© 2019 IJSRSET | Volume 6 | Issue 5 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology
DOI : https://doi.org/10.32628/IJSRSET196550

Subject Review : Key Generation in Different Cryptography Algorithm

Zainab Khyioon Abdalrdha*, Iman Hussein AL-Qinani, Farah Neamah Abbas
Department of Computer Science, Collage of Education, University of Mustansiriyah, Baghdad, Iraq

ABSTRACT

The importance of encryption in most organizations, therefore, it became necessary to encrypt data because data security is an essential component in order to maintain the security of data and information in various institutions. Encryption also helps to ensure the confidentiality and integrity of data during transmission through communication channels. Given the importance of the keys used in encryption as a key part in the strength of the algorithm and increase its security in most encryption algorithms, thus generating the key in many research the most important part in data encryption and its importance lies in the non-duplication of keys to ensure better results and theoretically impossible to break. In this paper, we try to describe and review many of the papers that were used to create the keys and compare them with each other.

Keywords: Public Key Cryptosystems, Private Key Cryptography, AES, Triple DES and RSA

I. INTRODUCTION

It is necessary to provide a secure transfer of information between the sender and the recipient, so the process of encryption is one of the mechanisms that provide information security when data is transmitted, a secure method must be provided because today security has become an important resource for most efficient operations of various requirements of any organization. The main purpose of security is to transfer important and sensitive information protected and unreadable only by authorized or recipient persons [1].

Data protection is an important way to provide a powerful tool is the use of encryption, which depends on many of the security mechanisms in the process of encryption and decryption of information. Encryption allows us to store sensitive data securely or transmit it over networks that are insecure that cannot be understood by anyone just the recipient (Kahn, 1967). To gain privacy, integrity and data integrity, the use of encryption is a powerful tool. Encryption distinguishes between two types of public encryption and private encryption, which has an ancient history, one secret key is used for encryption and decryption in this symmetric encryption and two keys are used in asymmetric encryption, one public and the other private. However, asymmetric encryption is one of the coding techniques, which is 1000 times slower than analogy, because it requires more computational processing [2].

The key resists cryptanalysis whenever the key is strong as it resists even against the attacker who detects all system information related to the creation or verification of the encryption key. The rest of this paper is arranged as follows: In Section 2, the

literature survey of some of the schemes proposed in the last decade. In section 3, comparative analysis of the schemes discussed. Finally, the conclusions are presented in section 4.

II. LITERATURE SURVEY

A.J and K.D in this paper [3], proposed an iris-based and fingerprint-based approach to creating a secure encryption key. This approach consists of three modes: extract features, create a biometric template, and create an encryption key. In the initial stage, the features, points and characteristics of the fabric are extracted from fingerprints and iris images respectively; after that, the resulting features are combined together at the feature level to create a multi-template biometrics. Finally, a secure encryption key produces 256 bits of biometrics. For multi-template experimentation.

In this paper S. V., K. G and M Lal [4], introduced a technique to produce a fingerprint unlock able key to overcome these problems. The flexibility and reliability of encryption is enhanced by the use of extensible biometric features. There are many biometrics systems that handle encryption, but the proposed revocable biometric system offers a new way to create an encryption key.

In this paper Z. Paral, and S.Des [5], described the reliability and sequencing of bits and their use with cryptography as a key using non-challenging physical function circuit elements. This method reflects the traditional model of using general challenges to create secret PUF responses where the key is collected from a series of small integers that are a series of indexed bits produced by PUF circuits (circles); then a unique PUF pattern is stored in each indicator continuously between Provisioning and all future generations of keys. To retrieve integers, the results of the newly repeated PUF string are searched on the highest inventory probability of matching patterns. This means that complex debug logic is not required as BCH decoders. The method only reveals data for relatively short PUF outputs in the general store, which frustrates the chances of modeling attacks.

Asst. Prof. R. M. and S. S in this paper [6] , used here to establish a public secret key across the network channel depending on the neural networks to be used in the neural encryption across two connected networks where these networks receive an input vector, including generate output bit and then be trained according to this bit and through the two networks and vectors weighing show a new phenomenon depending on the time used where networks synchronize the key is used to send information across the channel and its mission is to encrypt and decrypt the transmitted information

Chen Hong et al. to reduce the time and space complexity [7], provided a method for generating a public key encryption system. This method developed the keys by using the generator to generate a random number, then used Miller Rabin's algorithm to perform a preliminary test and then used the Stain algorithm to generate public and private keys.

R. S. D, A. K. G and P. Sh in this paper [8], Use the added homomorphism properties to modify the RSA algorithm and call it the modified RSA algorithm (MREA). MREA relies on the problem of factoring in addition to the assumptions of the critical compound residue which is the impossibility hypothesis for this security has become better compared with RSA. This method, which is an additional cryptographic system, where the encryption of C1 + C2 can be calculated with the public key and in terms of performance and safety, this modified method MREA better than the RSA algorithm.

S A. N and S. A in this paper [9] Introduced in this method to speed up the implementation of the RSA algorithm during the process of transferring data

between different networks and the Internet, a program developed in C # was used to generate keys are saving in databases that are created by SQL Server 2008 R2. These keys are used before the RSA algorithm is used, and the key creation phase stored in the RSA-Key Generations Offline databases is called an inevitable phase that is implemented in each portal before using this algorithm. If the database matches the algorithm, it must be used in all network gateways, and the process of controlling the database through a special protocol programmed in C # called RSA Handshake Database Protocol, and the work of this protocol is to control each gateway runs RSA-key generations offline .Here is a new process for exchanging key values between gateways, which is the exchange of indexes to fields in the table that contain public and private key values stored inside the database before beginning the encryption and decryption process using the RSA algorithm, rather than using the real value exchange, n and e and d.

Ra. H and S. H. H. S. in this paper [10], described how the key is generated from the image and the key generated is used in the encryption of the AES algorithm, after which the watermark key is encrypted in the image and the S-Box generated for this key makes the AES algorithm more robust and more reliable.

Ch.T and V.R in this paper [11], a new variant of the RSA algorithm is proposed, which characterized from the way the keys are created from the standard RSA. This research relied on standard RSA, N Prime RSA and Dual RSA to generate PA's PSA key and security analysis. Finally, Pell's RSA application, Blind signatures, has been proposed.

Ma Wil, I. M, and Je B. S in this paper [12], in this work, a protocol for the creation of a switch based on the method of selecting the frequency of the multipath channels is presented. This system is characterized by the fact that it does not require the movement of the device during the generation of the key and hence the repetitive state of this sensor network with fixed nodes. This protocol is through durability and security as a result of the experiments that have been applied to it.

G.M, S., R., V.V in this paper [13], presented a method for generating the key is using a similar structure of the alphabetical frame and is composed of a special character set based on the Triple DES algorithm for experimental purposes, which is characterized by a random block-based security block and ease of execution and to avoid image distortion due to transmission noise problems during transmission of the image to the recipient to create the key.

P.M, L K.R, Li. C and Jo S. K in this paper [14] This work presented a method to generate the key depending on the color image where the use of three-color channels of images, namely red, green and blue RGB and rely on the colors mentioned to generate the key There are many algorithms that exist to encrypt and decrypt user messages around the world, but the process of creating a user key for encryption must be a difficult task. To protect messages from the intruder you must take steps forward to protect this key by creating a secret key based on session-style images. The proposed algorithm will work better than the methods used to create traditional keys and the RC5 algorithm was used to encrypt messages.

O. K. Jasim M in this paper [15], provided an evolution to the key generation of the Advanced Encryption Standard (AES) algorithm, where the development is between AES-based SES, the specific secret key generated from the quantum key distribution process, and the symmetric encryption algorithm is a prominent algorithm.

In this paper Li, G., Hu, A., Z, Y., Pe, L., & Va, M [16], presented a real time suggestion in the time-

varying TDD channel where a log field differential (LDD) was used and the results were analyzed in terms of the mean square error (MSE) between the special channels between Alice and Bob and the effective error-to-error ratio (ESER) to evaluate performance. The analysis shows that the proposed conversion can eliminate the effect of HFD, however an improved noise reduction technique has been improved, and numerical results show that the proposed LDD conversion provides similar performance to the ideal condition without HFD, and therefore, can be used as a simple, flexible and practical solution to generate The secret key in the TDD channel over time.

This paper A. Ab, Ka A., E K. El, and Ah A. E [17], presented a way to create a key through the use of an evolutionary algorithm (EA) which is characterized by being intelligent dynamic as a seed, and the proposed method tends to promote RC4 with a high degree of randomness key. This was the secret key to create dynamically and this random key feature of the way RC4-EA is proposed and this will increase the strength of encryption algorithm RC4 against breaking the encryption. Numerous experiments were conducted on this proposed algorithm and the results showed improved RC4-EA encoding time and decoding. The proposed RC4-EA was used to encrypt the data in the Content Management System (CMS).

A. M., H. D and M S. [18], provided an idea in the encryption and key generation process where a 256-bit biometric external key is used to derive the initial seed of the chaotic maps applied where encryption is based on a messy basis that includes both the logistical chaos map and the tent map. Iterative using a data-based feedback mechanism that blends existing encryption parameters with previously encoded pixels. Accordingly, the relationship between the original and the encrypted image is confused and the proposed encryption can withstand any attack.

In this paper, S M. H and H [19], presented the use of a DNA-based algorithm to generate strong encryption for symmetric encryption applications. To generate an encryption key, four vectors (A, C, G, and T) generated by a private key input are used to create an n-size permutation. This can continue as much as new cryptographic keys require as rules created with the same flipping bus are recreated and reprocessed to identify new cryptographic keys.

P. L, E. B, A. S and A. E [20] Several simulation experiments were conducted to estimate the efficiency of these methods, and the best criteria for fuzzy extracts with a 192-bit key length were: FRR = 0.061, FAR = 0.023.

In this paper, P. G, S. U, G. S, N. B and R. S [21], presented both the AES and ECC algorithms and the private key is generated depending on these two algorithms. In general, AES has a key length of 128 bits with 10 times of redundancy so that users' operations will not get effective security, to increase the security level as 196 bits are used with 12 times of redundancy over the key. Through this development, users' operations can be highly secure and their data can be kept confidential.

A. Arya in this paper [22], introduced the use of Triple DC algorithm, which is safe to protect data by the intruder. This is necessary to ensure that the data remains safe. The algorithm specifies the mathematical steps necessary to convert data into data encryption and decryption.

W. Abed Sr in this paper [23], Generated of the key depending on the color image, where it relied on the color of the image where the frequencies of colors are taken by taking the frequency of the blue color as a maximum and then blow the number and the implementation of the scientific establishment of the key. Next, the private key is created and we choose the color image cover to hide text in this specific cover to test a suggested method for creating the private key and the masking process is done in the LSB segment which is the least important bit. Finally, the generated key is tested by hiding the process and changing the image extension.

A. Ostad, D. A & M. Nik in this paper [24], introduces the use of a new authentication protocol between the user and the session key agreement that is made via secure communication channels in TMIS. The result of analyzes used showed that this protocol provided security and performance and can solve the security barrier.

In this paper, R. Saha, G. Geetha, G. Kumar, and T. Kim [25], introduced the use of a symmetric random function constructor (SRFG). The process of generating keys in block coding is something new in this area. Depending on the AES algorithm the results showed that this method is robust against resistance to AES attacks

III. COMPARATIVE ANALYSIS OF THE SCHEMES

In section show the table 1: (Comparison of key generation systems in Various Cryptography) will explain the comparison among previous systems.

IV. CONCLUSION

In this paper, we reviewed a different key generation for different algorithms for the period (2010-2018). We discussed security for key generation, a literary study review and a paper from some authors where methods are compatible with any type of algorithm. Our future work is to review and scan the paper literature for image coding in a different encryption and compare it to the traditional encryption system. When reviewing the proposed research on key creation in several types, we observed the efficiency and security of algorithms used in all types of Algorithms. This review of the paper literature survey provides a brief description and analysis of algorithms and provides some assistance in improving encryption systems to ensure network security.

V. ACKNOWLEDGMENT

The authors would like to thank AL_Mustansiriyah University (www.uomusiriyah.edu.iq), Baghdad-Iraq for its support in the present work.

VI. REFERENCES

[1]. M. Nagendra & M. C. Sekhar, (2014)."Performance Improvement of Advanced Encryption Algorithm using Parallel Computation", International Journal of Software Engineering and Its Applications Vol.8, No.2, pp. 287-296.

[2]. Hardjono T. and Dondeti L. (2005). Security in Wireless LANS and MANS (Artech House Computer Security). Artech House, Inc., Norwood, MA, USA.

[3]. A.Jagadeesan and Dr. K.Duraiswamy, (2010). "Secured Cryptographic Key Generation from Multimodal Biometrics: Feature Level Fusion of Fingerprint and Iris, (IJCSIS) International Journal of Computer Science and Information Security, Vol. 7, No. 2, February 2010.

[4]. Sunil V. K. Gaddam and Manohar Lal, (2010). "Efficient Cancellable Biometric Key Generation Scheme for Cryptography", International Journal of Network Security, Vol.11, No.2, PP.61-69.

[5]. Zdenek (Sid) Paral, and Srinivas Devadas, "Reliable and Efficient PUF-Based Key Generation Using Pattern Matching", 978-1-4577-1058-2/11/$26.00c 2011 IEEE.

[6]. R. M.Jogdand and Sahana S.Bisalapur, (2011). "Design of An Efficient Neural Key Generation" International Journal of Artificial Intelligence & Applications (IJAIA), Vol.2, No.1.

[7]. Li Dongjiang, Wang Yandan, Chen Hong, (2012). "The research on key generation in RSA public- key cryptosystem", pp. 578–580.

[8]. Ravi Shankar Dhakar, Amit Kumar Gupta and Prashant Sharma, "Modified RSA Encryption Algorithm (MREA)", 2012 Second International Conference on Advanced Computing & Communication Technologies.

[9]. Sami A. Nagar and Saad Alshamma, "High Speed Implementation of RSA Algorithm with Modified Keys Exchange", 2012 6th International Conference on Sciences of

Electronics,Technologies of Information and Telecommunications (SETIT).

[10]. Razi Hosseinkhani and Seyyed Hamid Haj Seyyed Javadi, (2012). "Using image as cipher key in AES", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 2.

[11]. Chandra segar T and Vijayaragavan R "Pell's RSA key generation and its security analysis" IEEE – 31661, July 4 - 6, 2013, Tiruchengode, India.

[12]. Matthias Wilhelm, Ivan Martinovic, and Jens B. Schmitt, (2013). "Secure Key Generation in Sensor Networks Based on Frequency-Selective Channels", Ieee Journal on Selected Areas in Communications, Vol. 31, No. 9.

[13]. G.Manikandan, S.Ramakrishnan, R.Rajaram, V.Venkattesh, (2013)."An Image Based Key Generation for Symmetric Key Cryptogrpahy", International Journal of Engineering and Technology (IJET), Vol 5 No 3.

[14]. Priyanka.M, Lalitha Kumari.R, Lizyflorance.C and John Singh. K, (2013). "A New Randomized Cryptographic Key Generation Using Image", International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 6.

[15]. Omer K. Jasim Mohammad, (2014). "Innovative Method for enhancing Key generation and management in the AES-algorithm" 2014, DOI: 10.5815/ijcnis.2015.04.02.

[16]. Li, G., Hu, A., Zou, Y., Peng, L., & Valkama, M. (2015). "A Novel Transform for Secret Key Generation in Time-Varying TDD Channel under Hardware Fingerprint Deviation"., IEEE 82nd Vehicular Technology Conference (VTC2015-Fall). doi:10.1109/vtcfall.2015.

[17]. Ashraf Aboshosha, Kamal A. ElDahshan, Eman K. Elsayed, and Ahmed A. Elngar, (2015)." EA Based Dynamic Key Generation in RC4 Ciphering Applied to CMS" International Journal of Network Security, Vol.17, No.4, PP.405-412.

[18]. Ali M. Meligy, Hossam Diab and Marwa S. El-Danaf, (2016). "Chaos Encryption Algorithm using Key Generation from Biometric Images", International Journal of Computer Applications (0975 – 8887) Volume 149 – No.11.

[19]. Shakir M. Hussain and Hussein Al-Bahadili "A DNA-Based Cryptographic Key Generation Algorithm", 338 Int'l Conf. Security and Management, SAM'16.

[20]. Pavel Lozhnikov, Ekaterina Buraya, Alexey Sulavko and Alexander Eremenko "Methods of generating key sequences based on keystroke dynamics", 2016 Dynamics of Systems, Mechanisms and Machines (Dynamics), Date of Conference: 15-17 Nov. 2016.

[21]. P. Gayathri, Syed Umar, G. Sridevi, N. Bashwanth, Royyuru Srikanth, (2017). "Hybrid Cryptography for Random-key Generation based on ECC Algorithm", International Journal of Electrical and Computer Engineering (IJECE) Vol. 7, No. 3, pp. 1293~1298.

[22]. Akhil Arya, (2017). "Security Enhancement Using Triple Des Algorithm ", Computer Science Department, IIMT College of Engineering, Greater Noida, IJCSMC, Vol. 6, Issue. 4, April 2017, pg.353 – 355.

[23]. Wisam Abed Shukur, (2017). "A Proposed Method for Generating a Private Key Using Digital Color Image Features", International Journal of Applied Engineering Research ISSN 0973-4562, Volume 12.

[24]. Arezou Ostad-Sharif, Dariush Abbasinezhad-Mood1 & Morteza Nikooghadam, "A Robust and Efficient ECC-based Mutual Authentication and SessionKey Generation Scheme for Healthcare Applications" Received: 28 June 2018 /Accepted: 6 November 2018, Springer Science-Business Media, LLC, part of Springer Nature 2018.

[25]. Rahul Saha G. Geetha, Gulshan Kumar, and Tai-hoon Kim, (2018)." RK-AES: An Improved Version of AES Using a New Key Generation Process with Random Keys" Hindawi Security

and Communication Networks, Article ID 9802475,11pageshttps://doi.org/10.1155/2018/9802475.

Cite this article as : Zainab Khyioon Abdalrdha, Iman Hussein AL-Qinani, Farah Neamah Abbas, "Subject Review : Key Generation in Different Cryptography Algorithm", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 6 Issue 5, pp. 230-240, September-October 2019. Available at doi : https://doi.org/10.32628/IJSRSET196550
Journal URL : http://ijsrset.com/IJSRSET196550

TABLE 1. COMPARISON OF KEY GENERATION SYSTEMS IN VARIOUS CRYPTOGRAPHY

No. Ref	Algorithm	Key Size	Flexible	Features	Method of Key Generation
[3]	multimodal biometrics	256-bit	Efficiency	The results show good efficacy for iris images and fingerprints for different people	Iris and fingerprint
[4]	AES Encryption/ Decryption algorithm and Fingerprint.	128, 192, 256 bits	Yes	Excellent Security	The use of extensible biometric features to generate Cryptographic Key.
[5]	Sequencing of bits and their use with cryptography as a key using non-challenging physical function circuit elements	/	Efficiently and reliably Faster and raised security level Increase the number of PUFs.	Responses for the lack of security risk we had to use 4-XOR Referee PUF	Keys can be generated reliably and efficiently using our scheme in the face of extreme environmental variability.
[6]	Neural Networks	A public secret key	/	Synchronization depending on mutual learning.	Generating a public secret key between the sender and the recipient and agreed upon through a public channel to the two partners.
[7]	RSA, Miller Rabin's & Stain algorithms	128 bits	The results showed that the efficiency of RSA key generation was effectively improved.	/	The RSA keys are generated based on the Miller-Rabin algorithm and Stain algorithm
[8]	Modified RSA Encryption Algorithm (MREA).	256, 512, 1024, 2048	In terms of performance and safety, this modified method MREA better than the RSA algorithm.	/	Time of Key generation (ms) is 172, 484, 625, and 8125.

[9]	RSA algorithm	RSA-key generations offline algorithm	Process time is 2.5 and is faster than generations of online RSA keys	/	Generate RSA-Key Offline in the generated database and save all key values in tables.
[10]	AES algorithm	128 bit	The keys generated from the same image were compared with a difference of opacity, where it was noted that a picture with opacity is 1% lighter than the first image. We find 253 differences between S-Box1 and S-Box2, bringing about 99% of the second S-Box changed.	/	Generated key from the image.
[11]	RSA Algorithm	RSA, RSA for N Prime, and Dual RSA	The Pell equation shown by using various key parameters was implemented to create an effective public key cryptographic system.	The proposed RSA assessment is evaluated using the RSA standard	Create RSA key for PELL and its security analytics through Standard RSA, N Prime RSA and Dual RSA.
[12]	Presented in this protocol key generation work to create a key	/	The error correction in the protocol worked to mitigate the impact of the measurement error and effects resulting in a compatibility rate of no more than 97%.	Provide secrets of up to 50 bits in this proposed protocol	Key generation depending on the master protocol relies on frequency selectivity for multipath channels.
[13]	Triple DES algorithm	192 bits	This type of approach to key generation with a shared and dynamic approach reveals difficult and effective tracking because image capture from websites is only valid for one day.	The key that is generated is inherently dynamic This is an important feature of the algorithm	A proposed new image-based algorithm that is dynamic and challenging and avoids sharing keys such as transmission noise and brute force attack

[14]	RC5 algorithm using to encryption of the message & to generate the key depending on the colour image where the use of three-color channels of images, namely red, green and blue RGB	Created keys with variable lengths depending on the resolution of the images, the key is difficult to break	The method used greatly reduced the complexity of the key and this is an efficient point	/	The generated key differs because it uses time-dependent sessions to select the image responsible for key generation and the generation process will be created depending on the encryption time
[15]	QAES Algorithm	128, 192, 256 bits	- Experimental results and analysis show the following: The QAES algorithm produces keys that are difficult for attackers to predict because they are more complex and unbreakable than those generated by AES. - The ability to generate a high percentage of independence and the use of algorithms NIST tests this ability lies a point of strength and efficiency in the algorithm QAES.	- A safer environment is achieved against various cryptographic analysis attacks. This is achieved using the QAES algorithm, which is considered flexible in the algorithm. - The result of the AES and QKD integrations is where the detection of the QAES symmetric encryption algorithm is detected. - Because the quantum key is generated, the QAES encryption speed will be very slower (0.409 seconds) than using AES	Generate the key from the quantum key distribution process
[16]	using the Hardware Fingerprint Deviation (HFD) problem	The key creation rate indicates the length of the key that was created	An effective analysis technique was used to reduce noise and motion effect on the design parameters	It is particularly suitable for creating secret keys in the wireless system under medium or high media	To provide adequate key generation in TDD
[17]	RC4-EA method	128, 256 bits	Creating a random secret key will increase security based on RC4-EA	To keep this data in authentication, RC4-EA has been applied to encrypt data in	To generate a random secret key, the EA method is used to generate the dynamic key as a seed for RC4.

			and this is the main advantage	CMS.	
[18]	Chaos based encryption techniques	256-bits	- The proposed model has sufficient durability and is effective against common attacks. - High efficiency of the proposed algorithm.	The proposed method for generating an external secret key using a biometric secret image is described as being highly flexible	The key generation and encryption method depend on each pixel and previous encrypted information and for chaotic maps.
[19]	DNA	To generate a key uses four vectors generated from a private key input to create the volume n and vectors generated from this permutation are four which are processed mathematically using a linear formula and the key is created	Always generated encryption keys have an Entropy 0.7 and an ideal operating length of 0 and 1 for all key lengths and an acceptable average length of operation. For a 48-bit encryption key, it provides a maximum 14% operating length of 0 and 9% for 1, and an average operating length of 4% for both 0 and 1. These parameters decrease with increasing key length.	/	Use the algorithm as a cryptographic key generator depending on DNA
[20]	To create encryption keys and password is built on the basis of the parameters of the keystroke dynamics.	192 bits	The validity of the study is 0.99, the confidence period is 0.02.	/	A 192-bit key creation method has been developed, based on keystroke dynamics
[21]	Combine between AES & ECC algorithms	AES, key length 128, 196 bits	Provides a high level of security and efficiency for the user and keeps their data	/	Using the AES and ECC algorithms, the private key was created

			confidential.		
[22]	Triple DES Algorithm	Three times of key size is 192 bits	Their main size is important, they are very effective against brute force attack	/	Key generation based on Triple DES Algorithm
[23]	Create a special key depending on the colours of images such as blue	/	- After the concealment, various types of noise such as Gaussian, etc. are added. - To test the encryption key, we use watermark technology in the image cover, and we check the image quality performance to show the contrast in the original and retrieved images using NC, PSNR and MSE as quality measures.	The use of color image characteristics in terms of color frequency to create an encryption key in the encryption system is a new idea and a clarity and high flexibility.	The process of generating a special key from the characteristics of a digital color image such as color (red, green and blue); which is done by calculating the color frequency and then taking the maximum blue color and a stroke by its number and performs the addition process to produce the generated key.
[24]	Use a protocol to authenticate between the user and the session key agreement in TMIS	/	Perform the protocol he is highly efficient.	/	High security protocol in terms of keys
[25]	Advanced Encryption Standard (AES)	AES-256 bits using the SRFG	RK-AES is an efficient in all respects of encryption algorithms as a result of random application in this generation	Results indicate that RK-AES has a noise characteristic compared to the original AES which is three times better and 53.7% than avalanches	The time it takes to generate a key, which generates an exchange between security and time, is an important element of the key generation process