IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 3, Ver. VI (May – Jun. 2015), PP 44-51
www.iosrjournals.org

A New Approach for Video Encryption Based on Modified AES Algorithm

Asst. Prof: Dr. Salim Ali Abaas[1,] Ahmed Kareem Shibeeb[2]
Dept. of Computer Science, College of Education, Al-MustansiryaUniversity, Baghdad, Iraq

Abstract: *The securityof videoapplications such as commercial videos, military videos and othershave become an important field of research recently. One of the most secure algorithms is Advanced Encryption Standard (AES) algorithm;however this algorithm is inefficient for dealing with video encryption due to its slowness property. This paper proposes a new modifiedof AES to make it more suitable for encrypting digital video. The Modification focuses on the slowest transformations in original AES which is mix columnstransformationsand replace them with newHenon map chaoticbased mask and one mix columns transformation. Resulting in a significant reduction in encryption and decryption time and enhance the security level of AES algorithm, and also the key space is increased as observed in the simulation results of proposed system.*

Keywords*: AES-128, Chaotic mask, Henon map, Sub-Byte, Mix columns.*

I. Introduction

1.1 Background

With the rapid progress of Digital Communication Technologythe security of digital image/video plays a significant role in computing technology. Recently, the main considerationin data storage and transmission is theinformation security [1]. An increasing amount and security sensitivity of the information, such as audio, images, video and other multimedia applications make it requires quick and safe ways to achieve its security [2]. There are many approaches for the information security which include steganography and cryptology. The block ciphers have played a vital role inthe science of cryptography when the Data Encryption Standard algorithm (DES) has been introduced. The small block size and short key problemsof the DES algorithm make it more vulnerable to Differential Cryptanalysis (DC) and Linear Cryptanalysis (LC), in addition to security problems, the DES algorithm is slow encryption algorithm. The Advanced Encryption Standard algorithm (AES) is new encryption standard instead of DES algorithm according to the viewpoint of National Institute of Standards and Technology(NIST).The advanced encryption standard algorithm provides multiple keys lengths(128 bits, 192 bits and 256 bits) on the contrary of the data encryption algorithmwhich provides short key length (56 bits), as well as the AES Very powerful against all known attacks and faster than DES algorithm.Although the accepted speed of AES algorithm, but it is not efficient to encrypt digital video due to the large size of the video compared to other multimedia applications [3].So,this paper proposes an appropriate modification for original AES-128 to make it more suitable for digital video encryption.Modification will focus on the mix columns step to modify it with new chaos based matrix to reduce the time of encryption and decryption processes, and at the same time provide high diffusion and confusion in the proposed algorithm.

1.2 Literature Review

Several attempts have been made in the literature towardAES algorithm enhancement andmultimedia encryption. Hephzibah and Gnanou [4] introduce a chaos-based video encryption based on the Lorenz system, when the plainvideo was divided into frames, then checked whether the frame was a large size, it will get macro-blocks from theframefor encryptingit. And take advantage of the Lorenz system properties for the purpose of frame'spixels confusion. As observed in [4], the proposed system is fast and insecure.

S.Kamali et al.[5] introducea new modified for AES algorithmto decreased the pattern appearance and to encrypt square image onlyby adjusting the shift rows step based on the first cell value of the state array , if its value is odd, thenthe first and third rows are remaining in an original state, whereas the second and fourth rows are shifted one and three bytes to the left, respectively.Meantime, if its value is even, then the first and fourth rows are unchanged, while the second and third rows are shifted three and two bytes to the right, respectively. Likewise, the proposed method in [6], ituses the same of previous method to reduce the calculation of the video encryption completely. This modification is a quick somewhat, but not enough for encryptingvideo. In [7], divide the plain image into blocks then reordering of the block's pixels is performed by changing the positions of pixels. Finally, these blocks are passed randomly to AES algorithm. This method used to decrease the correlation between plain image and cipher image and disregards the increase in encryption time.However, three modifications on AES algorithm is proposed by S.Wadi and N.Zaina to make it more suitable for encrypting HD imagesby increasing AES security and reducing its computation cost and hardware requirement through, using the mix columns transformation as additionaltransformation in key schedule operation to enhance the security level, reducing the mixcolumns step in AES-128 bits to five instead of ten to reduce the encryption time and constructing simple and one S-boxfor encryption and decryption processes to reduce the requirement of hardware. The first modification increases the security level and requires more time for the encryption process.On the contrary, the second modification which provides less encryptiontime and low security level than original AES, while the third modification reduces the security level of AES as a result of the low nonlinearity of new S-box as obtained in [8].

II. Advanced Encryption Standard Algorithm Specification

The AESis designed to agree with principles of Substitution-Permutation Network mechanism. Thus it involves some of operations during the encryption and decryption; these operations take 4×4 matrix called the state which represents 16 byte of data as input. There are four basic operations used over the encryption process to encrypt the plain text which are:Substitution byteby using the Substitution Box (S-box), Shifting Rows, Mixing Columns and XOR'ing with Round Key.However, at the decryption process the inverse of previous steps will be used to decrypt original data which are: InvSubBytes, InvShiftRows and InvMix-Columns in addition to AddRoundKey transformation . The sub- keys for number of rounds (Nr) thatare used in encryption and decryption processes will be created by using an operation of the key schedule [9].

2.1. Stages of Rounds

2.1.1 Sub-Byte / Inverse Sub-Byte

The Sub-Byte function uses a substitution table (S-box) to substitute the bytes of state array. The byte substitution step used to increase the security level of AES algorithm because it agrees with nonlinearity requirement [10]. However**,** in the decryption process theInvS-box table instead of S-boxwill be used to implement Inverse Sub-Byte operation.

2.1.2 Shift Rows/ Inverse Shift Rows

Some references assume the shift rows operation as the second operation at the encryption round; while it can be applied before the Sub-Byte step without any effect on the algorithm. In shift rows operation the data matrix processes in row-by-row fashion. The first row remains unchanged, whilethe rows numbered with 2, 3 and 4 of the state matrix are rotated one, two and three bytes in cyclic way to the left-side, sequentially. In another side**,** the inverse shift rows operation is obtained by remaining the first row unchanged and rotating the rows numbered with 1, 2, and 3 cyclically rotate to the right-side, with one, two and three bytes, respectively [11].

2.1.3 Mix Columns / Inverse Mix Columns

After applying the Shift Rows operation, the Mix Columns step is performed, in this step each column in the state array is multiplied by a known 4x4 matrix defined as follows:

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$$

The multiplication operation is implemented on this matrix is not a normal multiplication. Rather, the multiplication operation is carried over a Galois-Field (GF), where the multiplication operation can be obtained as follows: Multiplication by 01 means no change, multiplication by 02 means is handled as shifting byte to the left with one bit, and multiplication by 03treated as shifting to the left, then XOR'ing with the operand [12].
The Inverse of Mix Column operation is applied by multiplying each column of a state array by another special matrix defined as follows:

$$\begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix}$$

2.1.4 AddRoundKey / Inverse AddRoundKey

The first AddRoundKey operation is implemented with the master key before starting the regular rounds operations of the algorithm. The AddRoundKey transformation is the part of the algorithm which takes each byte in the state array and XOR this byte with a corresponding byte in the round key.

2.2Key Expansion (Key Schedule)

The key expansion or the key schedule is an operation of generating a number of sub-keys from the initial key for each round to be used in the AddRoundKey operation. Therefore, the number of needed sub-keys is equal to the number of rounds (Nr) and hence the round keys contain 44words (where each word equal to four bytes)will be generated for AES-128. When the words indexed from 0 to 43.The first four word (W0, W1,W2,W3) are filled with the given cipher key, however columns in locations that are a multiple of 4 (W4 , W8 ,W12 … etc.) will be computed by three operations which are:The RotWordThe SubWord and addthe result of a RotWord and SubWord operations with word Wi-4 and with a Round Constant (Rcon[i])[13].

III. Chaotic HENON Map

The noticeable properties of chaotic systems which are sensitivity to the initial condition and control parameter values, unpredictability and their capability of generating random numbers made them used over the last years in many cryptography[13].There are many chaotic maps with multi dimension ,one of these chaotic maps is Henonmap that is a two dimensiondiscrete-time nonlinearmapexplained by:

$$\begin{aligned} Y_{n+1} &= 1 - aY_n^2 + Z_n \\ Z_{n+1} &= bZ_n \end{aligned} \qquad \boxed{(1)}$$

in each of the equation, the current and next chaotic states are (Y_n,Z_n) and (Y_{n+1},Z_{n+1}) respectively, while thevalues of a and b are map parameters. Any of the previous parameters (a, b) or initial states (Y_0 ,Z_0) could be to become a key to the aforementioned map[14,15].The Henon map exhibits chaotic behavior when $a \in [1.16,1.41]$ and$\in [0.2,0.3]$. The parameters values that commonly used in Henonsystem are (a= 1.4, b = 0.3) as shown in Figure (1).

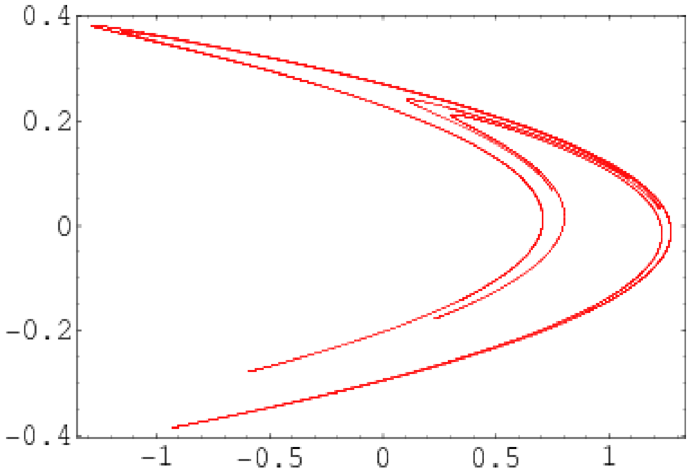


Figure (1): The strange attractor of Henon map with control parameters values (a= 1.4, b = 0. 3) .

IV. The Proposed Scheme

The multiplication over Galois Field is one of the greatest importance mathematical operation appliedduring the mix column step and one of thehigh calculation and computational overhead operation in AES [16]. Therefore, the mix columns and its inverse are two of the slower operations in the encryption and decryption process. This is due to the fact that, it involves matrixes multiplicationover Galois Field.This problem is opposed to adapt the original AES to encrypt video. To overcome the problem one mix columns for first round will be performed inaddition to new chaotic maskinstead of remained mix columns steps and their inverse in AES-128 for encrypting video frames due to the superiority of proposed scheme in terms of speed and the sensitivity to initial conditions and control parameters and also the increase ofkey space and key sensitivity. This modification is as shown in the following encryption and decryption algorithms:

Encryption Algorithm:

- The initial value (Y_0 , Z_0) and two control parameters (a, b) of Henon map in addition to the cipher key that expanded into array of 176 bytes as initial key of the algorithm.
- Due to the high sensitivity of the last three numbers for each output sequence, the proposed system takes the remainder of dividing the last three number of the map equations output (Y,Z) on the 256 to convert them into hexadecimal values, and save it in 4×4 matrix as chaotic mask.
- Sort the matrix values in ascending order.
- Assign the new index of sorted matrix as permutation key and matrix values as substitution key.
- Read the plain video and extract its frames. Then each frame is divided into blocks of the size 128 bits that is placed into the state array.
- Add the state array with cipher key.
- Substitute each byte with Sub-Byte transformation.
- Apply shift rows transformation.
- Use one mix columns transformation for first round and replacethe remained mix columns transformations (from the second round to Nr-1th round) with new chaotic maskfor scrambling the bytes positions of the state array by using permutation key, then the scrambled state array is XORed with chaotic mask values (substitution key).
- XOR the current state array with round key.
- Reassembling the encrypted frame from the encrypted state array, then collecting the cipher frames to create a cipher video.

Decryption Algorithm:

- Set the Henon map keys and cipher key which will also expand.
- Construct the Henon map based chaotic mask.
- Sort the chaotic mask values.
- Assign the substitution and permutation keys based on the values of generated mask and index of sorted chaotic mask, respectively.
- Read the encrypted video.
- Apply add round key transformation.
- Perform inverse of shift rows transformation.
- Use InvS-box to apply invers Sub-Byte transformation.
- Reapply add round key transformation.
- Perform inverse of chaotic mask stage for the first eight rounds by XOR'ing the state array with chaotic mask values, then descrambleit by using the permutation key, however the ninth round will be involved mix columns transformation.
- Finally, re-collecting the encrypted frames for cipher video compositing, then save it.

The block diagram of the proposed scheme for encryption and decryption processes is shown Figure (2).

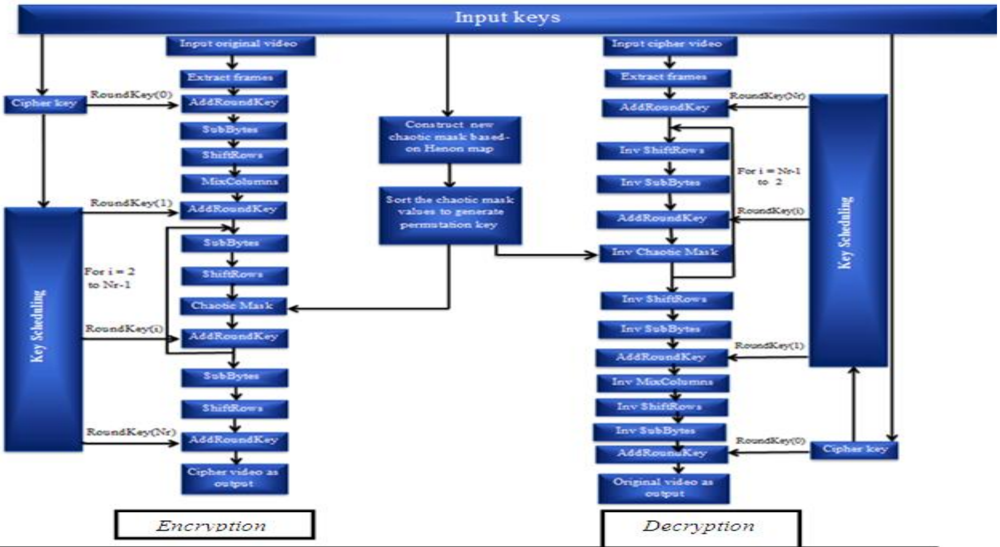


Figure (2):Block diagram of the proposed scheme for the encryptionand decryption processes.

V. Simulation Results

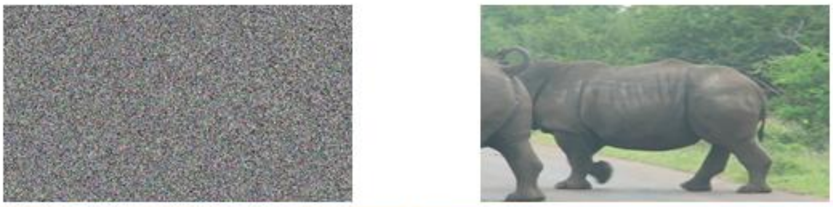
5.1 Security Analysis

5.1.1 Key Space Analysis

The total number of various keys thatcan be used in a proposed method is also known asthe key space.A high secure encryption system depends onthe strength of encryption keys. Whereas the key strength is mainly dependent on the key space. In another words, the relationship between the encryption key and the cipher message should be as complex as possible so any change of one bit of the encryption key will produce a total different cipher message.To achieve high resistance against many attacks such as brute-force attack, the key space of cryptosystemmust be large as possible [17]. The proposed methodconsists ofthe exist cipher key which is 2^{128}in addition to four real values that provided by the initial conditions (Y_0,Z_0) and control parameters (a, b) of Henon map, whilst each real value is 64 bits. Hence the total key space of proposed scheme is 2^{384},whichcan make the brute force attack is impossible on this proposed algorithm .

5.1.2 Key Sensitivity Test

The key sensitivity for each cryptosystem means that the encrypted videomustbecompletely differentfrom the original video, if there is any change between encryption and decryption keys. A strongciphering system requires large key sensitivityas much as possibleto ensure security of the system.The proposed scheme is high sensitive to anysmall change in one of all the keys. If the keys of the proposed system areY_0=0.50000001, Z_0=0.20000001, a=1.39999,b=0.200012 and a cipher key=abcd12349876efab,the key sensitivity test of the proposed algorithm has been applied on Rhinos(45) frame by using the same key that is used in decryption except that the value of (Y_0) is slightly changed to 0.50000002 and the plainframe is displayed in Figure(3).



a.Frame decrypted with incorrect ke b.Frame decrypted with right key

Figure (3):Result of key sensitivity analysis: a.Frame decrypted with incorrect key

5.1.3 Resistanceto Differential Cryptanalysis

The differential cryptanalysis is one of the most powerful cryptanalysis against block cipher, the differential cryptanalysisattempts toobserve differences of the cipherframe in the tiny change of the original frame to find the relationship between the original frame and the cipherframe. To evaluate the cryptosystem resistanceagainst differential attack,two measures (NPCR) and (UACI) commonly used , whereas the (NPCR) means the change rate of the number of pixels ofthe encryptedframe when only one pixel of the originalframeis changed and the(UACI) meansthe unified average changing intensity whichgauges the average intensity of variations between theoriginalframe and encryptedframe [19].Their definitions are as follows:

$$NPCR = \frac{\sum_{i,j}^{N,M} Diff\ (i,j)}{M \times N} \times 100\,\% \qquad \boxed{(2)}$$

$$UACI = \frac{1}{M \times N}\left[\sum_{i,j}^{N,M} \frac{C_1(i,j) - C_2(i,j)}{255}\right] \times 100\% \qquad \boxed{(3)}$$

In equation (2), the Diff (i, j) is determined by the initial cipher frameC_1(i, j) andciphered frame that is changed some grey level of the pixelsC_2(i, j), if C_1(i, j) = C_2(i, j) then Diff (i, j) = 0, otherwise, Diff (i, j) = 1.WhileM and N in both equations (2) and (3) are the width and height of the frame. The ideal NPCR and UACI values for 8-bit gray scale frames are 99.609% and 33.464%,respectively.

Table 1 shows the test results of NPCR and UACI measures for the proposed scheme that compared with original AES algorithm . It is discovered that the NPCR and UACIvalues of the proposed scheme are close to their ideal values. Thus, the proposedmethodhas great capacity of resistance to the plain text attacks anddifferential attacks.

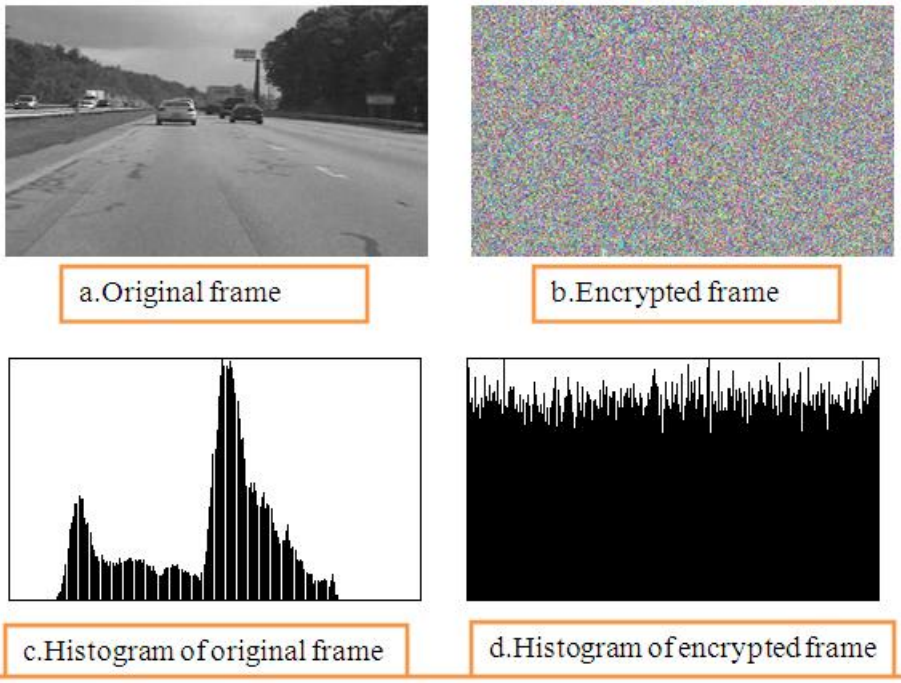
Frames	NPCR for original AES (in %)	UACI for original AES(in %)	NPCR for Modified AES (in %)	UACI for Modified AES(in %)
Rhinos (41)	99.6367	33.5693	99.6615	33.5298
Vipmosaicking(28)	99.6054	33.3138	99.6576	33.51
Shacky-Car(86)	99.5989	33.4324	99.6223	33.4046
Viplane(4)	99.58	33.3485	99.6544	33.4134

Table (1): Measurementsof NPCR and UACI for different frames.

5.2 Statistical Analysis

5.2.1 Frame Statistic Characteristic

The pixel valuesdistribution of each frame can be reflected byImage histogram. a flat histogram of cipher frame may mean that frameresist statistic attacks [20]. Figure (4) shows the red, green and blue channelshistograms of the originalframe and the cipherframe. We can see that, the histogram of the cipherframeisfairly uniformdistribution. Hence the proposed method does not present any clue to employ any statistical attack on the encrypted frame.



a.Original frame

b.Encrypted frame

c.Histogram of original frame

d.Histogram of encrypted frame

Figure (4): Histogram of original frame and encrypted frame

5.2.2 Information Entropy Analysis

Frame information entropy is defined to measure the degree of randomness ordisorder in the systemto give a description of the frametexture [11, 15]. Whenever thehistogram analysis only shows the cipher frame in a qualitative way, the information entropy used to get the quantitative analysis.The formula for calculation entropy H(x) For a frame with n gray level is:

$$H(x) = -\sum_{i=1}^{n} p(x_i)\log_2 p(x_i) \quad (4)$$

WhereH(x)represents of the frame and P(x_i) is the emergence probability of x_i . If every symbol has an equal probability, i.ex={x_0 , x_1, x_2 ,…x_{2^8-1} } and P(x_i)=1/2^8(i=0,1,…255), then the entropy is H(x)=8 which corresponds to an ideal entropy of a 256 gray-scale image.

The entropy analysis of encryptedframe is very closed to the ideal value as obtained in Table (2). Therefore, the proposed scheme resist the entropy attacks.

Frames	Actually Entropy	Cipher Frame Entropy with original AES	Cipher Frame Entropy with Modified AES
Vipmosaicking(62)	7.2803	7.9972	7.9973
Rhinos (63)	6.9627	7.9973	7.9977
Shacky-Car(57)	7.0824	7.9971	7.9969
Viplane(75)	6.6389	7.9967	7.9973

Table (2): Entropy analysis of different plain and cipher frames.

5.3 Time Analysis

Theefficiency of proposed scheme have been measured with important metric to compare amongcryptosystems is to compute the encryption and decryption time [21] . Time analysis has been implemented under C#.net on a 2.20 GHzIntel®Core ™ i3 CPU and 2 GB RAM -HP 650 laptop.Compared to original AES, we can show that the running speed of theproposed method is fast,when executed in the same conditions and environment.as obtained in Table(3).

Frames	Original AES Time(ms)		Modified AES Time(ms)	
	Encryption	Decryption	Encryption	Decryption
Viplane(53)	389	1033	231	305
Rhinos (3)	490	1300	286	385
Vipmosaicking(4)	489	1311	286	387
Shacky-Car(30)	492	1331	287	387

Table (3): examines quantitatively the encryption and decryption time of the original AES and proposed scheme.

VI. Conclusion

Generallyspeed and securecryptosystems are very desirable for multimedia applications.In this paper, an efficientmethod has been introduced for video encryption based on the combination of 2D Henon chaotic map and AES algorithm. Whereas Henon map is used to construct new chaotic mask to replace mix columns transformations except the first mix columns due to the slowness and security of the mix columns transformation in original AES. Efficiency of the methodhas been confirmed through above simulation results. According to these results the proposed scheme provides high key space, high key sensitivity and less time for encryption and decryption processes than original AES as well as itoffers high resistance against differential and statistical attacks.

References

[1]. S. Al-Maadeed, A. Al-Ali, and T. Abdalla, “A New Chaos-Based Image-Encryption and Compression Algorithm”, Journal of Electrical and Computer Engineering, 2012.

[2]. K.Sakthidasan, A. Sankaran And B.V.Santhosh Krishna “A New Chaotic Algorithm For Image Encryption And Decryption Of Digital Color Images”, International Journal Of Information And Education Technology, June 2011.

[3]. Axantum Software AB, "About AES – Advanced Encryption Standard", Svante, Seleborg, 2007.

[4]. H. Kezia and Gnanou F. Sudha, “Encryption of Digital Video Based on Lorenz Chaotic System”, IEEE, 2008.

[5]. S.Kamaliand et al, “ A New Modified Version of Advanced Encryption Standard Based Algorithm for Image Encryption” International Conference on Electronics & Information Engineering, IEEE,2010.

[6]. P. Deshmukh and V. KolheAxantum, “Modified AES Based Algorithm for MPEG Video Encryption”, S.A.Engineering College, Chennai, Tamil Nadu, India, IEEE, 2014.

[7]. Tanvi, “An Image Cryptosystem based on Pixel Scrambling and AES Algorithm”, International Journal of Computer Applications, 2013.

[8]. S. M. Wadi and N. Zainal, “High Definition Image Encryption Algorithm Based on AES Modification”, Springer, 2014. BehrouzeA.Forouzan, “Cryptography and Network Security”, McGraw Hill, International Edition, 2008.

[9]. J. Daemen and V. Rijmen, “The Design of Rijndael”, USA:Springer-Verlag New York, Inc., 2002.

[10]. S. Singh and A. Jain, “An Enhanced Text to Image Encryption Technique using RGB Substitution and AES”, International Journal of Engineering Trends and Technology (IJETT), 2013.

[11]. Naif B. Abdulwahed, “Chaos-Based Advanced Encryption Standard”, M.Sc. Thesis, King Abdullah University of Science and Technology, Computer Science Program, KSA, 2013.

[12]. WilliamStallings,”Cryptography and Network Security Principles and Practice”, Fifth Edition, Pearson Education, Prentice Hall publishing ,2011.

[13]. M. G. Avasare and V. V.Kelkar, “Image Encryption using Chaos Theory”, International Conference on Communication, Information & Computing Technology (ICCICT), IEEE, 2015.

[14]. A.Prusty,A.Pattanaik and S. Mishra, ”An Image Encryption and Decryption Approach
Based on Pixel Shuffling Using Arnold Cat Map and Henon Map”, 2013 International Conference on Advanced Computing and Communication Systems (ICACCS -2013), IEEE,2013.

[15]. G. Mehta and et al,”An Efficient and Lossless Fingerprint Encryption Algorithm Using Henon Map and Arnold Transformation”, International Conference on Control Communication and Computing (ICCC), IEEE, 2013.

[16]. [16] M.Kumarand S.Rajalakshmi,”High Efficient Modified MixColumns in Advanced

[17]. Encryption Standard using Vedic Multiplier", International Conference on Current Trends in Engineering and Technology, IEEE, 2014.

[18]. G.Hanchinamani and L.Kulakarni,"A Novel Approach for Image Encryption based on Parametric Mixing Chaotic System",International Journal of Computer Applications (0975 – 8887), 2014.

[19]. J. Zhang,"An Image Encryption Scheme Based on Cat Map and Hyperchaotic Lorenz System",IEEE International Conference on Computational Intelligence and Communication Technology, IEEE, 2015.

[20]. X. Huangand et al,"A Color Image Encryption Algorithm Based on a Fractional-Order Hyperchaotic System",Entropy, 2015.

[21]. P.Aggarwal and S.Vishwanath,"Design and Implementation of Video Encryption for Multimedia Applications",Journal of Engineering Research and Applications, 2014.

[22]. J.Chenand et al,"A fast image encryption scheme with a novel pixelswapping-based confusion approach",Springer, 2014.

[23]. S. Bahrami and M.Naderi,"Encryption of Video Main Frames in the Field of DCT TransformUsing A5/1 and W7 Stream Encryption Algorithms",Springer, 2014.