doi:10.25195/2017/4318

Hybrid Cipher for Secure Multimedia by using AES and RC4 Chain

Kassim Mohammed Awad[1] , Ali Makki Sagheer[2], Ayoob Abdulmunem Abdulhameed[3]

[1]College of Computer Science and Information Technology/ University of, Anbar
kassim.1991@yahoo.com
[2]College of Computer Science and Information Technology/ University of, Anbar
ali_makki_sagheer@yahoo.com
[3]Department of Management information system/ University of, Information Technology and Communications
ayub_abd@yahoo.com

Abstract— ***With development, technology, computer science، computer networks and transmission of multimedia between two or more parts, a security of multimedia becomes an essential issue since most of the systems became easy to attack. In this newspaper, we suggest a model to Hybrid Cipher for Secure Multimedia by using AES and RC4 Chain. The analysis and evaluate the performance of this model is measured by testing several parameters. Show The resulting multimedia is found to be more distorted in hybrid Cipher.***

Keywords— Multimedia Security; Security; AES; RC4

1- INTRODUCTION

In recent years, with the development of digital communications and digital transmission of multimedia. Become many of us in connection with the internet and intranet networks and transmits digital multimedia without think about the safety of digital multimedia. We share a much of our own data and secrets. Today in telecommunications networks has become necessary to protect multimedia because this multimedia are either files or medical pictures of these needs to be high confidentiality to prevent a thief from modification. Or the data may be, especially in a company or organization also needs to secure and save this data from unauthorized persons [1]. Encryption is the process of converting plain_multimedia to cipher_multimedia in order to be invisible this means to prevent anyone not authorized to recover the original multimedia. Encryption is used mainly to ensure confidentiality. Usually, companies or organizations use encryption before transmission to ensure the confidentiality of information during transmission across networks and be decrypted by the intended person [2].

While in the past, encryption indicates to the "encryption and decryption using secret keys". Today there are three kinds of keys: -"symmetric-key and asymmetric-key and hashing". The

Symmetric key uses one key secret for "encryption and decryption". In the asymmetric key, there are two keys instead of one where the key public key is used to encrypt the private key is used to decrypt. In hashing, "a fixed-length message digest is created out of a variable-length message". Symmetric encryption includes two classes: - stream ciphers and block ciphers. "In a stream-cipher, encryption and decryption are done one symbol (such as a character or a bit) at a time". We have a plain-multimedia stream, a cipher-multimedia stream, and a key stream. In a block cipher, a block of plain-multimedia symbols of size N (N>1) are encrypted together, creating a block of cipher-multimedia of the same size [3].

2- RELATED WORKS

In 2012 Prabhudesai . And Vijayarajan [8]. Developed a novel mix cipher by merging the features of double ciphers called "AES (Advanced Encryption Standard) and Rc4 (also identified as ARC4)". The features of in cooperation ciphers have been calculated and a novel cipher merging the features of mutually the ciphers is created which is added more protected than the basic encryptions. AES features are safety and its confrontation against attacks and the main features of Rc4 is quickest. Then, these features are mixed in a new created code. Thus, it shows to be quicker than the basic AES and protected against greatest attacks. Three grouping ways have been expressed to create a mongrelized cipher and the process along with the strong point and flaws outline. The third cipher is the main cipher that is focused on this newspaper. It is also displayed, that this cipher is impervious against most attacks. This determination ensures the " confidentiality" of the data which is used to encode.

In 2013 Nares and et al. [2]. Have emargined a new amalgam cipher by joining the features of 3 ciphers name "AES (Advanced Encryption Standard), Rc4 (identified as ARC4) and Serpent". The features of in cooperation ciphers are calculated, and a novel cipher merging the features of in cooperation the ciphers is produced that is more protected than the plain codes. "AES, SERPENT features are its security and its resistance against attacks and the main specific of Rc4 is its speed". Thus, these features are mixed in the new produced code. Thus, it shows to be quicker than the basic AES and protected against greatest attacks.

In 2014 Dilpeet K. and Gurjit S. B.[7] used a combined concept of existing encryption algorithms AES and RC4 along with Hash Function and whitening to obtain a hybrid model which can be used for encrypting various kinds of data.

3- THE PROPOSED SYSTEM

The security of multimedia performs by "using symmetric-key that is both encryption and decryptions use the similar key. The key must be distributed to both the transmitter and the receiver of the multimedia". When seeing time difficulty, effectiveness, and costs, "symmetric-key" encryption is considered the finest solution, and key sharing remains a problematic when using this method. The AES algorithm is practical with" key length of 128-bits" which is appropriate for the resolution of encoding, multimedia with dissimilar size and handling time resulting in an equitable cost. As shown in fig.1.

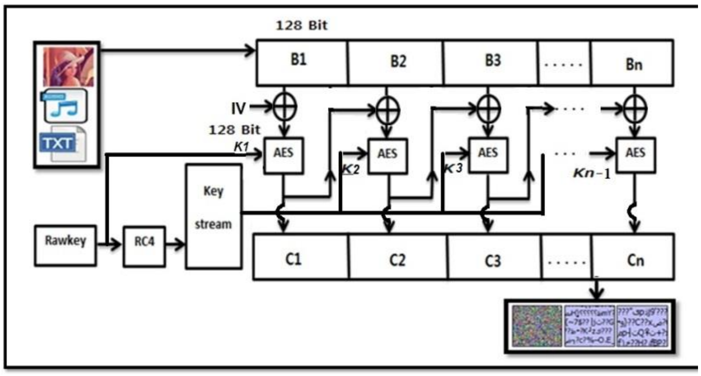

Figure 1: The Encryption Model.

Before encryption, the multimedia converted to an array of bytes. To products the first block of cipher multi, first block of multi plain is XOR with an" initialization vector (IV)" the result encryption of the original key. The second block of multi plain is XOR with previous block of multi cipher, the key for the second block is generated by entering the original key to RC4 algorithm to Products Key Stream. The rest of the block plans are encrypted in the similar case. The following steps show the encryption equation:

C1=E([IVxorB1],K1)

Ci=E([Ci-1 xor Bi],key_stream) 1< i≤n

K1=key_Raw

Ki=key_stream (generated by RC4) 1< i ≤ n

Where ***n*** is the number of blocks, ***P*** is the multi plain, ***K*** is the key, ***C*** is the multi cipher and ***E*** is the encryption algorithm . The decryption model is shown in fig.

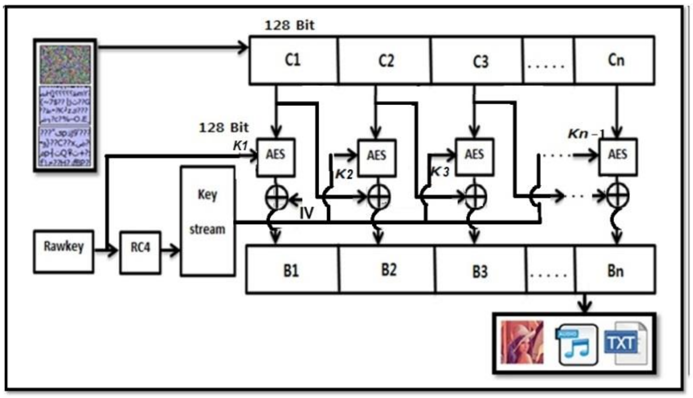

Figure 2: The Decryption Model.

The decryption model works in reverse. To products the first block of multi plain , first block of multi cipher is decrypted with the original key after that the result XOR with " an initialization vector (IV)".The second block of multi cipher is decrypted by the key stream after then the result XOR with previous block of multi cipher. Through the decryption process, all blocks will be determined by the prior block to be decrypted right, otherwise these blocks will not decrypt right . This can also be measure useful when the multi plan is not recovered in the correct form, it directs that the multi plan has been possibly disclosed or altered. Then, this system can also provide integrity by privacy . The following steps show the decryption equation:

P1 = D(C1,K1) XOR IV

Pi =D(Ci,key_stream) XOR Ci-1 1 < i≤ n

K1= original key

Ki=key_stream (generated by RC4) 1< i ≤ n

Where ***D*** means the decryption algorithm.

4- RESULTS AND DISCUSSION

The suggested system is tested on four selected images, four audio files and four text files with different sizes. The proposed system is implemented on a PC with a 2.30 GHz Core i3 CPU and 4 GB of RAM. Visual C#.NET programming language was used to implement the suggested system. In this segment, a number of measures of taken into account; "histogram, correlation coefficient, Number of Pixel Changing Rate (NPCR) and Unified Averaged Changed Intensity (UACI), Execution Time and entropy of information".

a. Histogram

The histogram is a statistical measure used to supply image statistics. It computes the frequency distribution of the elements in each input color image by distributing the amount of pixels to each value [4].

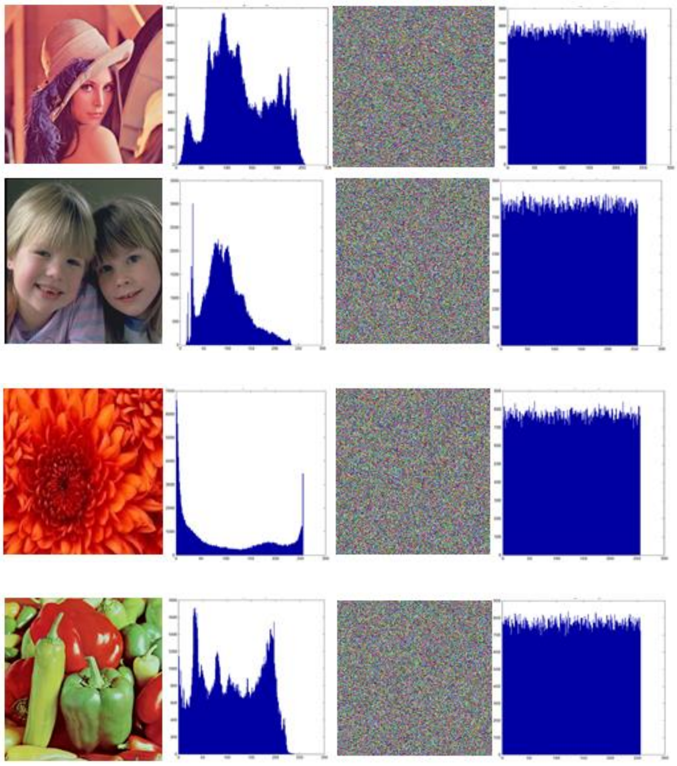

Figure 3: Histograms of Plain and Cipher Images.

The histogram measures in Fig 3 explain distributed pixel values and different between origin image and cipher image, where distributing pixel values for image-cipher are equivalent to avoid-attacks from obtain plain image.

b. Correlation Coefficients

The correlation coefficient is a measure that is can be used to compute the amount of match between two variables. It is a beneficial ration to determine the encryption quality of any encryption system. The encryption system to be, well, if encryption Algorithm hiding all features of a normal image, and encoded image is all random and very uncorrelated. The correlation his values range from -1 to 1, where Values near to 1 indicate that there is a positive "relationship between the variables ,Value near to -1 indicate that there is a negative relationship between the variables, Value near to or equal to 0 suggest there is no relationship between the variables". In this paper correlation value near to zero. It indicates to the efficiency and performance of an image encryption process. "Correlation coefficients" can be calculated using equation1 [4,5].

$$\mathrm{R} = \frac{\frac{1}{N}\sum_{i=1}^{N}(Pi-P)(Ci-\overline{C})}{\sqrt{\frac{1}{N}\sum_{i=1}^{N}(Pi-\overline{P})^{2}\frac{1}{N}\sum_{i=1}^{N}(Ci-\overline{C})^{2}}} \qquad (1)$$

Where P & C are the average of the image and it after one pixel modification for plain or cipher image which that means "gray-level" values of two neighbouring pixels in the input image, shows the resulting correlation that can be achieved on "horizontal, vertical and diagonal" in the following Table 1 .

Table 1: Correlation Coefficients of Two Adjacent Pixels for Plain and Cipher Image.

File Name	Direction	Plain Image	Cipher Image
Lena	Horizontal	0.9874	0.3352
	Vertical	0.9674	0.3148
	Diagonal	0.9827	0.5867
Children	Horizontal	0.9882	0.3211
	Vertical	0.9557	0.3342
	Diagonal	0.9852	0.5894
Chrysanthemum	Horizontal	0.9552	0.3184
	Vertical	0.9263	0.3329
	Diagonal	0.9210	0.5624
Pepper	Horizontal	0.9825	0.3236
	Vertical	0.9862	0.3196
	Diagonal	0.9705	0.6053

c. Attack Resistant

Commonly, the attacker tries to make simple changes in the cipher multimedia such as changing one pixel of the encrypted image or one byte for audio and text, if the attacker is discover any related information about plain multimedia from the cipher multimedia then the algorithm used for encryption is ineffective. Encryption algorithm to be good must be able to resist differential attack. This is required measuring the effect on pixel change or byte change by using two extensive analyses; they are the "number of pixel changing pixel rate (NPCR) and unified averaged changed intensity (UACI)" [5,6]. They are computed by equations 2 and 3.

$$\mathrm{NPCR} = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j)}{\mathrm{MxN}} x100\% \qquad (2)$$

$$\mathrm{UACI} = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{|C1(i,j)-C2(i,j)|}{255}}{\mathrm{MxN}} x100\%\% \qquad (3)$$

D(i, j) =0 if C1 (i, j) = C2(i, j) otherwise D(i, j) =1 where C1 (i, j) & C2(i, j) are the pixel values in the location of the (I,j). The multimedia are tested here where each type of multimedia is encrypted double, the first one is a plain multimedia which is encrypted by the suggested model , the second is the cipher of plain multimedia after modifying one bit from key encryption. Shows the result NPCR and UACI in Table 2.

Table2:NPCRand UACI Values for Encrypted Multimedia with Encrypted Multimedia after Changing Key One Bit.

File Name	NPCR	UACI
Lena	99.6353	33.4640
Children	99.6570	33.4095

Chrysanthemum	99.6345	33.4554
Pepper	99.6753	33.5215
Audio1	99.6176	33.6007
Audio2	99.6050	33.3510
Audio3	99.6353	33.4666
Audio4	99.6345	33.5464
Text1	99.8991	32.8253
Text2	99.6570	34.1024
Text3	99.5689	33.9876
Text4	99.6753	33.3223

The optimal value for NPCR is 100%. In this newspaper all NPCR values are proximate to optimum values. From other side, values of UACI are dissimilar from one file to another, depending on the density of values.

d. *Entropy of Information*

Entropy is a very important measure for multimedia encryption. The idea of entropy is to compute the degree of the ambiguity between plain multimedia and encrypted multimedia. The best case will be when the probability of each value is identical. The entropy, H (m) can be computed by equation 4 [4, 5].

$$H(m) = \sum_{i=0}^{2N-1} p(mi)x\log_2 \frac{1}{p(mi)} \quad (4)$$

Where:P(mi)is the probability of mi, H (m) =8 is optimal entropy for multimedia (mi) involves of 256 values when

there are equal probabilities for all value. Shows the result in table 3.

Table 3: Entropy for Multimedia Before and After Encryption

File Name	Entropy_plain Multi	Entropy_cipher Multi
Lena	7.2352	7.9972
Children	7.4485	7.9971
Chrysanthemum	6.9929	7.9974
Pepper	7.3374	7.9970
Audio1	3.4408	7.9968
Audio2	2.0473	7.9982
Audio3	3.4209	7.9984
Audio4	2.9756	7.9983
Text1	4.2866	7.7841
Text2	4.3381	7.9236
Text3	4.3973	7.9485
Text4	4.3819	7.9665

e. *Execution Time*

The execution time for the encryption practice is a very significant measure. Therefore, the suggested encryption model has good execution time for encryption, plain multimedia and decrypted by using the same secret key. Results of testing for different file multimedia [4]. Shows the result in Table 4.

Table 4: Execution Time for Encryption and Decryption Multimedia

File Name	Enc_Time/ms	Dec_Time/ms
Lena	740	1307
Children	747	1310
Chrysanthemum	741	1320
Pepper	742	1312
Audio1	1333	440
Audio2	2272	654
Audio3	3955	684
Audio4	4210	898
Text1	92	122
Text2	89	248
Text3	103	286
Text4	152	425

5- CONCLUSION

With the development of digital communications, multimedia encryption plays a important role, Therefor, an efficient encryption system is necessary. The applied algorithm for encryption is "AES with 128-bit key length". AES key size should be 128-bit. Therefore, the suggested model uses the RC4 algorithm to generated key stream used to products a random key of the wanted size and give more security because if the same multi plain block is repeated, this suggested model produces different multi cipher blocks. Evaluate the performance of this model is tested by applied measures such as histogram where noted distributed pixel values for image cipher are equivalent to avoid attacks from obtain plain image, correlation coefficient noted correlation value near to zero It indicates to no relationship between the variables, Attack Resistant(NPCR and UACI) noted all NPCR values are near to optimum values(100%) and UACI values depending on the density of colors ,entropy of information near to optimum values and suitable execution time. This model can be enhanced the speed of encryption process and decrease the cost of multimedia transition by compression of the multimedia before encryption.

REFERENCES

[1] Reena J. Shah And Bhavna K. Pancholi," Multimedia Security Techniques ", International Journal Of Innovative Research In Electrical, Electronics, Vol. 2, Issue 5, May 2014.

[2] Naser Aghajanzadeh, Fatemeh Aghajanzadeh and Hamid Reza Kargar,"Developing a new Hybrid Cipher using AES, RC4 and Serpent For Encryption and Decryption", International Journal of Computer Applications (0975 – 8887), Volume 69– No.8, May 2013.

[3] Shaaban Sahmoud, Wisam Elmasry And Shadi Abudalfa," Enhancement The Security Of AES Against Modern Attacks By Using Variable Key Block Cipher",International Arab Journal Of E-Technology,Vol.3,No.1,January 2013.

[4] Abdulrahman Dira Khalaf," Fast Image Encryption based on Random Image Key",International Journal of Computer Applications (0975 – 8887), Volume 134 – No.3, January 2016.

[5] Jawad Ahmad And Fawad Ahmed," Efficiency Analysis And Security Evaluation Of Image Encryption Schemes ",International Journal Of Video & Image Processing And Network Security IJVIPNS-IJENS, Vol:12 No:04.

[6] M. Kiran Reddy And K. J. Jegadish Kumar,"Security Analysis Of Fbdk Block Cipher For Digital Images",IJRET: International Journal Of Research In Engineering And Technology Essen: 2319-1163 | Piss n: 2321-7308.

[7] Dilpeet K. and Gurjit S. B. , "Improving Encryption Process by Making a Hybrid Encryption Scheme", Department of Computer engineering Punjabi University, Patial, September, 2014.

[8] Prabhudesai K. and Vijayarajan V. S, "An Amalgam Approach using AES and RC4 Algorithms for Encryption and Decryption", VIT University, Vellore, September 2012.