common and conveniently available as now, used to present/carry the information in past like video/images. Video data shows more authenticity rather than conventional text information, so today it is considered as an important source/media to carry information. Furthermore, today handheld devices are pervasive as they allow users to carry computational power in their hands. The technical report, June, 2013 released by Cisco systems says that number of users with mobile devices is expected to rise to 5.2 billion in 2017 from 4.3 million in 2012. Further, it states that smartphones, laptops and tablets will drive 93% of global mobile data traffic by 2017. Today, 66% of global mobile data traffic is mobile video traffic pertaining to different multimedia services like video chatting, video conferencing, and entertainment services. These statistical figures speak volume about video consumption through mobile devices i.e. constrained devices in terms of computing resources and battery power. In current scenario due to convenience and technological advancement more and more users and businesses use smart phones as effective communication tool to discuss their business plans/activities or to share personal matters/affairs. All users have the right to maintain their privacy and confidentiality of communication, while it is travelling over communication channels. To boost faith of users in technology enhanced communication tools security mechanisms were evolved to protect the information from unauthorized access. Cryptology is the fool proof technology to offer secure communication, but in current scenario heterogeneity in communication technology and limited capabilities of accessing devices pose new challenges. Since the 1990s a lot of research efforts have been made for the development of specific video encryption algorithm keeping in the view peculiar requirements of video services. Today, energy consumption by encryption algorithm is major concern because of the critical limitation of battery power of constrained devices. Battery power is critical limitation than processor speed /memory as memory and processor technologies doubles with the introduction of every new semiconductor

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

advancement. Users of the hand-held devices generally have complaints about the battery life of the device. Optimizing the energy efficiency of mobile application can increase battery life span. Therefore, power efficient encryption techniques are critical need of time keeping in view the exponential growth in wireless technologies and hand held devices. Some of the paper presents lightweight cryptographic techniques.

Literature Survey

Video encryption techniques are specifically designed to meet real time processing need and perceptual encryption, not required for text encryption. Today's major challenge is how to protect the multimedia content over network. To meet the said requirement two major multimedia security technologies are being developed:

(1) Multimedia encryption techniques
(2) Multimedia Watermarking technology

Encrypting the entire multimedia stream using standard encryption method is known as naïve approach. In the naive approach for video encryption, the MPEG stream (bit sequence) is treated as text data, and encrypted using standard encryption algorithms like DES (Data Encryption Standard) [2], RC5 (Rivest Cipher), AES (Advanced Encryption Standard), etc. Though this approach is supposedly the most secure for video encryption, it is computationally infeasible for real-time applications. Arguing that the full content of the video is not critical, selective encryption algorithms were proposed [2, 3, 4].

Secure MPEG was the first selective encryption method ,in this DES was used to achieve confidentiality and to achieve problem of data integrity CRC was incorporated[5]

These methods encrypt a selected portion of the video data (for example headers of the video streams, I frames and I-blocks in P and B frames, I frames and motion vectors in P and B frames, etc.) using text-based encryption algorithms. This decreases encryption time. For real-time applications, light-weight encryption algorithms were also proposed [5, 6, 7]. These methods encrypt using simple XOR or encrypt selected bits of the video data (for example, sign bits of I frames, motion vectors, etc.). These encryption algorithms are much faster than selective algorithms. Also, they add less overhead on the codec. (Note that if encryption modifies the syntax of the MPEG bit stream, it adds overhead to the MPEG codecs.) Another category of algorithms is video scrambling.

Video scrambling is popular method of applying fast yet very insecure distortion of signal. Solution was good for cable companies to make the free viewing of paid cable channels more difficult than doing nothing. Early work was based on analog devices.This was done by applying filter banks or frequency converters to permute the signal in the time domain or distort the signal in the frequency[8] .These schemes seriously lake security.

However, in most of these methods, computational efficiency comes at the cost of security. Maples and Spanos [8, 9] proposed a selective encryption algorithm called AEGIS. Using the DES algorithm, the AEGIS algorithm encrypts only the I frames of the MPEG video stream. However, Agi and Gong [10] showed that partial information leakage from the I-blocks in P and B frames renders AEGIS unsuitable for applications like military where each and every part of the video data is important. Qiao and Nahrstedt [4] proposed another selective Video Encryption Algorithm (VEA). In this algorithm, a chunk of I frame is divided into two halves. Both the halves are XORed and stored in one half. The other half is then encrypted using DES. The VEA provides good security and reduces the number of XOR operations significantly compared to AEGIS. These selective encryption algorithms are secure, but they are not practical for real-time implementations because they require high computational time. Choon [6] proposed a light-weight and cost effective encryption algorithm based on the Shannon principle of diffusion and confusion. These principles can be achieved by permutation of macro blocks followed by XOR operation on the permuted macro block. Choo [5] proposed another light-weight encryption algorithm on the uncompressed raw MPEG data named Secure Real-time Media Transmission (SRMT), which uses two block transpositions and a XOR operation. Tang [11] proposed a scramble based encryption algorithm using permutation of the DCT coefficients.

The basic idea is to use a random permutation list to replace the zig-zag order of the DCT coefficients of a block to a 1 × 64 vector. Zeng and Lie [12] extended Tang's permutation range from a block to a segment, where each segment consists of several macroblocks. Within each segment, the DCT coefficients of the same frequency band are randomly shuffled within the same band. Apart from shuffling of the I frames, they also permute the motion vectors of P and B frames. a computationally efficient, yet secure video encryption scheme using RC5 for encryption of the DCT coefficients[13].

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

However, light-weight encryption and scramble-only methods provide less security than the naïve encryption. The drawback of these algorithms is that they trade-off security for speed.

Fuhrt and Kirovski(2004) has given detailed overview of early video encryption algorithms. Fuwen Liu and Harmut (2010) classified encryption algorithms according to their association with video compression. They have also evaluated performance of video encryption algorithms taking in to consideration the various performance parameters like: encryption efficiency, compression efficiency, security offered, video codec compliance etc. Even though different classifications of video encryption are extensively presented, we analyze existing encryption algorithms according to their association with compression and amount of data to be encrypted duly taking into consideration strength and weakness of each approach. According to the amount of video data selected for encryption, video encryption can be classified in to the following three categories: Naïve, Scrambling and Selective.

In Naïve approach whole video data is encrypted using a symmetric key cryptosystem. However, even the fastest modern symmetric schemes such as DES or AES are computationally very expensive and not well suited for video data encryption, due to the need of processing, large volume of data in real time. However these techniques offer the highest level of security but practical implementation of such techniques is limited due to their time and space complexity [9,10].

Under scrambling techniques, no data is selected for encryption; only different permutations are performed to disguise the video. Video Scrambling offers fast, yet very insecure distortion of the video data. This technique mainly evolved due to the industrial need of protecting the viewers from free viewing of paid cable channel. Signal scrambling was based on using an analog device to permute the signal in the time domain or distort the signal in the frequency domain by applying filter banks or frequency converters [9,13]. However, these schemes are easy to break and hence not suitable for sensitive applications.

The above mentioned limitations of Naïve and Scrambling techniques triggered a different mainstream approach that exploits video encoding characteristics of data, popularly known as selective encryption techniques. Selective encryption techniques encrypt the selected portion of video stream rather than whole video stream [11,12]. In selective encryption, efficiency of encryption highly depends on selection of most effective portion of video stream for encryption as variables obtained at different stages during encoding process exhibits different importance levels over video content presentation [14]. One main challenge in selective encryption algorithm is to design a secure technique, which exhibits error resiliency property. Generally, standard ciphers have strong avalanche effect; hence they offer poor error tolerance [15]. Selective algorithms generally conventional encryption algorithm during the encryption step [16].

Further, according to the association of encryption techniques with the compression; they can be classified as: pre compression, in compression and after compression. As the names indicate in pre compression encryption takes place prior to the compression process i.e. independently. This approach meets the highly desirable requirements of robust video security technique like codec independency and format compliance hence this category encryption has potential for future. While as in-compression encryption techniques are codec dependent designs and problem with post compression techniques are syntax compliance. Both in-compression and post compression have strong avalanche effects hence highly unsuitable for error prone transmission environment i.e. wireless networks. Further Daniel etc. clearly states that encryption techniques that work before compression at the encoder side, and after decompression at the decoder side, a unique and desirable feature [16].

Now days, novel multimedia specific type encryptions are emerging and termed as non-conventional encryption-based approach. For example, approaches like Huffman table permutations, chaotic map-based, Hopfield neural network based multimedia encryption all belong to this class. Encryption framework defined by D.Hooda et all is highly energy efficient approach based on RRP concept. RRP is good choice for the digital video data encryption as digital video data has high redundancy over short range [1].

Shujun Li et all present a security analysis of techniques based on secret Huffman tables. They have carried out cryptanalysis of an MPEG-video encryption scheme based on secret Huffman tables. Their cryptanalysis work concludes that, firstly, the key space of the encryption scheme is not sufficiently secure against divide-and-conquer (DAC) cipher text-only attack; and secondly its security against the chosen-plaintext attack is very weak. The insecurity is mainly due to the separated use of different Huffman tables for different sets of syntax elements [17,18].

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

In today's scenario, server and client systems both fed the need of energy efficient techniques, as, though servers are high end/powerful systems but demand lots of inherent concurrency to serve millions of demands. On the other hand, client systems do not need concurrency but generally have limited resources in terms of processing speed, battery power or memory. Hence, there is a critical need to adopt energy optimization approaches while designing the software solutions. Fast & real time processing needs of cryptographic techniques have motivated hardware implementation of cryptographic techniques and light-weight cryptographic techniques. Many security chips/secure network interface cards architecture are suggested in literature and security boxes that include implementation of symmetric ciphers are commercially available and are in use. Hardware implementation of remote referencing passing is presented by integrating PROM based security module with network interface card that enables on the fly security with flexibility for algorithm change at short notice. The limitation of this approach is its network dependency. The lightweight cryptographic techniques offer good speed but on cost of security [19].

Parallel Multi-Key Encryption by Alexander Wong et al presents an efficient parallel video encryption algorithm suitable for consumer devices [20].

In recent years, a lot of attention has been devoted towards development of video encryption based on chaos theory. Chaos based cryptography is falls under modern cryptography techniques. The features which make it advantageous over conversational cryptographic techniques are: ease of generation, sensitive dependencies on seed, and non-periodicity. These are the major reasons that in recent much attention has been devoted to the usage of chaos theory to implement encryption technology. Moreover, chaotic signal generation is a low cost affair; hence it is most suitable technique for the encryption of large bulky data [21, 22, 23, 24, 25, 26, 27]. A detailed survey on image, video and multimedia encryptions based on chaos theory is presented by Zhaopin [28] and Su [35].

Various multimedia encryptions have been developed so for due to recognized potential benefits of chaotic encryption [29, 30, 31, 32, 33, 34]. Chaos based image encryption are broadly classified into two categories: full encryption and partial encryption as per data encrypted. Moreover, with respect to the encryption process they are classified as Block encryption or Stream Cipher. Their association with compression categories them compression combined and compression independent.

This research work is inclined towards video encryption; therefore the study of some of video encryption is carried out to understand working principles of chaos based video encryptions. So far, many chaos based video encryption methods have been proposed, however, practical acceptances of these are still not realized. According to the relation between compression and encryption, these may classified in to three types: raw video data encryption, encryption with compression and compressed video data encryption. Encryption with compression process means realizing encryption in the encoding process before the entropy coding. Compressed video data encryption here means realizing encryption after the entropy coding.

Li et al described a chaotic video encryption scheme for real time digital video based on multiple digital chaotic systems. Under this scheme. each plain block is XORed by a chaotic signal, and then substituted by a pseudo random S-box based on chaotic map [31].

Ganesan proposed a public key video encryption based on chaotic maps [35]. In PKVE, when number of frames is large then first, they use phase scrambling [36] and the encrypt the data using Chebyshev maps [37]. Otherwise, each frame is encrypted using Arnold scrambling [38].

Kezia et al propose a scheme where each frame of video is encrypted by confusing the position of pixel using a high dimensional Lorenz chaotic system. In this scheme, a unique key is used to encrypt each frame instead of changing the key for a particular number of frames [39].

Some of selective video encryption schemes based on chaotic theory are also proposed. A human video object encryption system based on logistic map is proposed by Tzouveli. In this scheme, firstly, face regions are detected and afterwards body regions are extracted using geometric information of the location of the face regions. These extracted/detected human video objects are encrypted using logistic map [86]. Ntalianis et al proposed a video object based encryption scheme which works on automatic extraction of video object with the help of appropriate color segment fusion approach. Afterwards, for each video object multi resolution decomposition is performed and the lowest resolution pixels are encrypted using a chaotic cipher module. Finally, encrypted regions are propagated towards higher resolution levels and the encryption process is repeated until the highest resolution level is reached [40].

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

Encryption of the video data in compression process takes place during the encoding process, before the entropy coding like Context adaptive variable length coding, Context adaptive binary arithmetic coding, variable length coding, run length coding, Golomb, and Huffman etc. Yang et al [50] proposed a chaos based video encryption in DCT domain, where I-frames are selected as encryption objects. Firstly, DCT coefficients of I frames are scrambled using double coupling logistic maps, then by using another logistic map DCT coefficients are encrypted. In this, five keys are used, which makes this secure against brute force attack.

Lian proposed an efficient chaos based encryption for image/video based on encryption of only DC(Direct current) coefficient and signs of AC(Alternate current) coefficient of each frame. The encryption takes place after the color space transformation (pre-encoding), block portioning, DCT transformation and quantization, and before zig-zag scan and VLC (post –encode) [42].

Chaos based encryption for compressed video data is proposed by Lian (2007) and Qian(2008). Lian proposed chaos based encryption, where intra macro blocks and motion vectors are encrypted using discrete piecewise linear chaotic map. Encryption process is carried out after VLC and before packaging [52, 53]. A fast chaos based encryption under same domain for MPEG-4. In this scheme file format information like file header, packet header, and so on, are left unencrypted in order to support bit rate control. Motion vectors, sub-bands, code blocks or bit planes are partially encrypted by a stream cipher based on a modified chaotic neural network [51].

Qian proposed a multiple chaotic encryption system for MPEG-2 video. In this scheme for stream partial encryptions, block permutation and confusion after block permutation, three chaotic maps are defined named as logistic map, 2-D baker map and 4-D hyperchaotic map, respectively [54].

In today's scenario, servers and clients both fed the need of energy efficient techniques, as , though servers are high end/powerful systems, but require lots of inherent concurrency to serve millions of demands. On the other hand, client system do not need concurrency but generally have limited resources in terms of processing speed, battery power or memory. Hence, there is a critical need to adopt energy optimization approaches while designing the software solutions. Present research work presents an energy efficient approach to offer security to digital video applications. Fast & real time processing need of cryptographic techniques has motivated towards hardware implementation of cryptographic techniques. Many security chips and secure network interface cards architecture are suggested in literature and security boxes that include implementation of symmetric ciphers are commercially available and are in use. Hardware implementation of remote referencing passing is presented by integrating PROM based security module with network interface card that enables on the fly security with flexibility for algorithm change at short notice. The limitation of this approach is its network dependency [20].

Conclusion

Based on the state of the art in video encryption, we observe that:

• For complete and provable security of the video data, the entire video needs to be encrypted. However, a naive encryption of the complete video stream is computationally infeasible.

• The encryption algorithm should not be susceptible to attacks like known-plaintext attack and cipher text-only attack. Computational efficiency should not come at the cost of security.

Encryption techniques are good enough to address for main issues of multimedia security:

Confidentiality

Authentication

Copy right protection

Lots of efforts in recent years has been to developing technology to enable users to enjoy/use multimedia services anywhere, anytime, and with any device using any type of network and security needs. Popularity of video consumption through constrained devices are on rise but better power of constrained devices are major limitation. Today energy consumption by encryption algorithm is major concern because of the critical limitation of battery power of constrained devices. Battery power is critical limitation as memory and processor technologies double with the introduction of every new semiconductor advancement . In current scenario, there is need to develop power efficient cryptographic technique to address security needs of multimedia application, keeping in the view heavy load on video servers and limited resources capabilities of client devices. Therefore designing of a security technique to reduce the consumption of power during the encryption/decryption process both is critical need.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

References

[1] *Darshana Hooda and Parvinder Singh; Self Adjustable Security Technique Based on Remote Reference Passing for Digital Multimedia Services; CSI Transaction on ICT, CSIT (June 2013), 1(2):116-125, Springer.*

[2] *William Stalling, Network Security , PHI publication*

[3] *T. B. Maples and G. A. Spanos. Performance Study of a Selective Encryption Scheme for the Security of Networked, Real-Time Video. In Proc. of Fourth International Workshop on Multimedia Software Development '96), 1995*

[4] *L. Qiao and K. Nahrstedt. A new algorithm for MPEG video encryption. In Proc. of First International Conference on Imaging Science System and Technology, pages 21–29, 1997*

[5] *E. Choo, L. Jehyun, L. Heejo, and N. Giwon. SRMT: A lightweight encryption scheme for secure real-time multimedia transmission. In Multimedia and Ubiquitous Engineering, pages 60–65, 2007.*

[6] *L. S. Choon, A. Samsudin, and R. Budiarto. Lightweight and cost-effective MPEG video encryption. In Proc. of Information and Communication Technologies: From Theory to Applications, pages 525–526, 2004.*

[7] *W. Zeng and S. Lei. Efficient frequency domain selective scrambling of digital video. In Proc. of the IEEE Transactions on Multimedia, pages 118–129, 2002*

[8] *T. B. Maples and G. A. Spanos. Performance Study of a Selective Encryption Scheme for the Security of Networked, Real-Time Video. In Proc. of Fourth International Workshop on Multimedia Software Development '96), 1995*

[9] *G.A. Spanos and T.B. Maples, "Security for Real-Time MPEG Compressed Video in Distributed Multimedia Applications," in Conference on Computers and Communications, 1996, pp. 72-78.*

[10] *I. Agi and L. Gong. An empirical study of MPEG video transmission. In Proc. of the Internet Society Symposium on Network and Distributed Systems Security, pages 137–144, 1996.*

[11] *L. Tang. Methods for encrypting and decrypting MPEG video data efficiently. In Proc. of ACM Multimedia, pages 219–229, 1996*

[12] *W. Zeng and S. Lei. Efficient frequency domain selective scrambling of digital video. In Proc. of the IEEE Transactions on Multimedia, pages 118–129, 2002.*

[13] *A. Biryukov and E. Kushilevitz. Improved cryptanalysis of RC5. Lecture Notes in Computer Science, 1403:85–100, 1998.*

[14] *Z. Chen, Z. Xiong, and L. Tang. A novel scrambling scheme for digital video encryption. In Proc. of Pacific-Rim Symposium on Image and Video Technology (PSIVT), pages 997–1006, 2006.*

[15] *W. Zeng and S. Lei. Efficient frequency domain selective scrambling of digital video. In Proc. of the IEEE Transactions on Multimedia, pages 118–129, 2002.*

[16] *A. Massoudi, F. Lefebvre, C. De Vleeschouwer, B. Macq, and J.-J. Quisquater, Overview on Selective Encryption of Image and Video: Challenges and Perspectives. EURASIP Journal on Information Security Volume 2008.*

[17] *Shujun Li, Guanrong Chen, Albert Cheung, Kwok-Tung Lo, Mohan Kankanhalli, On the Security of an MPEG-Video Encryption Scheme Based on Secret Huffman Tables.*

[18] *J. Zhou, Z. Liang, Y. Chen, and O. C. Au, "Security analysis of multimedia encryption schemes based on multiple Hu.man table," IEEE Signal Processing Letters, vol. 14, no. 3, pp. 201–204, 2007.*

[19] *Thomas Eisenbarth, Christof Paar and Axel Poschmann,Sandeep Kumar,Leif Ushadel.A survey of Lightweight-Cryptography Implementations. Design and test of ICs for Secure Embedded Computing(IEEE Design & Test of Computers)(2007) .*

[20] ***Alexander Wong** and William Bishop, An Efficient, Parallel Multi-Key Encryption of Compressed Video Streams, in the proceedings of the IASTED International Conference on Signal and Image Processing, Honolulu, Hawaii, August 2006*

[21] *K. T. Alligood, T. Sauer , J. A. Yorke, Chaos : An Introduction to Dynamic Systems, Springer Verlag, New York, 1997.*

[22] *T. Yang , C. W. Wu, L. O. Chua , Cryptography Based on Chaotic Systems, IEEE Transactions on Circuits and Systems : Fundamental Theory and Applications, Vol 5(44),469-472, 1997.*

[23] *G. Alvarez, S. Li, Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems, International Journal of*

Bifurcation and Chaos Vol. 16(7):2129-2151, 2006.

[24]G. Alvarez, F. Montoya, M. Romera, G. Pastor, Breaking two secure communication systems based on chaotic masking, IEEE Transaction on Circuit and Systems II: Express Briefs, Vol.51(10):505-506, 2004.

[25]R. L. Devaney, An Introduction to Chaotic Dynamical Systems (2nd edition), Westview Press, San Francisco, 2003.

[26]J. He, H. Qian, Y. Zhou, Z. Li , Cryptanalysis and Improvement of a Block Cipher Based on Multiple Chaotic Systems, Mathematical Problems in Engineering, Vol. 2010: 14pages, 2010.

[27]E. Solak , Cryptanalysis of Observer Based Discrete-Time Chaotic Encryption Scheme, International Journal of Bifurcation Chaos, Vol. 2 (15): 653-658, 2005.

[28]Su Zhaopin, Guofu Zhang and Jianguo Jiang, Multimedia Security: A Survey of Chaos – Based Encryption Technology, www.intechopen.com .

[29]G. Chen , Y. Mao , C. K. Chui , A Symmetric Image Encryption Scheme based on 3D Chaotic Cat Maps, Chaos, Solitons & Fractals Vol.2(3):749-761,2004.

[30]H. Gao, Y. Zhang, S. Liang, D. Li , A New Chaotic Algorithm for Image Encryption, Chaos, Solitons & Fractals Vol.29 (2): 393-399, 2006.

[31]S. Li, X. Zheng, X. Mou, Y. Cai , Chaotic Encryption Scheme for Real-Time Digital Video, Proceedings of SPIE, SPIE Press, San Jose, CA,149-160, 2002.

[32]S. Lian, Efficient Image or Video Encryption based on Spatiotemporal Chaos System, Chaos, Solitons & Fractals Vol.40(5):2509-2519, 2009

[33]Z. Su, J. Jiang, S. Lian, Hierarchical Selective Encryption for G.729 Speech based on Bit Sensitivity, Journal of Internet Technology Vol.5 (11): 599-607, 2010.

[34]Y. Wang, K. W. Wong, X. Liao, G. Chen, A New Chaos – Based Fast Image Encryption Algorithm, Applied Soft Computing Vol. 11 (1): 514-522, 2011.

[35]K. Ganesan, I Singh, M. Narain, Public Key Encryption of Images & Video in Real Time using Chebyshev Maps, Proceedings: Fifth International Conference on Computer Graphics, Imaging and Visualization, IEEE Computer Society, Washington DC,USA, 211-216, 2008.

[36]N. K. Nishchal, J. Joseph, K. Singh, Fully Phase Based Encryption using Fractional Fourier Transform, Optical Engineering, Vol. 42:1583-1588,2003.

[37]P. Bergamo, P. D'Arco, A. Santis, L. Kocarev, Security of Public Key Cryptosystems based on Chebyshev Polynomials, IEEE Transaction on Circuits and Systems –I, Vol. 52: 1382-1393

[38]V. V. R. Prasad, R. Kurupati, Secure Image Watermarking in Frequency Domain using Arnold Scrambling and Filtering, Advances in Computational Sciences and Technology , Vol. 3(2): 236:244

[39]H. Kezia, G. F. Sudha, Encryption of Digital Video based on Lorenz Chaotic Maps with Finite Precision Representation, Chaos, Solitons & Fractals, Vol. 32(4):1518-1529

[40]P. Tzouveli, K. Ntalianis, S. Kollias, Security of Human Video Object by Incorporating a Chaos-based Feedback Cryptographic Scheme, Proceedings of MULTIMEDIA'04, ACM Press, New York, 10-16, 2004.

[41]K. S. Ntalianis, S. D. Kollias, Chaotic Video Objects Encryption Based on Mixed Feedback, Multi resolution Decomposition and Time-Variant S-boxes, Proceeding: ICIP (2) 2005, IEEE press, Genoa, Italy,1110-1113,2005

[42]S. Lian, J. Sun, G. Liu , Z. Wang, Efficient Video Encryption Schemes Based on Advanced Video Coding, Multimedia Tools Applications, Vol 38(1):75-89, 2009.

[43]C. Li, S. Li, G. Chen, W. A. Halang, Cryptanalysis of an Image Encryption Scheme based on a Compound Chaotic Sequence, Image and Vision Computing Vol.27(8):1035-1039, 2009.

[44]Z. Su, G. Zhang, J. Jiang, Chaos Based Video Encryption Algorithms, Springer Verlag, New York, 2011.

[45]C Cokal, Solak, E,(2009). Cryptanalysis of a Chaos-based Image Encryption Algorithm, Physics Letter A, Vol.373(15):1357-1360

[46]J. Fridrich, Image Encryption based on Chaotic Maps, Proceedings of IEEE Conf. on Systems, Man and Cybernetics, IEEE press, Florida, USA,1105-1110, 1997.

[47]Z Guan, F Huang, W. Guan, Chaos-based image encryption algorithm,, Physics. Letters A Vol.346(No.1-3):153-157, 2005.

[48]Y. Mao, G. Chen, S. Lian, A novel fast image encryption scheme based on the 3d

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

chaotic baker map, Int Bifurcat Chaos Vol.14 (No10):3613-3624, 2004.

[49]S. Lian, Z. Liu, Z. Ren, H Wang, Secure Media Distribution Scheme based on Chaotic Neural Network, Proceedings of ISNN 2007, IEEE Computational Intelligence Society, Nanjing, China, 79-87, 2007.

[50]S. Yang, S. Sun, A Video Encryption Method based on Chaotic Maps in DCT Domain, Progress in Natural Science Vol. 18 (10): 1299-1304, 2008.

[51]S. Lian, J Sun, Z. Wang, A Block Cipher based on a Suitable use of Chaotic Standard Map, Chaos, Solitons & Fractals Vol.26(1): 117-129, 2005

[52]S. Lian, J. Sun, Z. Wang, Security Analysis of a Chaos-based Image Encryption Algorithm, Physics Letter , Vol.351 (2-4):645-661, 2005.

[53]Lian, S, Sun, J, Z. Wang, A Chaotic Stream Cipher and the Usage in Video Protection, Chaos, Solitons & Fractals Vol.34 (1): 851-859, 2007.

[54]Q. Qian, Z. Chen, Z. Yuan, Video Compression and Encryption based on Multiple Chaotic System, 3rd International Conference on Innovation Computing Information and Control, IEEE Computer Society, Washington, DC, USA, pp. 561-564, 2008.

[55]M Salleh, S. Ibrahim, I.F. Isnin, Image Encryption Algorithm based on Chaotic Mapping, Journal of Technology Vol.39 (D): 1-12, 2003.