Open Access **Baghdad Science Journal** **P-ISSN: 2078-8665**
Published Online First: May 2022 **2022, 19(6): 1378-1386** **E-ISSN: 2411-7986**

DOI: https://dx.doi.org/10.21123/bsj.2022.6398

Comparison between RSA and CAST-128 with Adaptive Key for Video Frames Encryption with Highest Average Entropy

Enas Tariq Khudair ***Ekhlas Falih Naser**** ***Alaa Noori Mazher***

Department of Computer Sciences, University of Technology, Baghdad, Iraq
*Corresponding author: 110022@uotechnology.edu.iq
E-mail addresses: 110038@uotechnology.edu.iq , 110027@uotechnology.edu.iq

Received 5/6/2021, Accepted 12/1/2022, Published Online First 20/5/2022, Published 1/12/2022

Abstract:

Encryption of data is translating data to another shape or symbol which enables people only with an access to the secret key or a password that can read it. The data which are encrypted are generally referred to as cipher text, while data which are unencrypted are known plain text. Entropy can be used as a measure which gives the number of bits that are needed for coding the data of an image. As the values of pixel within an image are dispensed through further gray-levels, the entropy increases. The aim of this research is to compare between CAST-128 with proposed adaptive key and RSA encryption methods for video frames to determine the more accurate method with highest entropy. The first method is achieved by applying the "CAST-128" and the second is achieved by applying the "RSA ". CAST-128 utilizes a pair of sub-keys for each round as a quantum of five bits that was utilized as a key of rotation for each round and a quantum of 32 (bits) was utilized as a key of masking into a round . The proposed adaptive 128-bits key can be extracted from the main diagonal of each frame before encryption. RSA is a public-key cryptographic technique which can be known as (asymmetric) cryptography. An asymmetry of a key depends on factoring a product of two big prime values. A comparison was applied on several videos and the results showed that CAST-128 method proved the highest degree of entropy even if the frames have lots of distorted data or unclear image pixels. For example, the entropy value of a sample of a girl video is 2581.921 when using CAST-128, while it is 2271.329 when using the RSA; also the entropy value of a sample of a scooter video is 2569.814 when using the CAST-128, while it is 2282.844 when using RSA.

Keywords: Asymmetric key, CAST-128, Cryptography, RSA, Symmetric key

Introduction:

The safety of data within a video becomes further substantial nowadays because of the quick development in the compression of multimedia video and the latest evolution within the technologies of the internet [1]. Those breakthroughs have enabled data of video to be employed like a medium out of which critical information can be transmitted and stored easily. Hence, the data of video need to be protected from unauthorized arrival through the way of storage and transmission. Encryption of video is the most secured and established ways for protection of video's content[2]. With the quick growth within the technology of multimedia, numerous armies via the world are employing videos for training recently recruited troops. Such critical data have to be preserved either within storage or transmission[3]. One potential road for protection the information within multimedia is to stop the arrival of unauthorized users. But this way cannot produce certain that the information of multimedia is secure physically. Another simple way is to encrypt the stream of bits completely via an algorithm of cryptographic like AES or DES[4]. However, videos possess generally a great amount of the data and demand real-time operations. In the situation of wireless-mobile systems, they are restricted within power of processing; bandwidth and memory are rarely capable for handling the dense encryption processing capacity[5]. Therefore, taking into sight the particular features for resource-limited systems, novel algorithms for encryption the video must be developed. With real-world applications, an algorithm of encryption the video has to take into account diverse arguments like efficiency within computational, security, efficiency of compression and so on. Various kinds within applications of video demand various securities' levels[6]. For example, within the video deep security will be best while within purposes of military or financial information, high level of security is desired to prevent totally unauthorized arrival[7]. An efficiency of computational referees that the process of decryption or encryption should not take too much delays of time and meet the requirements of real-time implementations[8]. Compression of video is utilized to decrease the storage area and conserve bandwidth, therefore; the process of encryption should own the minimal impact on an efficiency of the compression. An algorithm of video encryption should supply adequate security and high efficiency of computational[9].The first disadvantage of employing DES is that, the hardware enforcement of DES is extremely rapid; DES is not prepared for software and runs slowly. The second disadvantage is that DES utilizes one private key only for decryption and encryption because it is symmetric technique so if the key is lost within encryption of data then it cannot obtain the readable data at the receiving party. The main advantage of employing CAST-128 is that it is faster significantly compared with DES. The primary advantage of RSA method is increasing convenience and security. Private keys are never supposed to be revealed or transmitted to any party. But the secret keys of DES must be transmitted which may be a way for an enemy who can reveal these keys over their transportation. RSA can supply a technique for signatures digitally which is a major second advantage within RSA.

The contributions of this paper are:

1. Using the RSA encryption method.
2. Using the CAST-128 method with the adaptive key.
3. The adaptive key used in the CAST-128 encryption method is extracted from the main diagonal of each frame. Each frame is with size 128x128 pixels.
4. Calculating the entropy values for each method.
5. The process of comparing the methods used on the basis of the highest entropy, where the method with higher entropy is considered the best method for encoding.

Related Works

Tremendous content of data transported via the network made encryption of video extremely an important topic, but when encryption of video works have been reviewed, it can be observed that works which focus on this topic are few.

The next works introduce the most significant algorithms for encrypting the video:

1. Ibrahem et al [10], suggested a method for encryption of video via employing a chaotic system to generate the key and stream-cipher .They employed chaotic chart as one time generator of the key which produced the key of encryption. Two methods were suggested for key generation. The first method utilized cat-map as a created key while the second method introduced larger space of key because it employed three values initially, two for cat-map and one for logistic-map that increased the number of premier values and equations' number leading to rise the time for generation of key. Empirical outcomes displayed that both suggested methods are secure and they can reconstruct video with perfect (MSE) equal to zero and extreme amount for PSNR.
2. Kunte et al [11] proposed a work for emphasizing an encrypting simply the frame's chunk which was of greater awareness of (Video on Demand) VoD. Selecting novel encryption of video depended on entropy and was calculated via utilizing special parameters like PSNR, coefficient of correlation, Histogram and NPCR. The outcomes provided most the optimum amounts and employed for exercises of the method in (VoD).
3. Cheng, et al [12], proposed an encryption procedure for (H.264/AVC).This procedure encodes a video to numerous pieces through the employ of (Cipher Feedback) (CFB) style of AES with a dynamic key. The key was updated too in real-time and was produced via (PRNG). The framework of encryption goes via three levels. A novel (4-D) hyper chaotic procedure was produced to protect the privacy of data. Empirical outcomes displayed that the proposed methodology for encryption of video owned less time and better effect for encryption.
4. Nahresdt et al [13], produced a novel algorithm known Video- Encryption-Algorithm (VEA). It depends on the statistical characteristics of (MPEG) video norm and an algorithm of symmetric-key which decreases the encrypted data amount. An algorithm of VEA splits the input stream of a video into two chunks and those chunks are extra split to segments of data to list of odd and list of list. After that, a key of encryption is utilized to the list of even. The encoded resultant list is merged XORed with the list of odd and the concatenated outcome is the ultimate cipher-text. As an outcome, VEA is protected from known plain text attack due

to every frame will have a various key.

5. Wang et al [14]. suggested a technique which is considered the connection amidst the descendant and current frames. The encrypted current-frames further dependent on descendant -frames. They simply encrypted the current-frames, while the dependent-frames are not encrypted. The main advantage of this technique is reducing the rate of bit within a video to a great scope.

Proposed Methodology

The proposed methodology for video frames encryption and decryption is made up of three steps. In the first step, the video frames series are taken from video stream. The keys for the methods of encryption have been prepared and then CAST-128 encryption method is applied on each frame, then the encrypted frames have been stored. After that, RSA encryption method is applied on each frame, and the encrypted frames are stored in the second step. For the third step, entropy is computed for each frame to find the best encryption method based on highest average entropy. A flowchart for the proposed methodology is shown in Fig. 1:

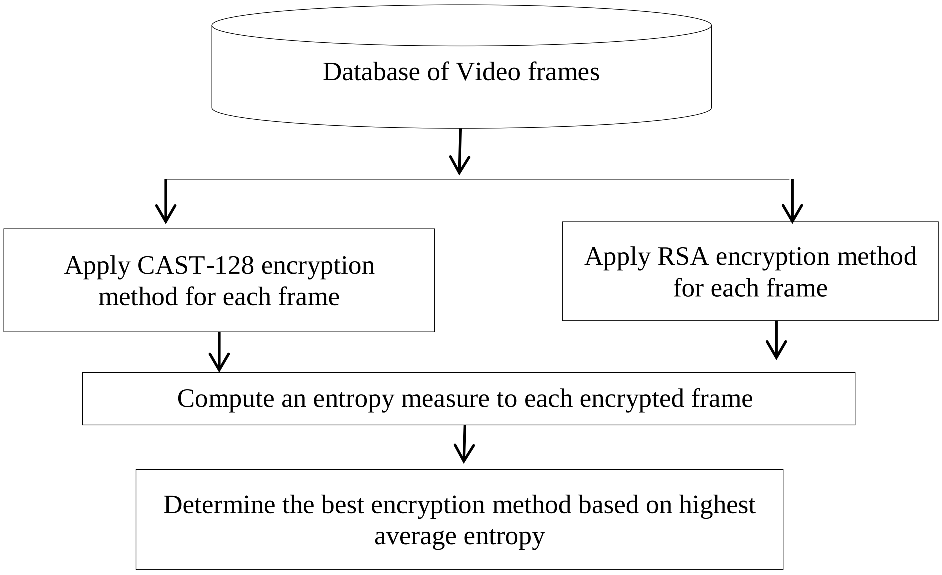

Database of Video frames
Apply CAST-128 encryption method for each frame
Apply RSA encryption method for each frame
Compute an entropy measure to each encrypted frame
Determine the best encryption method based on highest average entropy

Figure 1. Block diagram of the proposed system for key frames extraction

CAST-128 with Adaptive Proposed Key Encryption Method

A suggested methodology for encryption of a video frames has two steps. The values of the main diagonal of an image can be extracted as a key in the first step. Secondly the steps of CAST-128 can be calculated.

- **CAST-128 Key Generation**

The key of CAST-128 can be extracted from the main diagonal of each frame. The size of each frame is 128x128.The key is calculated from the following formula:

```
1) for i=1 to image_width
2) for j=1 to image_height
3) if ( i=j) then key[i]=pixel[i,j]
```

- **CAST-128 Steps**

Secondly the steps of CAST-128 can be calculated. (CAST-128) employs the pair of sub keys per-round as a quantum of 5-bits [kr_i] which can be employed as a key of rotation for rounding [i] and a quantity of 32-bits [km_i] are employed like the key of masking for rounding [i]. Three diversified functions for rounding can be employed in the algorithm of CAST-128 [15]. The parameters of the rounds can be illustrated below:-

1) Input the data [D] to the operation ([I_a]) and ([I_d]) represent the extreme worthy (byte) via LSB "least significant bit" for ([I]).
2) [S_i] refers to (ith s-box).
3) [O] is the operation's output.

The process of encryption and decryption using CAST-128 is illustrated in Fig.2.

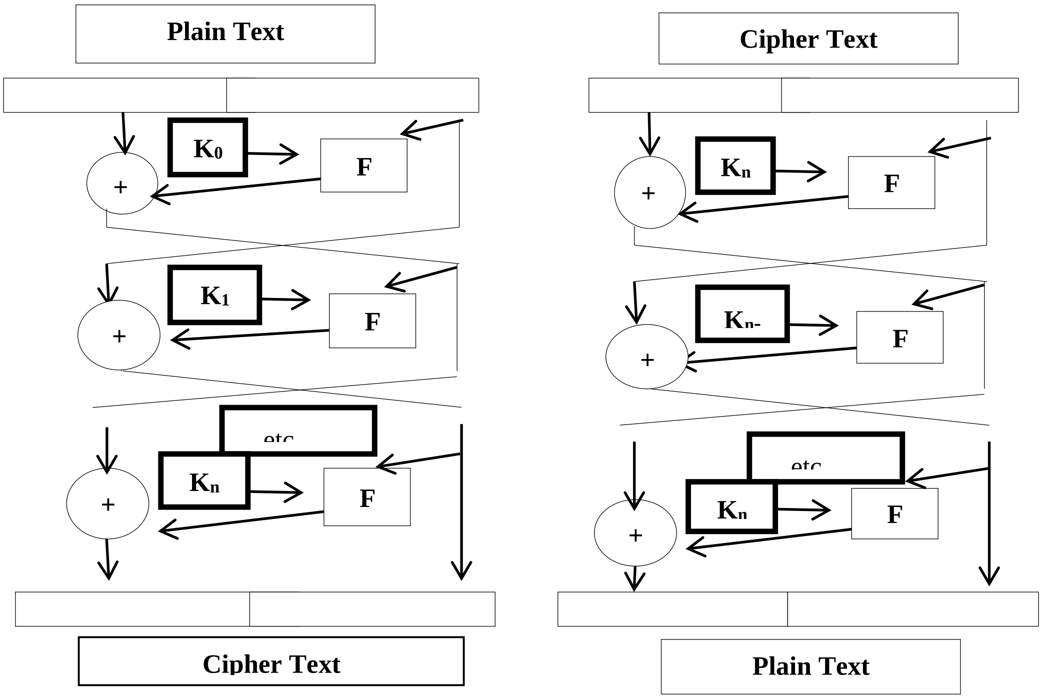


Figure 2. Decryption and Encryption of CAST-128 [16]

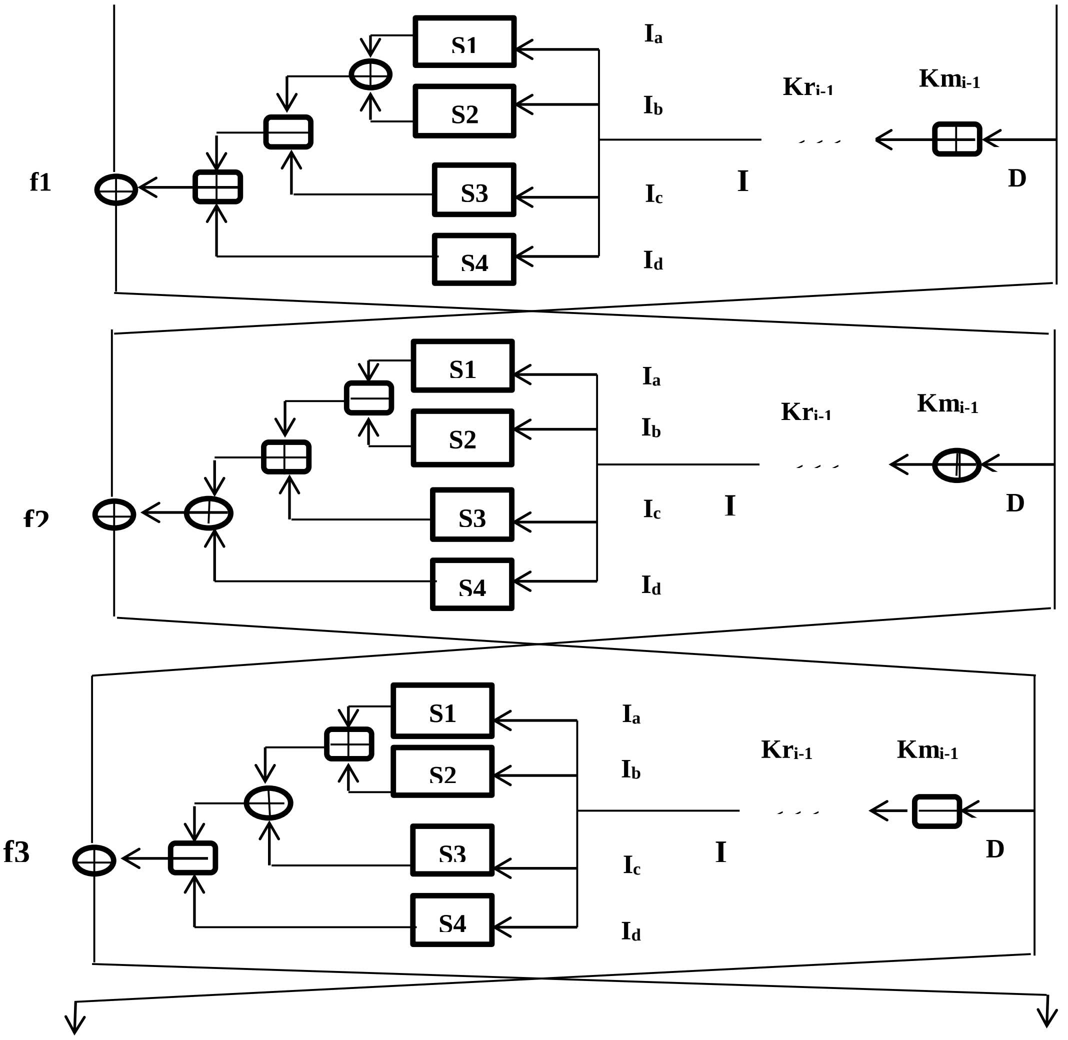


Figure 3. Encryption Procedure for CAST-128[16] [16]

Table 1. shows the conventions of Function F

Rounds (1,4,7,10,13,16)	$(I = ((Km_i + R_{i-1}) <<< Kr_i)$, $F = ((S_1[I_a] \wedge S_2[I_b]) - (S_3[I_c])) + S_4[I_d])$
Rounds (2,5,8,11,14)	$(I = ((Km_i \wedge R_{i-1}) <<< Kr_i)$, $F= ((S_1[I_a] - S_2[I_b]) + (S_3[I_c])) \wedge S_4[I_d])$
Rounds (3,6,9,12,15)	$(I = ((Km_i - R_{i-1}) <<< Kr_i)$,$F= ((S_1[I_a] + S_2[I_b]) \wedge (S_3[I_c])) - S_4[I_d])$

Function (F) can be defined for these conventions as illustrated in Table 1 The function F in Fig. 3 was developed to obtain good diffusion, confusion and avalanche features. It employs the substitutions of S-box, exclusive OR operations, mod 2 subtraction and addition and key dependent rotation. (F) function's strength is dependent firstly on the S-boxes' strength. Additional usage of operations such as Boolean, arithmetic, and rotate gives it extra strength [17]. A function F encompasses employing four substitution-boxes (S-boxes), each with volume (8 x 32) leaves circular rotation operation and four operation techniques which are different relying on the number of rounds. These operation functions can be referred to in Fig. 2 as [$f1_i$], [$f2_i$],[$f3_i$] and [$f4_i$] . (I) can be used to define the intermediate value of 32-bits beyond the function of "left circular rotation" and the labels, the function F in Fig. 3 was developed to obtain good diffusion, confusion and avalanche features. It employs the substitutions of S-box, exclusive OR operations, mod 2 subtraction and addition and key dependent rotation. (F) function's strength was dependent firstly on the S-boxes' strength. Additional usage of operations such as Boolean, arithmetic, and rotate gives it extra strength. A function F encompasses employing four substitution-boxes (S-boxes), each with volume (8 x 32) left circular rotation operation and four operation techniques which are different relying on the number of rounds. These operation functions can be referred to in Fig. 2 as [$f1_i$], [$f2_i$], [$f3_i$] and [$f4_i$]. (I) can be used to define the intermediate value of 32-bits beyond the function of "left circular rotation" and the labels ([I_a], [I_b], [I_c] and [I_d]) can be used for defining ([I]) of 4-bytes while ([I_a]) was a maximum significant and ([I_d]) was a minimum significant [18].

RSA Encryption Method

A cryptographic algorithm of RSA is a public-key and also called asymmetric-cryptography. The asymmetry of a key relies on factoring the product of two big prime numbers [19]. Messages that were encrypted within a public-key could be decrypted also in a feasible time's amount via employing a private key. Exponent and Modulus operations are performed to produce the private and public keys [20]. The cryptosystem's security with RSA is associated with factoring great numbers and finding "eth" root modulus of a composite "n", then computing an amount "m" via "C=m^e (mod n)" in which "n ,e" represent the public key and "C" represents a cipher text. If an attacker calculates a secret exponent "d "from the public key "n, e " then "C" is decrypted via employing a standard process. But surely it is time - wasting to detect an integer factorization within a polynomial time, and this still proves (RSA) to be a robust algorithm [21]. Employing small and approximately close primes:
if the primes are small to an adequate degree, then a factorization of (n) will be a simple duty. if (p) and (q) are comparatively close, then detecting the common factors determines the public-key. It needs longer time for encryption and usage of a memory which finally slows down the algorithm's speed [22]. The parameters of RSA can be illustrated as:

1. Choose q and p which are primes, where $q \neq p$
2. Compute the value of n via $n = q*p$
3. Compute $(\Phi(n) = (p-1)*(q-1))$
4. Choose the variable (e) as integer type where $(GCD (\Phi(n), e) = 1)$ and $(1 <e < \Phi(n))$.
5. Compute the value of d via $(d \equiv e^{-1} \pmod{\Phi(n)})$)
6. The public-keys (n, e) and the Private-Keys (d, n).

For Encryption: (M) refers to the plain-text and must check (M < n). The Cipher-text (C) can be computed via ($C = M^e \bmod n$)

For Decryption: The Cipher-text(C) entered and the plaintext can be computed via ($M = C^d \bmod n$).

Entropy

Randomness is a substantial characteristic in the processes of cryptography because the information must not be capable to be predicted by an attacker. Entropy is a measure of information randomness [23]. It measures the information’s uncertainty. Within the information’s security, it requires algorithms of security to produce an encrypted message with a high degree of randomness so that there is no dependence between cipher-text and key, or it becomes less. With a high degree of randomness, the relevance among cipher-text and key turns out to be complicated. This characteristic can also be named confusion. A high grade of confusion is preferred so as to make it more complex to be predicted by an attacker. Entropy can be employed to reflect the cryptographic algorithms' performance [24]. We can calculate entropy using Eq.1 [25].

$$Entropy = \sum_{g=0}^{l-1} P(g) * [P(g)]^2 \qquad \mathbf{1}$$

"L" represents an overall number with gray levels ready. For a model "8-bits", there are 256 numbers that range from "0 to 255".

"p (g)= (N(g)/X*Y)"

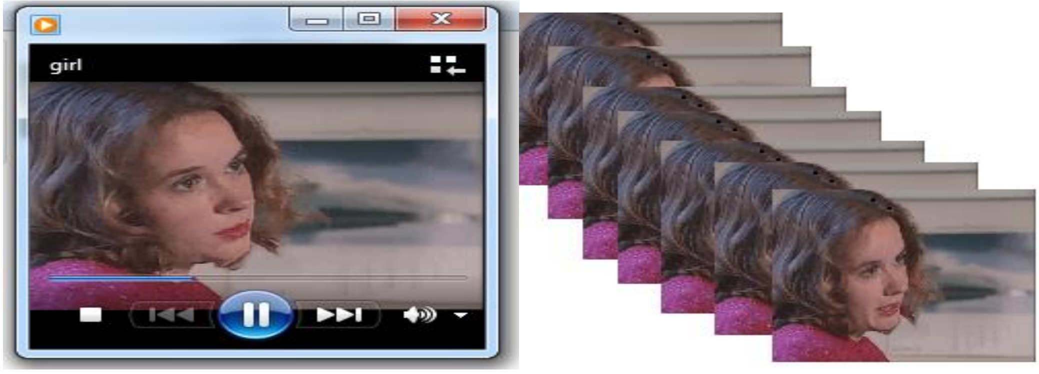
"N (g)" represents the numbers of pixels at gray level "p".

P (g) represents a probability.

Empirical Results

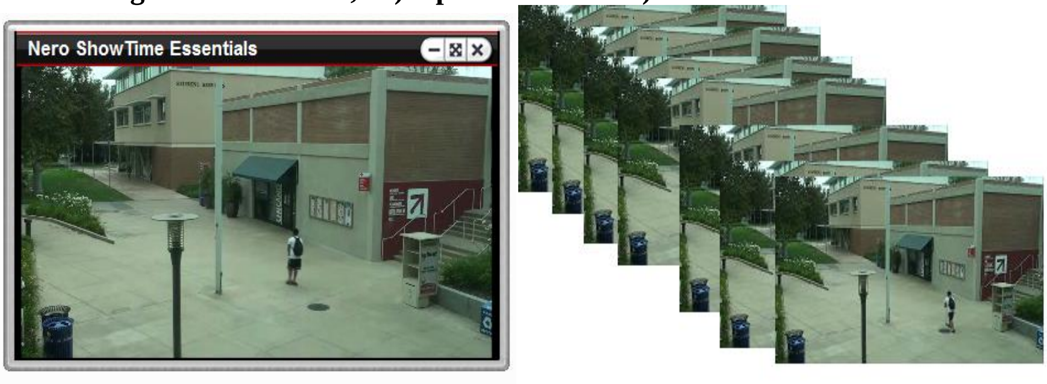
The empirical results of the proposed methods are discussed and displayed in this section. The proposed methods were implemented using C# programming language. The main libraries used with the implementation of this work are Accord.Net and AForge to load a video, extracts frames and then apply encryption methods. Five kinds of databases are utilized to evaluate the proposed methods. The proposed methods consist from three steps as illustrated bellow:-

1. At the first step, the video stream is loaded and the frames are extracted as shown in Fig.4 for girl video, Fig. 5 for scooter video and Fig. 6 for car video. The values of the variable p and the variable q are set to the length of a frame for RSA encryption method. While the key of CAST-128 is adaptive and extracts this key from the main diagonal of a frame.



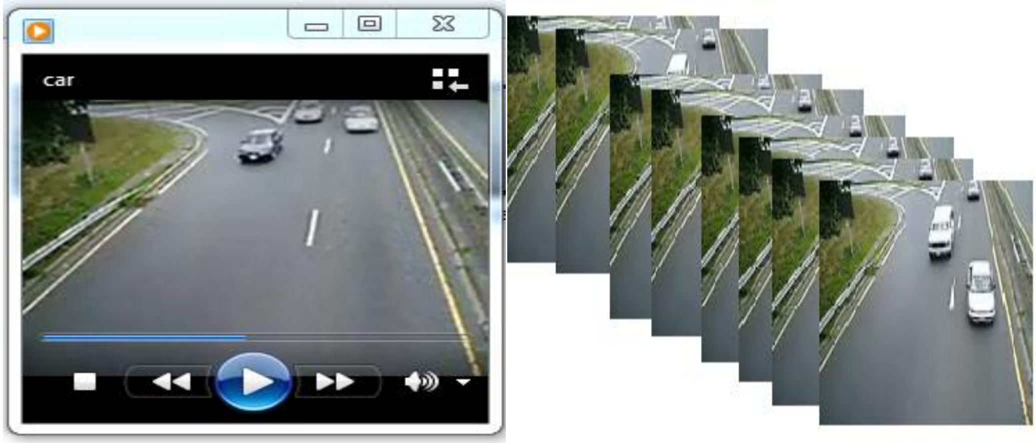
a) b)

Figure 4. Girl video, a) input video b) Frames from Girl video



a) b)

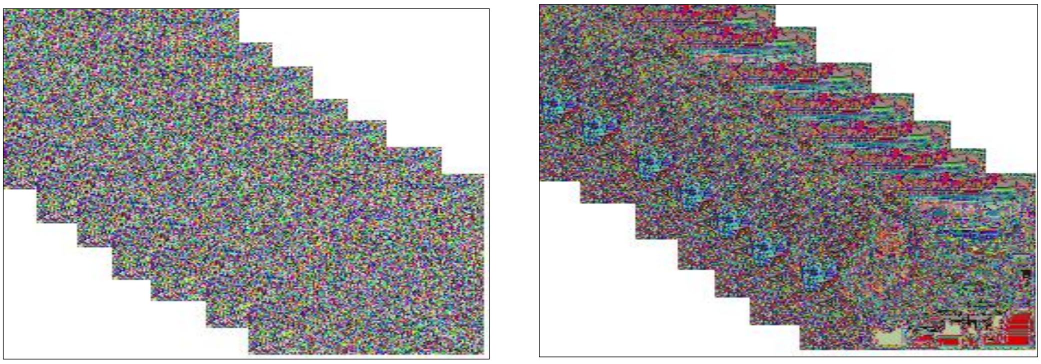
Figure 5. Scooter video, a) input video b) Frames from Scooter video



a) b)

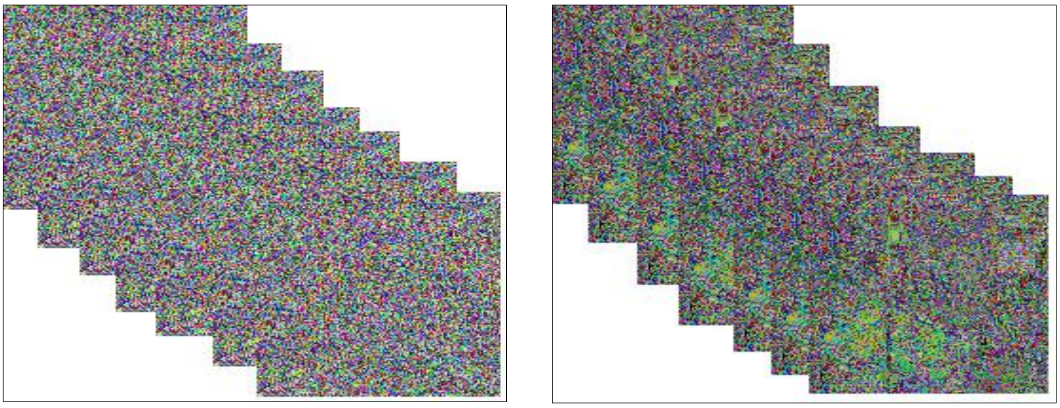
Figure 6. Car video, a) input video b) Frames from Car video

2. In the second step, the adaptive encryption key is extracted from the main diagonal of each frame that is used with the CAST method. CAST-128 and RSA encryption methods are applied to the video frames as shown in Fig. 7 for girl frames, Fig. 8 for scooter frames and Fig. 9 for car frames.



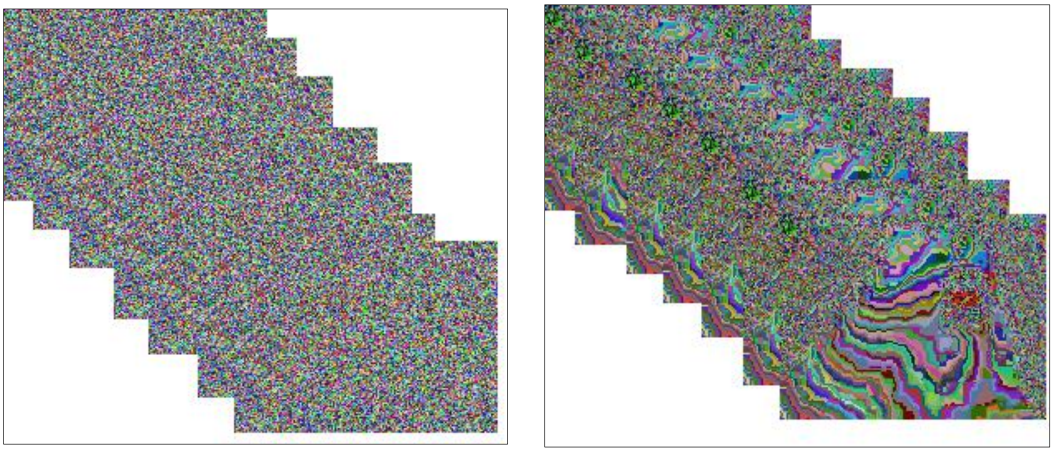
a) b)

Figure 7. Girl Frames after Encryption by a) CAST-128 method b) RSA method



a) b)

Figure 8. Scooter Frames after Encryption with a) CAST-128 b) RSA



a) b)

Figure 9. Car Frames after Encryption with a) CAST-128 method b) RSA method

3. In the third step, the entropy value is calculated for each frame which is encrypted by both CAST-128 with adaptive key and RSA. Entropy is a measure of disorder or randomness, and hence a measure of uncertainty. Thus, entropy can be considered as an assessment criterion for the significance of ciphering technique. The higher the entropy, the better the encryption algorithm. Entropy values for a sample frame of tested videos can be illustrated in Table 2.

Table 2. shows the comparison results between encryption with RSA and encryption with CAST-128 for samples of videos in terms of highest average entropy per byte of encryption.

		Average entropy of encryption with the methods	
Video name	**Frame No.**	**CAST-128 with adaptive key**	**RSA**
Girl	Frame1	2581.921	2271.829
	Frame20	2702.009	2399.003
	Frame 90	2492.229	2007.060
Scooter	Frame 5	2569.814	2282.844
	Frame11	2397.317	2089.014
Car	Frame 26	2697.407	2250.303
	Frame 30	2435.188	2197.668
	Frame 50	2723.317	2338.905
	Frame 101	2556.587	2299.092

Table 2 shows that CAST-128 with adaptive key scores highest average entropy with encryption .An entropy is a scale stage of randomness for information. Randomness is an important and highly demanded characteristic of cryptographic algorithms.

Limitations

There are different limitations of using RSA and CAST-128 as illustrated bellow:-

1. The main limitation of using RSA is that the security of (RSA) deepens on the functional difficulty of product's factoring of two great prime numbers.
2. The main limitation of using CAST-128 is that via of a renowned plain text attack, CAST 128 Key may be known via cryptanalysis linearly. It can be cracked via (2^17) selection plain-texts over one related key query within offline action of (2^48).

Conclusion:

The aim of this research is to compare between CAST-128 encryption method and RSA encryption method for video frames to find the best encryption method based on entropy value and determine the more accurate encryption method for highest entropy. The first method applied the "CAST-128 encryption method" and the second method applied the "RSA encryption method". CAST-128 utilizes a pair of sub-keys for each round as a quantum of five bits was utilized as a key of rotation to each round and a quantum of 32 (bits) was utilized as a key of masking into a round. RSA is a public-key cryptographic technique which can be known as (asymmetric) cryptography. An asymmetry of a key depends on factoring a product of two big prime values. For example, the entropy value of a sample of a girl video is 2581.921 when using CAST-128 encryption method, while it is 2271.329 when using the RSA encryption method; also the entropy value of a sample of scooter video is 2569.814 when using the CAST-128 encryption method, while it is 2282.844 when using RSA encryption method.

Authors' declaration:

- Conflicts of Interest: None.
- We hereby confirm that all the Figures and Tables in the manuscript are mine ours. Besides, the Figures and images, which are not mine ours, have been given the permission for re-publication attached with the manuscript.
- Ethical Clearance: The project was approved by the local ethical committee in University of Technology.

Authors' contributions statement:

E.T. K. wrote the research in the primitive image (the theoretical part). E.F. N. collected the samples of videos, extracted all frames from each video and then analyzed all colors for encryption (practical part of manuscript). A. N. M. did the interpretation, drafting the MS, revision, and proofreading.

References

1. Babatunde A., Jimoh, R., Abikoye O., Isiaka B. Survey of Video Encryption Algorithms. Int. J Inform Comm Tech. 2017; 5(1):65-80.
2. Ghodke M., Mali N. FPGA Based network security using cryptography. Int J Eng Tech. 2016; 3(3):469-471.
3. Bhoopal R., Shaik A. Design of cryptographically secure AES like S-Box using second-order reversible cellular automata for wireless body area network applications. Heal C Tech Let. 2016 Sep 22; 3(3):177–183.
4. Zhang Y. The unified image encryption algorithm based on chaos and cubic S-Box, J Comp Math Data Sci. (CMDS).2018;450:361-377.
5. Mohit K, Akshat A, Ankit G. A Review on Various Digital Image Encryption Techniques and Security Criteria. Int J Comp Appl. 2014 July 22; 96(13):19-26.
6. Noor A, Mokhtar M. Combining Several Substitution Cipher Algorithms using Circular Queue Data

Structure. Baghdad Sci J.2020; 17(4):1320-1327. https://doi.org/n 10.21123/ bsj.2020 .17.4.1320.

7. Shaikh A, Kaul V. Enhanced Security Algorithm using Hybrid Encryption and ECC, IOSR J Comp Eng. 2014 Jun;16(3) 80-85.
8. Kritika A, Manisha S, Sanjay B. Analysis of Cryptographic Algorithms for Network Security, Int J Comp Appl Tech Res. 2014; 3(2) : 130-135.
9. Karolin M, Meyyappan T. Image Encryption and Decryption using RSA Algorithm with Share Creation Techniques , Int J Eng Adv Tech. 2019; 9(2): 2797-2800.
10. Ibrahem M, Hamood L. Video Encryption Based on Chaotic System and Stream Cipher, Iraq. J Inform Comm. Tech. 2018; 1(2): 33-40**.**
11. Malladar R, Kunte S. Selective Video Encryption Based on Entropy Measure, Integrated Intelligent Computing, Communication and Security. Springer Nature Singapore Pte Ltd, 2019: 603-612.
12. Cheng S, Wang L, Ao N, Han Q. A Selective Video Encryption Scheme Based on Coding Characteristics, Symmetry. 2020; 12(3): 332.
13. Vivek P. Bharat M. Performance Comparison of Various Cryptographic Algorithms Along with Energy Consumption in Wireless Sensor Network. Int J Sci Tech Res. 2020; 9(3): 77-86.
14. Abdel-karim S, Hassan A, Naglaa F. Modifications on RSA Cryptosystem Using Genetic Optimization. Int J Res Appl Sci.2014; 19(2): 150 -155.
15. Shailaja S, Dr .Krishnamurthy G. Comparison of Blowfish and Cast-128 Algorithms Using Encryption Quality, Key Sensitivity and Correlation Coefficient Analysis. Amer J Eng Res. .2014; 3(7): 161-166.
16. Enas T, Ekhlas F. Image encryption and decryption using CAST-128 with proposed adaptive key, Coll Educ J. 2019; 5: 89-100.
17. Zhao J., Wang M., Wen L. Improved Linear Cryptanalysis of CAST-256. J Comp Sci. Tech. 2014;29(6): 1134-1139.
18. Rekha C, Krishnamurthy G. An Optimized Key Scheduling Algorithm for CAST -128 using dynamic substitution S-box. Int J Recent Tech Eng. 2019 Sept.; 8(3): 2585-2590.
19. Thippanna G. A Re-Examine on Assorted Digital Image Encryption Algorithm’s Technique. Bios Biomet J. 2018 Jan. 17; 4(2): 1-8. https://doi.org/10.19080/BBOAJ. 2017.04.55563.
20. Zoran H, Druga G, Varadin C. Comparative Analysis of Cryptographic Algorithms, Int J Digit Tech Econ. 2016 Dec. 15; 1(2):127-134.
21. Ahmad S, Shamma M, Alkhatib A. RSA Algorithm with a New Approach Encryption and Decryption Message Text by ASCII. Int J Crypt Info Sec. 2015 Dec; 5(3): 23-32.
22. Shankar K. An Optimal RSA Encryption Algorithm for Secret Images. Int J Pure Appl Math. 2018; 118(20): 2491-2499.
23. Priyadarshini P, Prashant N, Narayan D, Meena S, A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish . Int J Conf Info Sec Priv. 2016; 78(2016): 617-624.
24. Sahu J, Singh V, Sahu V, Chopra A. An Enhanced Version of RSA to Increase the Security. J Net Comm Eng Tech. 2017; 7(4):1-4.
25. Khadeeja G, Saif M, Majid J. Improved Image Security in Internet of Thing (IOT) Using Multiple Key AES. Baghdad Sci J. 2021; 18(2): 417-429. https://doi.org/ 10.21123/ bsj.2021.18.2.0417

مقارنة بين RSA و CAST-128 مع المفتاح المتكيف لتشفير إطارات الفيديو بأعلى متوسط إنتروبيا

أيناس طارق خضير **أخلاص فالح ناصر** **علاء نوري مزهر**

قسم علوم الحاسوب, الجامعه التكنولوجيه, بغداد, العراق.

الخلاصه:

يقوم تشفير البيانات بترجمة البيانات إلى شكل أو رمز آخر يتيح للأشخاص فقط الوصول إلى المفتاح السري أو يمكن قراءة كلمة المرور. يشار إلى البيانات المشفرة عمومًا باسم النص المشفر، بينما يمكن أن تُعرف البيانات غير المشفرة النص الصريح. يمكن استخدام الإنتروبيا كمقياس يعطي عدد البتات التي يمكن أن تكون مطلوبة لتشفير بيانات الصورة. نظرًا لأن قيم البكسل داخل الصورة يتم توزيعها من خلال مستويات رمادية أخرى ، فإن الانتروبيا تزداد. الهدف من هذا البحث هو المقارنة بين طرق التشفير CAST-128 و RSA لإطارات الفيديو لتحديد الطريقة الأكثر دقة مع أعلى إنتروبيا. يتم تحقيق الطريقة الأولى من خلال تطبيق "طريقة CAST-128" ويتم تحقيق الطريقة الثانية من خلال تطبيق "طريقة RSA". يستخدم CAST-128 زوجًا من المفاتيح الفرعية لكل دوره كمقدار من خمسة بتات تم استخدامها كمفتاح دوران لكل دوره وكمية 32 (بت) تم استخدامها كمفتاح إخفاء في الدوره. يمكن استخراج المفتاح المتكيف المقترح ذات 128 بت من القطر الرئيسي لكل إطار قبل التشفير RSA هي تقنية تشفير ذات مفتاح علم يمكن أن تُعرف باسم التشفير (غير المتماثل). يعتمد عدم تناسق المفتاح على تحليل حاصل ضرب قيمتين أوليتين كبيرتين. تم تطبيق المقارنة على العديد من مقاطع الفيديو وأظهرت النتائج أن طريقة CAST-128 أثبتت أعلى درجة من الانتروبيا حتى لو كانت الإطارات تحتوي على الكثير من البيانات المشوهة أو وحدات بكسل الصورة غير الواضحة. على سبيل المثال، قيمة الانتروبيا لعينة فيديو فتاة هي 2581.921 عند استخدام طريقة CAST-128، بينما تكون 2271.329 عند استخدام RSA؛ كما أن قيمة الانتروبيا لعينة فيديو سكوتر هي 2569.814 عند استخدام CAST-128 ، بينما تبلغ 2282.844 عند استخدام RSA.

الكلمات المفتاحيه: المفتاح غير المتماثل ، CAST-128 ، التشفير ، RSA ، المفتاح المتماثل