PRINT ISSN 1119-8362
Electronic ISSN 2659-1499

Full-text Available Online at
https://www.ajol.info/index.php/jasem
https://www.bioline.org.br/ja

J. Appl. Sci. Environ. Manage.
Vol. 28 (10) 3013-3018 October, 2024

Proposition of a Better Data Security Model for a Protective Information Exchange on the Internet with Advanced Steganographic and Cryptographic Algorithm.

*[1]ABDULLAHI, YY; [2]FAROUK, LG; [3]NUR, AS; [4]SALE, A

*[1]*North-Eastern University, Gombe, Gombe State, Nigeria*
[2]*Federal University Dutse, Dutse, Jigawa State, Nigeria*
[3]*Nile University of Abuja, Abuja, Nigeria*
[4]*Binyaminu Usman Polytechnic, Hadejiya, Jigawa State, Nigeria*

**Corresponding Author Email: Email: yahayaabdullahi565@gmail.com*
**ORCID: https://orcid.org/0009-0000-7350-1269*
**Tel: 08035987089, 09065952760*

Co-Authors Email: farouk.gambo@fud.edu.ng; abdulsalam.nur@nileuniversity.edu.ng; auwalus6@bupoly.edu.ng

ABSTRACT: Ensuring data security is an essential priority to be put forward once there will be a digital transmission between any two or more targeted audience. Hence, the objective of this paper was to propose a better data security model for a protective information exchange on the internet with steganographic and cryptographic algorithms. Three cryptographic symmetric key encryption algorithm (RC6, Rijndael and TwoFish) and four steganographic carrier object (Image, audio, text and video) were considered. Data obtained show that Rijndael (AES) takes less encipherment and decipherment time compare to RC6 and TwoFish in cryptographic symmetric key encryption algorithm, while image carrier achieves better Peak-Signal-to-Noise Ratio if related to audio, video and text steganography. This research suggests the use of Advanced Encryption Standard and image steganography for efficient information interchange on the internet.

DOI: https://dx.doi.org/10.4314/jasem.v28i10.8

Cite this Article as: ABDULLAHI, Y. Y; [2]FAROUK, L. G; NUR, A. S; SALE, A. (2024) Proposition of a Better Data Security Model for a Protective Information Exchange on the Internet with Advanced Steganographic and Cryptographic Algorithm. *J. Appl. Sci. Environ. Manage.* 28 (10) 3013-3018

Dates: Received: 30 July 2024; Revised: 29 August 2024; Accepted: 21 September 2024 Published: 05 October 2024

Keywords: cryptography; encipherment; imperceptibility; data security; steganography.

The internet is considered a public channel due to the fact that anyone can connect to it once the required resources are at one's disposal. Highly confidential credentials such as health status of notable individuals, military plans against their enemies and even huge financial transactions are exchange every now and then. Documents which can be regarded as containing a classified content must be secured from any sort of unauthorized access. A lot had been done by many prominent researcher's in trying to suggest a technique to be implemented when security setting is the major concern (Yahia *et al.*, 2023). The increase in the use of digital data such as image, audio, video and text files necessitate the need to for a reliable mechanism to protect them on the internet (Noor *et al.*, 2021). However, some researcher's claim that cryptography is so far the most feasible technique, cryptographic algorithm such as Advanced Encryption standard can be implemented both in hardware, software and relatively efficient for securing data (Taniya *et al.*, 2023). Meanwhile, others said that steganography is the one that standout and we say that since cryptography and steganography are the techniques considered to be efficient for now without regards to the future quantum cryptography we are going to analyse the performance of different cryptographic

**Corresponding Author Email: Email: yahayaabdullahi565@gmail.com*
**ORCID: https://orcid.org/0009-0000-7350-1269*
**Tel: 08035987089, 09065952760*

algorithm's and as well different steganographic algorithms based on the outcome of our experiment, we make genuine inferences. Steganography and cryptography can exceptionally provide security to both classified and unclassified data transmitted online (Ledya *et al., 2015*). Advanced Encryption Standard (AES) is known for its ability to encrypt large stream of data within a short period of time but require enough memory space for its encryption and decryption (Yahia *et al.,* 2023). A recent research by (Gaoyu *et al*., 2023) shows that even the CRYSTALS-Dillithium need more evaluation to meetup with the post quantum cryptographic requirement, they use a technology to see if its speed between processor and other modules can be improve prior to its implementation. The internet was still buoyance in the present of its inventors in 1970, government and organizations stated connecting computers with telephone lines, at this time the first group of hackers was born. They make use of telephone lines to hack into systems and steal highly delicate information, around 1980, hacking becomes a dominant international crime. Governmental and nongovernmental organization now raises an alarm that it is time to find solution this problem before it gets escalated (Meshds, 2022). The internet is a widely used medium where everything offered to clients are considered as a service. It is a convenient and efficient approach that offers a broad range of services when employing a distributed method. This technology, with its extensive and adaptable capabilities, is continually evolving, hence the need to secure these services increases rapidly (Nur hidayah *et al.,* 2023) Hence, the objective of this paper is proposing a better data security model for a protective information exchange on the internet with steganographic and cryptographic algorithm.

MATERIALS AND METHOD

We have considered three cryptographic symmetric encryption key algorithms namely Rijndael, RC6 and TwoFish which happens to be in the last five finalists of the NIST 1998 cryptography selection contest. We also benchmark different carrier objects (image, audio, video and text) for steganography, we have implemented all these algorithms using python programming; after these, we experiment to measure their various performance. We proposed a better method based on the outcome our experiment. In the cause of our experiment, we have sampled different file sizes within the range 25 KB to 125 KB respectively.

.

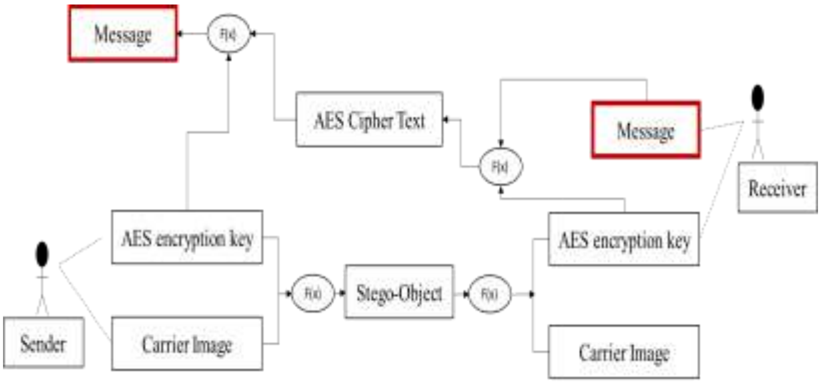
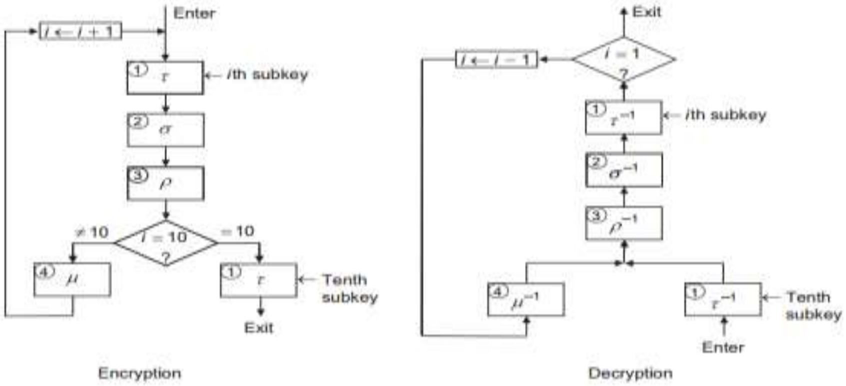


Fig. 1: Model of the proposed scheme.

Aes Algorithm Encryption and Decryption



Encryption Decryption

Fig. 2: AES encryption and decryption

The size of the file chosen does not matter or has little impact and what we are saying is that if the file sizes used are in Byte, the timing range goes down and increase with an equal amount if related to what we present in our table of values; likewise, if it's in Kilo Byte as ours, the condition steal does not change. Out proposed suggest the use of image steganography for distributing the symmetric secret key among targeted audience and then Advanced Encryption Standard for main message encryption and decryption. The sender initialises the communication by choosing a secret key, hide it using image steganography and send it to the receiver, at the receiver end he extract the secret key, use the secret key to encrypt a message and send it back to the sender, the sender now uses his chosen key to decipher the ciphertext sends to him, and it goes on this way.

Structure of the Proposed Scheme: Figure 1 was explained under materials and method

Step 1 This step is the encryption step. It is the only step that makes use of the key. The 128-bit subkey designated for that round and the 128-bit iterate are regarded as two 128- bit vectors over ***F***2 and are added component wise.

Step 2 This step is a nonlinear step in which each entry of the array is replaced by a function of itself. Thus, each byte *sij* of the four-by-four array *s* is replaced by *sij* ← *σ*(*sij*), where *σ* is an invertible nonlinear function that maps an 8-bit number into an 8-bit number. This function will be described later. For the moment, the function *σ*(*s*) can be described simply as a table look-up as given in Figure above, where the pair of hexadecimal symbols (*x*, *y*) represents the byte *s*.

Step 3 This step consists of a byte-level cyclic shift on each of the four rows of ***s***.

Step 4 This step consists of an operation on each column of matrix ***s***. (Blahut, 2014).

Peak Signal-to-Noise Ratio: The PSNR calculates the PSNR ratio in decibels between two images. We often use this ratio as a measurement of quality between the original image and the resultant image. The higher the value of PSNR, the better will be the quality of the output image. For calculating the PSNR, MSE is used (Nadipally, 2019). We calculate the PSNR by using Equation 1.

$$\begin{aligned} PSNR &= 10\cdot\log_{10}\left(\frac{MAX_I^2}{MSE}\right) \\ &= 20\cdot\log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right) \\ &= 20\cdot\log_{10}\left(MAX_I\right) - 10\cdot\log_{10}\left(MSE\right) \end{aligned} \tag{1}$$

Table 1: Signal to noise ratio (SNR) recommendation.

SNR Values	Requirement
5 – 10 dB	Cannot establish a connection
10 – 15dB	Can establish an unreliable connection
15 – 25dB	Acceptable level to establish a poor connection
25 – 40dB	Considered a good connection
41 + dB	Considered to be an excellent connection

The above table was drafted from (Rafay, 2023)

Design of The Proposed Scheme: The figure 2 is a use case diagram that state out clearly roles played by each communicating party and number of use cases available in the proposed method.

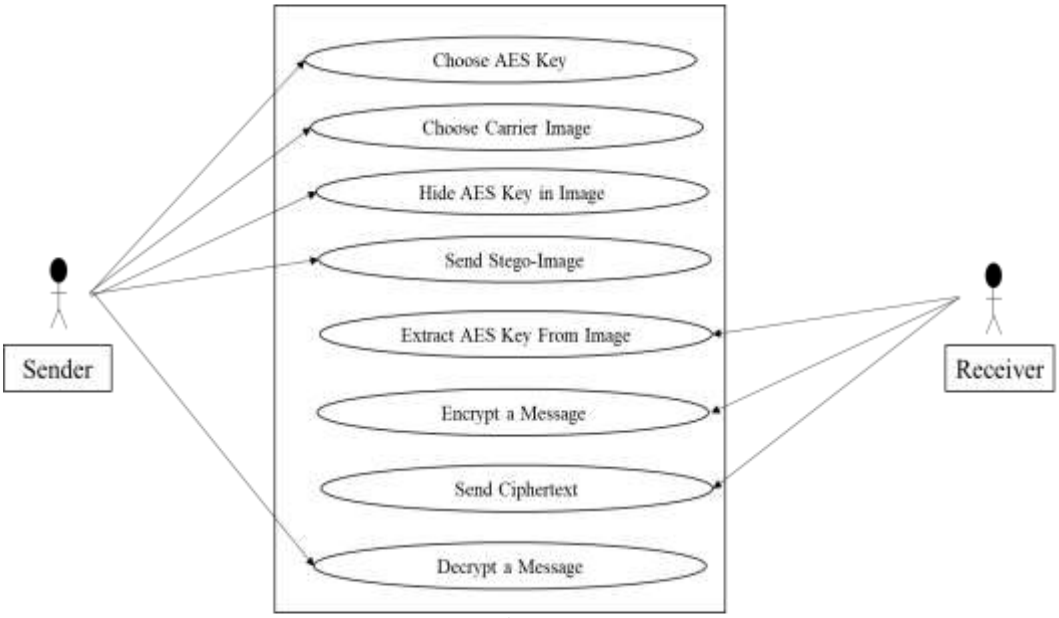


Fig. 2: Design of the proposed scheme.

RESULT AND DISCUSSION

We use encipherment/decipherment time to measure the algorithms performance. On the other hand, many steganographic carriers and techniques exist such impartial (LSB, MSB and Histogram shifting), transformation (Discrete Furrier Transformation, Discrete Domain Transformation and Discrete Wavelet Transformation), Distortion and lastly masking and filtering techniques (Aryfandy *et al.*,2017). For our own case we suggest the impartial image steganographic (LSB) techniques for efficient key secret distribution. We Peak-Signal to Noise Ratio (PSNR) as feature for selecting a better steganographic carrier object.

Encryption Time: For visualising the result of our experiment, we have used python programming language also. The result of the encryption time shows that Rivest Constant (RC6) had the longest encryption time followed by TwoFish which is actually a major pitfall for them since speed is an essential feature a reliably-efficient encryption algorithm. The algorithm with the best encryption time is Rijndael (AES) and that is one of the reasons why we proposed it, due to speed, security and its ability to encipher extremely large amount of data at once (SistlaVasundhara Devi, 2019). It is the standard use by the US government and was standardised by the National Institute of Standard and Technology (NIST).

Table 2: Encryption time of three different encryption algorithms.

S/N	Data Size	RC6	Rijndael (AES)	TwoFish
1	25 KB	1463.00 ms	218.5030 ms	410.492 ms
2	50 KB	2783.00 ms	457.8416 ms	569.091 ms
3	75 KB	2839.00 ms	616.0297 ms	726.095 ms
4	100 KB	1637.00 ms	869.1738 ms	891.761 ms
5	125 KB	3007.00 ms	895.3299 ms	933.490 ms

Table 1 is demonstrated visually using multiple bar chart below:

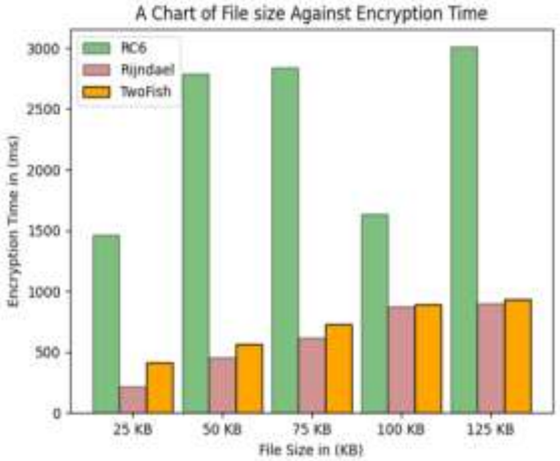


Fig. 3: A chart of encryption time against file sizes.

Decryption Time: Table 2 present the time taken by all the three algorithms considered to decipher a cipher text of the size given, figure 3 visualises it clearly.

Table 3: Decryption time of three different encryption algorithms.

S/N	Data Size	RC6	Rijndael (AES)	TwoFish
1	25 KB	1251.00 ms	526.1779 ms	3289.76 ms
2	50 KB	2362.00 ms	932.4438 ms	6339.24 ms
3	75 KB	2471.00 ms	1619.9935 ms	6930.91 ms
4	100 KB	1722.00 ms	1680.3208 ms	7070.10 ms
5	125 KB	3556.00 ms	2467.1490 ms	6969.67 ms

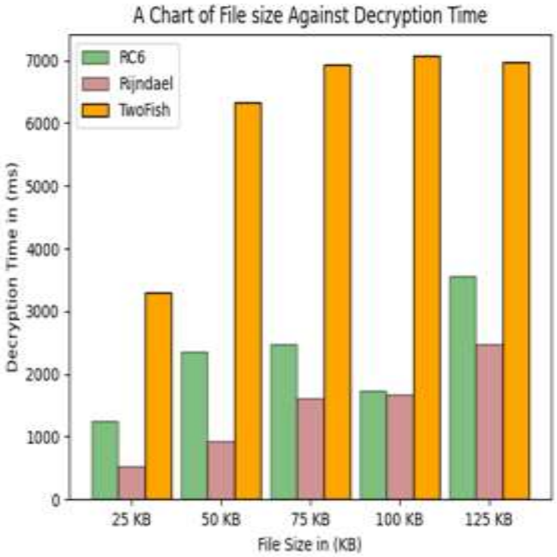


Fig. 3: A chart of decryption time against file sizes.

Based on figure 3, Rijndael perform faster decipherment followed by RC6 and then finally TwoFish. Fastness is a very important attribute for describing an encryption algorithm as an efficient one.

Data Hiding: The chart that visualises the above table is shown below in figure 4.

Table 4: Peak Signal to noise Ratio values of four carriers.

Stego object	Carrier Original Size	Secret Data Size	Stego Object actual Size	PSNR
Image	1.32 MB	3 KB	2.64 MB	51.0392 dB
Audio File	2.52 MB	3 KB	2.52 MB	33.5555 dB
Text File	37 KB	3 KB	42 KB	21.7652 dB
Video File	1.67 MB	3 KB	2.12 MB	31.1551 dB

The above chart display that the image carrier achieves the highest peak signal to noise ratio (PSNR) which is good for efficient imperceptibility. The two images below confirm our claim.

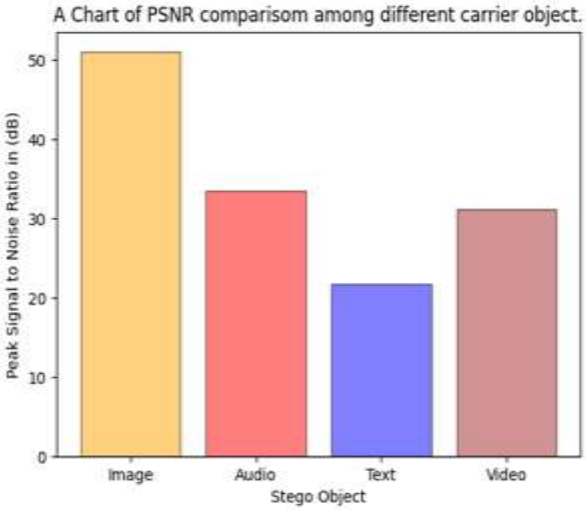


Fig. 4: A chart of PSNR against carrier objects.

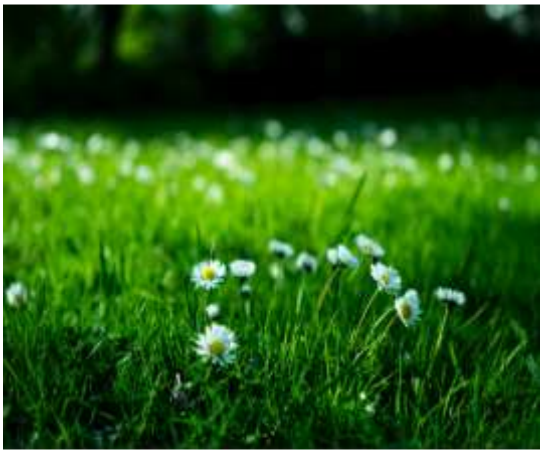


Fig. 5: Original image

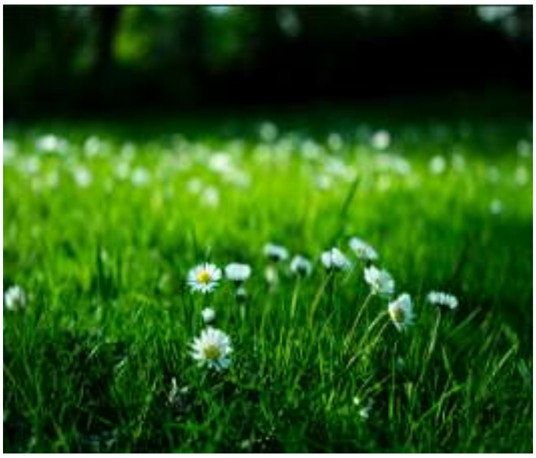


Fig 6: stego image.

From figure 5 and figure 6, one cannot be able to tell whether or not the image had been altered, but of course the first one is the actual image which does not contain any secret message, the second one contain a secret message embedded into it but undetectable with just a bare human eye. Since the goal is to secure our information in a public channel, the algorithms we proposed can be used to achieve that with better response time i.e. if secret key can remain undetectable in stego-image and secret message be scramble such that it appears meaningless to the intruders, we might say that goal achieved to some level. Even though our study considers how data can securely be transmitted, some pitfalls can be associated to it. These pitfalls can range from change in carrier (image, audio, video and text that might result in ease of detectability) sizes, more bandwidth utilization since the original message size expands, transmission speed can be slow if video/audio is used as stego-object and many more.

Conclusion: No one can claim to have a completely secure system, researchers and other international regulatory standard such as National Institute of Standard and Technology (NIST) continue to thrive towards finding lasting solution to the so-called challenges of data insecurity (which has been in existence since the inception of the internet) online. We have considered some secret key cryptographic algorithms, in which all the three we've considered are among the last five finalists of the NIST 1998 AES selection process and the four most commonly used carrier objects for steganography. Considering the output of our experiment, we proposed the use Rijndael and image steganography for reliable information exchange on the internet.

Declaration of Conflict of Interest: The authors declare no conflict of interest.

Data Availability Statement: Data are available upon request from the first author or corresponding author or any of the other authors.

REFERENCES

Aryfandy, F; Tito, WP; Randy, E S (2017). Steganography Methods on Text, Audio, Image and Video: A Survey. *Int. J. Appl. Eng. Res, 12*(13), 10485-10490.

Blahut, RE (2014). *Cryptography and Secure Communication.* USA: Cambridge University Press.

Bobby, S (2015). Overview Of Image SteganographyAnd Techniques. *Int. J. Inno. Sci., Eng. Technol, 2*(8).

Gaoyu, M; Donglong, C; Guangyan, L; Wangchen, D; Abdurrashid, I S (2023). High-performance and

Configurable SW/HW Co-design of Post-quantum Signature CRYSTALS-Dilithium. *ACM Trans. on Reconfgurable Technol. Systems*, *16*(3), 44.

Hadj, B; Ali, P; Hadj, S (2023). An Image Encryption Scheme Based on A Modified AES algorithm by Using A variable S-box. *J. Opt.*, 1-16.

Ledya, N; Gelar, B; Iwan, IT (2015). Designing Secured Data Using a Combination of LZW Compression, RSA Encryption, and DCT Steganography. *IEEE*. 12(40, 7-16.

Meshds (2022, May 17). *Hybrid Document Systems*. (Hybrid Document Systems) Retrieved March 21, 2024, from https://blog.mesltd.ca/a-history-of-information-security-from-past-to-present

Nadipally, M (2019). Optimization of Methods for Image-texture SegmentationUsing Ant Colony Optimization. *Sci. Direct*. 7(15), 7-16.

Nishtha Mathura, RB (2016). AES Based Text Encryption Using 12 Rounds with Dynamic Key Selection. *Sci. Direct.* 1036-1043.

Noor, AA; Aymen, Y; Ahmed, A (2021). Enhanced AES Algorithm Based on 14 Round in Securing data and minimizing processing time. *J. Phy*. 6(55), 8-10.

Nur Hidayah, M; Norsuhaida Binti, S; Muhammad, IH (2023). Data Security and Privacy Issues in Cloud Computing: Challenges and Solution Reviews. *TechRxiv*.

Palash, U; Mousumi, S; Syeda, JF; Masud, IA; Abu, M (2014). Developing an Efficient Solution to Information Hiding through Text Steganography along with Cryptography. *IEEE*, *ii*.

Rafay, K (2023, december 30). *omni calculator*. Retrieved december 30, 2023, from https://www.omnicalculator.com/physics/signal-to-noise-ratio.

SistlaVasundhara Devi, HD. (2019). AES encryption and decryption standards. *Int. conf. on com. vis. and mach. learn*.

Souvik Bhattacharyya, AK (2014). DCT Difference Modulation(DCTDM) Image Steganography. *Int. J. Info. Netw. Sec. (IJINS))*, *iii*, 40-63.

Sridevi, S; Narayana, RT (2022). FPGA Implementation of AES Algorithm for High Speed Application. *Analog Integrated Circuits and Signal Processing*, 1-11.

Taniya, H; Amanpreet, K; Shagun, S; Sudesh, MB (2023). A Survey on Perfomance Analysis of Different Architectures of AES Algorithm on FPGA. *Modern Electronic Devices and Communication Systems*, 39-54.

Yahia, A; Ali M; Khaldun, AM; Mohamad Afendee, M (2023). Cloud data security and various cryptographic algorithms. *Int. J. of Elec. and Com. Eng. 13*, 1867~1879.