Journal of Cases on Information Technology
Volume 24 • Issue 2

A Performance-Based Comparative Encryption and Decryption Technique for Image and Video for Mobile Computing

Raya Basil Alothman, Department of Computer Science, College of Education for Pure Sciences, University of Mosul, Iraq
Imad Ibraheem Saada, Alquds Open University, Palestine
Basma Salim Bazel Al-Brge, College of Law, Al-Mustansiriayah University, Iraq

ABSTRACT

When data exchange advances through the electronic system, the need for information security becomes a must. Protection of images and videos is important in today's visual communication system. Confidential image/video data must be shielded from unauthorized uses. Detecting and identifying unauthorized users is a challenging task. Various researchers have suggested different techniques for securing the transfer of images. In this research, the comparative study of these current technologies also addressed the types of images/videos and the different techniques of image/video processing with the steps used to process the image or video. This research classifies the two types of encryption algorithm, symmetric and encryption algorithm, and provides a comparative analysis of its types, such as AES, MAES, RSA, DES, 3DES, and BLOWFISH.

KEYWORDS

Decryption, Image/Video Encryption, Image/Video Processing, Mobile Computing, Symmetric and Encryption Algorithm

INTRODUCTION

Multimedia data security is becoming increasingly important, along with an increase in digital forms of communication on the Internet. The use of a wide range of images and videos in various types of applications already puts a great deal of attention on security and privacy issues. Multimedia data encryption helps prevent improper and unintended release of confidential information in transit or storage.

Sensitive information is stored on the Internet due to the massive spread of wireless devices. Therefore, safety has become an important issue. Many of the studies also emphasize the significance of cloud computing. Here, individuals can send and store information on the Internet. researches in this domain indicate an increased rate of access attempts and attacks to destroy information. In the cloud computing paradigm, security especially in terms of privacy is a major concern. For data exchange purpose, the entirely secure system remains an unfulfilled target that requires many studies and evaluations.

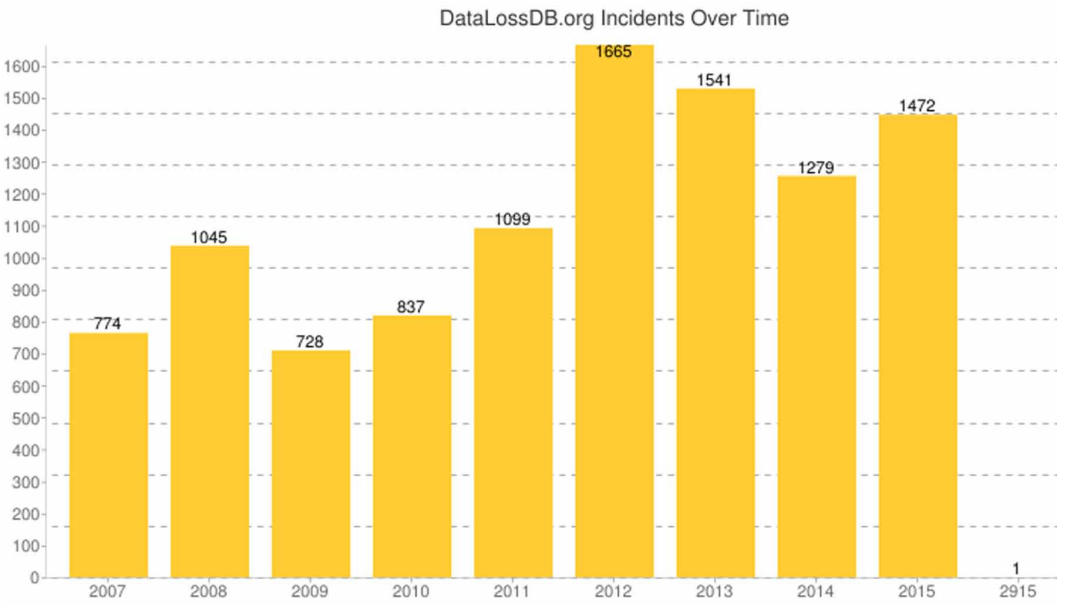
Cloud computing has expanded over the last couple of years into our lives as a new model for a vast number of business applications. Cloud computing comprises a range of systems that Using powerful data centers and servers that house user-required applications accessible through the Internet

DOI: 10.4018/JCIT.20220101.oa1

(Sanjay Ram and Vijayaraj, 2011). Such cloud-based computing systems have been used as platforms for media services and IT infrastructure for consumers and businesses (Nazir and other, 2015).

Along with developments in cloud computing, the main concern is posed by the intruder. Unauthorized exposure to cloud-based confidential data is given to attackers. Use a variety of techniques, as shown in Figure 1, to access cloud severe without legal permission. According to DataLossDB, in the first 8 months of 2014 there were 1,279 data breaches, compared with 1,472 cases in 2015(Chou,2013).

Figure 1. Data breach incidents according DataLossDB



A number of researchers work on these issues to establish consumer trust in cloud computing (Bisong and Rahmat, 2011). It is possible, by virtualization-led techniques, to the complexities of cloud computing (Koganti and other, 2013). Another way to achieve security and confidentiality in CC is to include a particular encryption mechanism (Prasanthi and other, 2014). The use of the Internet is growing fast, and a number of services are required to secure data on the Internet. They all protect internet data by using a particular encryption algorithm. This study includes several well-known encryption algorithms: AES, MAES, RSA, DES, 3DES, and BLOWFISH.

Challenges of Implementing Cryptography Algorithms By Mobile Devices

Mobile Computing Portable devices, such as smartphones, palmtops, etc., offer convenient access to people with diverse sources of global information immediately anywhere at any moment. It is a device that is constantly evolving towards the needs of consumer desires by using the principle of Bring Your Own Device–Bring Your Own Device (BYOD–BYOT). A mobile device may be a Personal Digital Assistant (PDA), a handy Cell Phone or Web Phone, a laptop, or any of the numerous devices mentioned above that allow the user to complete the tasks without being linked or connected to a network. The cellular and smartphone world poses different challenges for consumers and service providers. Physical constraints such as the weight of the unit, the batteries, the size of the screen, the portability, the efficiency of the radio transmission and the error rate are becoming more significant.

Although the device facility requires the versatility of the customer, the system, the network, the service provider and some other difficulties, it gives users the ability to provide new services and additional information. The main challenges in mobile computing are low bandwidth, high error rate, power limitations, security, limited capabilities, disconnection and problems caused by client mobility. Given these obstacles, encryption is becoming a major concern because it is linked anonymously. When adapting cryptographic algorithms to mobile computing, hackers do not have the chance to reach mobile devices. Various cryptographic algorithms have been used to maintain security in mobile devices and provide secrecy, transparency, availability, non-repudiation, permission and trust and accounting (CIANATA).

Energy Consumption By Mobile Devices

In addition to scientific and technological advancements, consumers are drawn to, love, work and live with innovative and convenient electronic products. This is the phenomenal advancement in communication technologies and the widespread use of the Internet that contributed to the development and development of m-commerce. Conversely, we have seen a growing demand for mobile devices. The quest for easier, cheaper and faster options has led to the introduction of PDAs, cell phones and pagers. Therefore, even though the PC interface was the main target for client software, we would expect commercial applications to switch from the traditional desktop to these mobile devices. Mobile devices have become very common in the ubiquitous world and have a wide range of applications, including audio-visual, event logging, surfing the Internet, making phone calls, etc.

Battery life is the key issue limiting the long-term usefulness of mobile devices, since devices have not always been attached to immovable power supply, but battery-supplied, and the limitation of portability places limits on battery size and weight. Technical advancements such as semiconductive and wireless communication technologies are not resistant to battery technologies. The capacity of the battery thus represents a major challenge for modern mobile devices and systems growth. In reality, the consumer can build and use other programs. The energy from mobile device battery is consumed by every continuous operation. As a consequence, for new smartphones the total battery life is usually less than two days(Korhonen, 2011) and for using smartphones it is even shorter. Moreover, 80% of mobile users take steps to improve their mobile battery life(Rahmati and other, 2007).

Traditional cryptographic protocols need a significant amount of energy to store and transmit data. For order to extend the battery life, a mobile device should use the minimum possible energy level while at the same time ensuring an acceptable level of safety. In consideration of the limited energy budget of mobile devices, the security given by each algorithm must be modeled on the basis of its energy consumption (Fotiou 2012). The issue of energy consumption is therefore the most important issue for mobile end nodes. Extensive research is being carried out on optimizing the battery life of mobile computing devices, understanding charging behaviour and battery signals, customizing power-saving settings, predicting the level of power consumption (Krintz and other, 2004). Nevertheless, any energy management policy requires accurate predictions of energy consumption and battery life, which are difficult without reliable energy measurement and evaluation of methods and resources.

Problem Statement

Several problems must be solved when using multimedia encryption methods, as previous works have pointed out: it takes a considerable amount of time to encrypt and decrypt multimedia data because of the huge size of multimedia data. Accordingly, carefully selected multimedia data segments can be encrypted based on the visual significance or simplified encryption methodologies used to reduce the cost of computing (Cheng and Lemer(2015).

The images still can be encrypted with conventional methods of encryption. The implementation of standard techniques to raw images, however, leads to a substantial increase in bandwidth which leads to a serious bottleneck in the communication of images (Ding and other, 2016).

The security level of digital encryption methods is not as high as the traditional approaches of text-based encryption. Given that the short durability and reliability of the streaming media is taken into account, the security level should be set to prevent the manipulation of encrypted data. Therefore, in order to meet realistic constraints such as real-time operation, it is essential to diminish the security level of crypt processes to a minimum satisfactory level.

In comparison to text data, multimedia data can be compressed at very high compression rates without losing the human visual system features. Encrypted multimedia data can also be compressed intentionally to comply with channel bandwidth constraints or compressed accidentally by unauthorized persons. It is therefore believed that, even after a deficiency of encryption, encrypted digital data can be decrypted. This form of encryption must be resistant to compression deficiency (Li and other, 2017).

Cryptography

Cryptography is the Science of Information Security derived from Greek cryptography, meaning hidden (Rhee, 2003). It is the method of data protection, of translating data to an unreadable cipher format. The method of translating data into a cipher format is known as encryption, while the process of transmitting back data in a cipher format to the original data is known as decryption. The purpose of cryptography is as follows:

- Confidentiality: Assures that private data remains private.
- Integrity: Makes sure an entity is not illegitimately manipulated.
- Failure to repudiate: ensures the refusal of information or interaction from a party.
- Authentication: Ensure that all parties seeking access have the characteristic.

Cryptography algorithms play an important role in information security. We can be classified into symmetric and asymmetric key cryptography.

Symmetric algorithms are of two types (Stallings, 2000): block ciphers and stream ciphers. Block ciphers operate on data in groups or strings. For examples, Data Encryption Standard (DES), Advanced Encryption Standard (AES) and Blowfish. Channel ciphers are running on a single bit at a time. RC4 is an algorithm for a flow cipher.

For encryption and decryption of symmetrical keys the sender and receiver use the same key. As illustrated in figure 2, a symmetric key encryption can be defined as a secret key, since the sender as well as the receiver must maintain the key safe and protected. When two parties choose to exchange data using secret key encryption, a backup of the same key must be produced.

Asymmetric key (or public key) encryption is used to solve the problem of key distribution. Two keys are used for Asymmetric key encryption; secret keys and public keys. The public key is used for encryption purposes and the private key is used for decryption purposes (e.g. Electronic Signatures). The public key is known to the public key and the private key is revealed to the owner only.

A two-key cryptosystem that helps two parties to easily interact on a non-secure communication-platform without having to share a secret key and solve the problem of the secret key sharing using two keys rather than one key. For more details see figure 3.

Image Encryption

The primary principle in the image encryption is to transfer the image securely over the network so that no unauthorized client can be able to decrypt the file. Image content has peculiar properties, such as mass restriction, high separation and strong interaction between pixels, which require extraordinary preconditions for any encryption procedure (Hussain and other,2010). The most well-known method for protecting digital photographs is to encrypt computerized records in such a way that a particular archive document should not be detected. There are a few ways to do this, such as steganography,

Figure 2. Symmetric key algorithm

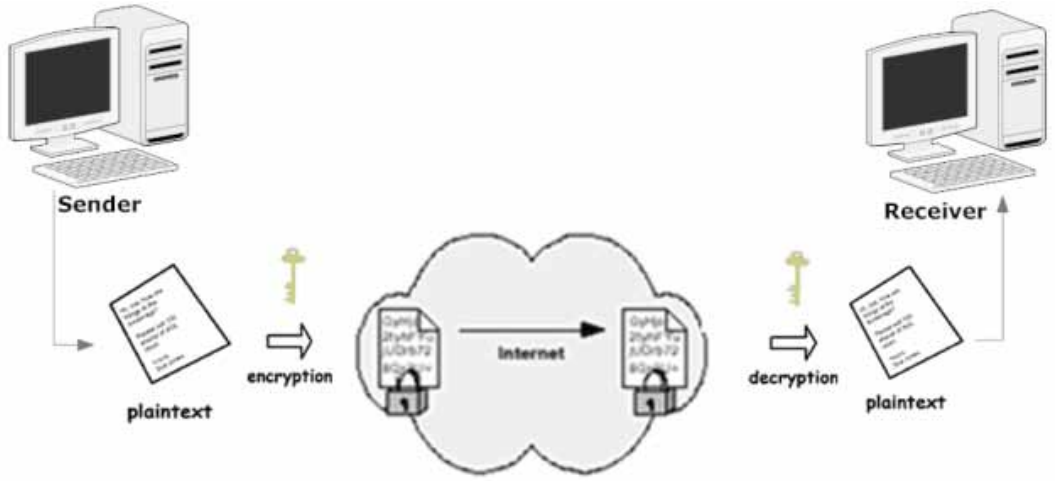
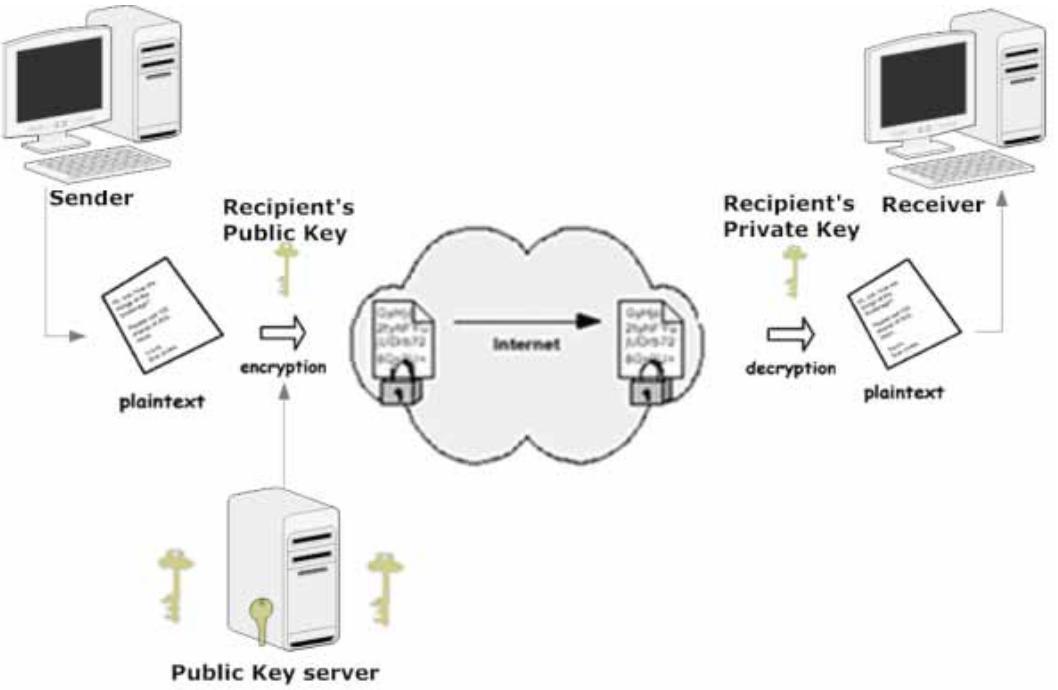


Figure 3. Asymmetric key algorithm



folding, sophisticated watermarking and cryptography. The focus here is on the encryption methods of advanced digital images that focus on chaos mapping. Fundamentally, image encryption is the methodology of changing data using an algorithm to make it ambiguous to anyone, with the exception of those with exceptional learning, usually referred to as a key and changing data using an "encryption algorithm" to a structure that cannot be deciphered without a decryption key.

From the other point of view, the decryption of the image recovers the actual data from the encrypted structure image. There are more than a few computerized image encryption systems available to encode and decrypt image content, and there is no simple, open encryption formula that fits the distinctive image kinds. The chaotic mapping-focused encryption strategy also reduces the computational difficulty of the encryption process by providing encoded advanced images to maintain a multi-level encryption strategy. A large portion of algorithms specifically designed to decode or encode computerized images was introduced in the mid-1990s. There are two major groups of image encryption algorithms: (a) non-chaos random methods and (b) selective or non-selective methods dependent on chaos. The vast majority of these algorithms are meant for a particular compact or uncompressed image configuration, and some of them are also acquiescent setups.

There are schemes that give soft encryption (degradation), while others sacrifice the solid nature of encryption. A majority of algorithms are scalable and have different modes, from regression to solid encryption (Murillo-Escobar and other, 2011). Cryptography approaches based on confusion have distinctive applications in different zones, for illustrations; online communications, security, medical services, visualization and situating, phone picture coverage, interactive media systems, psychological imaging, tele-pharmaceutical, defense and policy records, and so on. The development of the method of picture encryption is progressing towards the possibility of unregulated possible outcomes. New strategies for encryption methods are disclosed on a regular basis (Subramanyan, 2011).

Video Encryption

Traditional commerce requires security of data in all aspects of multimedia format and a very necessary requirement of traditional commerce. The applications associated in the real world as of video conferencing applications and VOD applications requires that only the paid users can access the multimedia data presented before the various user stream.

No doubt authentication-controlled mechanisms are available in order to manage the accessibility of multimedia formatted data in distributed form. But, on formats of wireless networks, networks of satellite or any other IP network system the data in multimedia format cannot only be made secure by such authentication mechanisms. Treating the complete data in the format of binary form confirms that it is one of the greatest famous techniques to secure underlying data in multimedia format. Further, the complete data is encrypted with the usage of secret key algorithms for encryption such as the Data Encryption Standard Algorithm also called as DES for short, AES, IDEA, etc. Secret key encryptions are very complicated and require heavily computed values. The problems faced are described in two implementations.

In the software, as the algorithms are implemented it shows that it is slow enough in processing the large data amount that are formed applications in the multimedia format. The other one is related to hardware where its applications in hardware format implementations additional costs are added at both the ends of data generators and also the receiving users. There are two major factors causing challenge to multimedia data encryption. First, typical multimedia data have large size (the size for e.g., of any MPEG-1 video format of two hours is in and around 1GB). Secondly, processing of the data in multimedia formats has the need to get processed in the real-time-frame scenario. The video codec-device is put or overlaid with heavy burden when large or huge data is being processed in a very small timespan. Heavy affects are also seen on the requirements related with space and storage and also the network communications are drastically burdened. The application of algorithms of both encryption as well as decryption type aggravates the faults and causes the latency to increase either at the time or even after the phase of encoding.

Related Work

Agrawal et al.(Agrawal and Mishra, 22012) suggested that the common symmetrical core encryption algorithms DES, TRIPLE, AES, and Blowfish should be studied in depth. Symmetrical algorithms run rapidly, and the buffer size of Symmetric algorithms is smaller than asymmetric algorithms,

such as RSA, etc. Symmetric key coding is the same as Asymmetric key coding protection level. The preeminence of Blowfish algorithm over other algorithms is relied on reliability and key size. The Blowfish algorithm's F feature provides high security for 64-bit plaintext encryption.

The three algorithms DES, RSA and AES were analyzed in a comparative way by Seth et al.(Seth and Mishra,2011) taking into account other processing time, resource use and performance bit parameters. The RSA has been found to contain the longest cryptography and to use very large energy, but for RSA algorithms it is the lowest performance. DES has the least time for encryption and the least amount of memory use for AES, while the time discrepancy between AES and DES algorithms has been shown to be very low depending on the used text files and experimental research.

The four most used symmetric algorithms are DES, 3DES, AES and Blowfish, which have been developed by Mandal et al.(Mandal, 2012). Comparison of the block size of a circular block, the key time, encoding / decryption time and CPU cycle times for output and power consumption were carried out using the mentioned four parameters. Blowfish were found outperform than other algorithms. AES has an advantage over the other 3DES and DES in terms of efficiency and decryption time. 3DES has the lowest performance of all of the above algorithms.

The three algorithms for Aes, 3DES, and RSA have been discussed by Marwaha et al.(Marwaha and other,2013). DES and 3DES are crypto algorithms of a symmetrical key, and RSA is a crypto algorithm of an asymmetric key. Algorithms were evaluated for their data security ability, the time required for data encryption and algorithm throughput. The performance of different algorithms was different based on the data. The conclusion was that 3DES ' security and scalability over DES and RSA is far greater and makes it even less processing power and time to encrypt and decrypt data through DES, however, the brute force technology of DES encryption can easily be broken in comparison with 3DES and RSA, the last secure algorithm is making it

Six of the most common encryption algorithms were addressed to Abdul et al.(Elminaam and other, 2009),which are DES, 3DES, RC2, BLOWFISH and RC6 (Rijndael). The performance of these algorithms was evaluated in different scenarios such as data size, data format, battery power, key sizes and speed of encryption / decryption process. The findings shown in either the Hexadecimal Base Encoding or Base 64 Encoding were found to make no significant difference. Second, BLOWFISH was found to perform much more efficiently as with other common encryption algorithms used by RC6 when the packet size has been adjusted. Although it was found that the form of RC2, RC6 and BLOWFISH was time consuming compared to other algorithms when adjusting the data shape, such as the image rather than the text. However, 3DES is still weak in comparison to the DES algorithm. To end, it is easy to see that a greater key size leads to a clear change in battery and time use in the event of a decrease in key size.

Apoorva et al. (Apoorva, 2013) contrasted the most popular symmetric cryptography algorithms: AES, TWOFISH, CAST-256 and BLOWFISH. The analysis took into account the action and effectiveness of algorithms when different data loads were used. The analog was made on the basis of the following parameters: rpm, block size and key dimension. It has been noticed that blowfish is superior to another method because it takes less time. Although this difference was not clearly visible when the scale of the data was very small. But it was very clearly visible for a file greater than 100 KB in size.

The three common symmetric key algorithms, DES, AES, and Blowfish, are being discussed fairly by Thakur et al.(Thakur and Kumar, 2011). The main problem was the effectiveness of algorithms within various settings and when various data loads have used the measurements given take into account the action and output of algorithms. The parameters such as rpm, block size, and the key size were used to produce the analogue. The simulation software was introduced based on Java programming. Finally, Blowfish were outperformed than other algorithms.

Alam et al.(Alam and Khan,2013) have been able to check for the accuracy and practicality of the many cipher block algorithms in symmetrical key encryption (DES, 3DES, CAST-128, BLOWFISH, IDEA & RC2). Data size (different data formats), encryption and decryption time, the speed for

Table 1. Comparative Analysis of Different Algorithms

Algorithm	Year of use	Key length	Size of block	No. of round
DES	1977	56-bits	64-bits	16
AES	2000	128-bits, 192-bits, 256-bits	128-bits	10, 12, 14
3DES	1978	128-bits, 112-bits, 56-bits	64-bits	48
BLOWFISH	1993	32-bits, 448-bits	64-bits	16
RSA	1977	1024 to 4096 bits	64-bit	-

encryption and decryption of each cipher block, and power consumption were used to evaluate block cipher algorithms. Due to its three-phase properties, 3DES was found to have a higher power consumption and poor performance than DES.

Saini (Saini, 2014) assesses the efficiency of numerous algorithms namely, DES, AES, RC2, Blowfish, 3DES, and RC6. The results have showed that the optimal algorithms are well-proven and recorded. A good cryptographic system balances what is possible with what is appropriate.

Alanazi et al.(Alanazi, 2010) conducted a comparative study of three Algorithms (e.g, DES, 3DES and AES)based on nine measurements such as, Cipher Type, Key Duration, Block Size, protection, Possible Keys, Security, etc. However, this study has illustrated that AES is better than other algorithms.

In the cloud network and a single Processor with certain input sizes, Arora et al.(Arora and others, 2012) has also analyzed the performance of multiple algorithms. This paper aims at explaining the advantages that companies use to encrypt large volumes of data in quantitative measures such as Speed-Up Ratio by using cloud tools in applying encryption algorithms (RSA, MD5 and AES). The following are three different patterns of software: RSA, MD5, and AES. The results of this study have showed that the algorithms used in the cloud scenario (i.e. the Google App) are more efficient than ones have been utilized in a single system. RSA is the maximum time-consuming for both uniprocessor (local) and server (appengine) applications, and MD5 is the least time consuming. AES reaches the maximum speed-up ratio with lowest input sizes, on other hand the speed-up ratio decreases dramatically as the input size raises. For every input scale, the speed-up ratio is the maximum for AES, accompanied by MD5 and the lowest for RSA algorithms.

Comparison of Various Algorithms

Implement Algorithms (AES, MAES, DES, 3DES, RSA, and Blowfish)

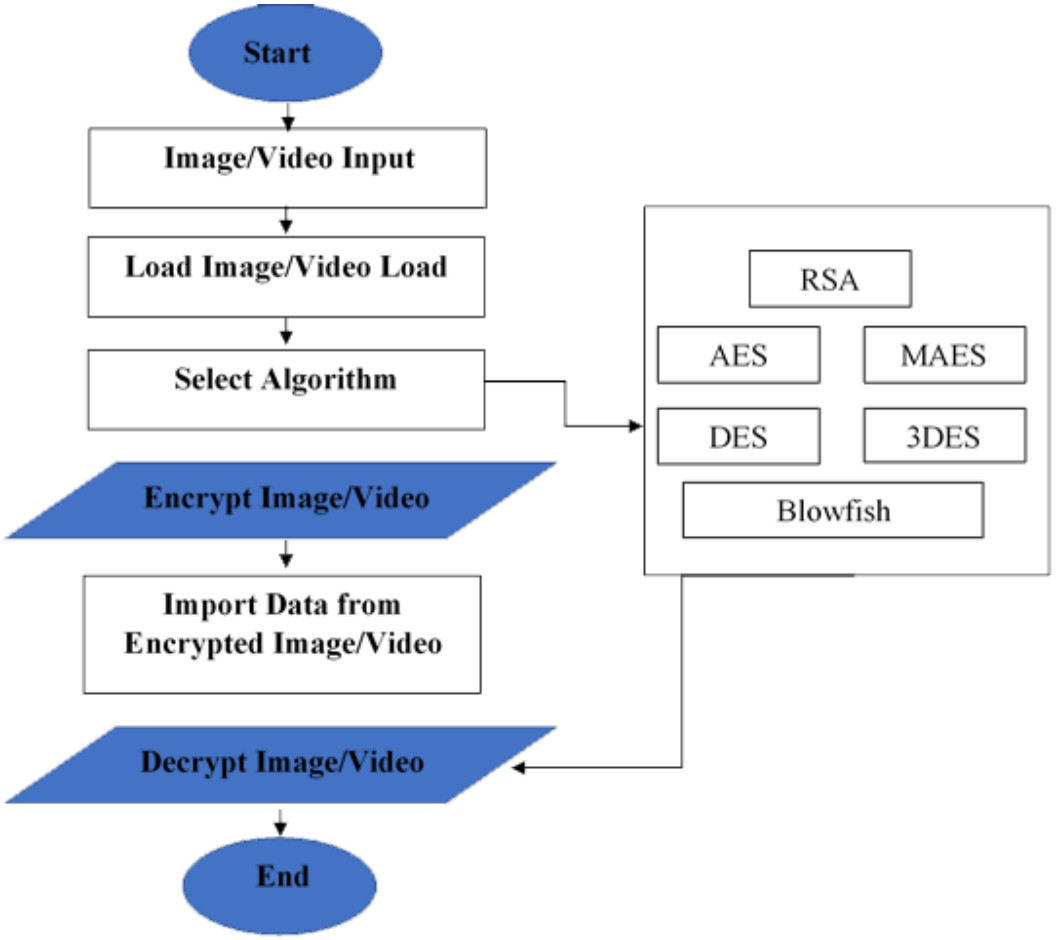
This phase shows the graphical representations of the workflow are shown in a step-by-step process and the activities are represented for cycle, decision and simultaneity. The starting point of the process flow can be shown by specific symbols, and the end of the flow can also be represented by a specific end symbol. The arrows depict the control stream between objects. Depending on the study requirement, different object states can be represented using different structural symbols. Choose a file then upload it. Running the encryption file; by algorithm.

The image / video frame sequence is encoded using the integrated versions of AES, MAES, DES, 3DES, Blowfish,and RSA. Nevertheless, the performance evaluation of the proposed algorithm justifies its significant contribution to high-end compression access as well as ensuring the high quality of the encryption algorithm.

Experiment Settings

The experiment details will be given in the next subsections as follows:

Figure 4. Process Flow



Hardware Specifications: This study has conducted experiment based on personal Dell PC with Processor: Intel® core ™ i53210M CPU @ 2.50GHz, 4GB Ram.

Software Specifications: The tests are conducted on Windows 10 and MATLAB programming language. Using MATLAB, various videos and images were encrypted. Windows 10 invloves MATLAB to permit access to encryption and then run it.

Dataset: The two image files namely 1.JPG and 2.JPG are considered for simulating the algorithm. Both files have the same pixel 580x387 but different file size.

Design Phase

This process obtained image and video from random samples, researched and used encryption algorithms. The two methods (image and video) were used. This project has designed and implemented an encryption technique with a number of parameters. Then the tests run with all the output parameters.

Implementation Phase

This segment shows the influence of encryption with various image / video sizes and formats. The technical measures are used to analyse the performance of encrypted data. The approach consisted of combination of quantitative and descriptive analysis. It was mainly based on the analysis and

Figure 5. Selected image 1

Figure 6. Selected image 2

Figure 7. Selected video 1

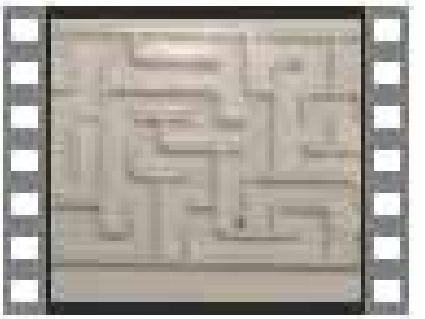


Figure 8. Selected video 2

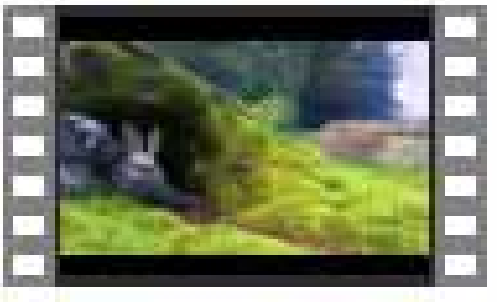


Figure 9. Experiment Environment

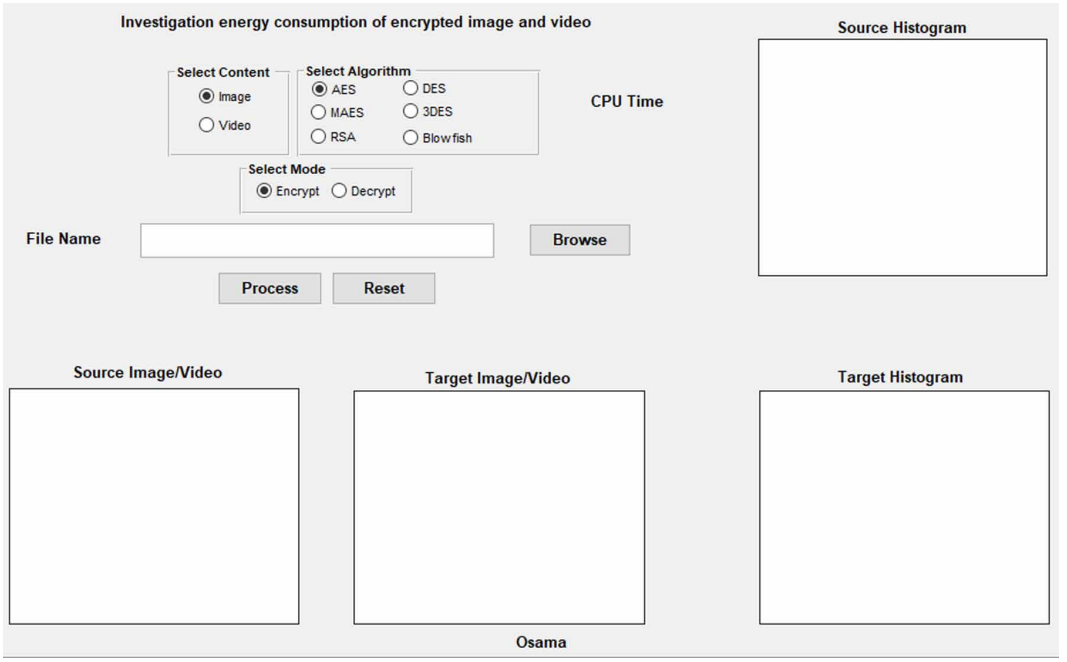


Figure 10. Attached Image/Video

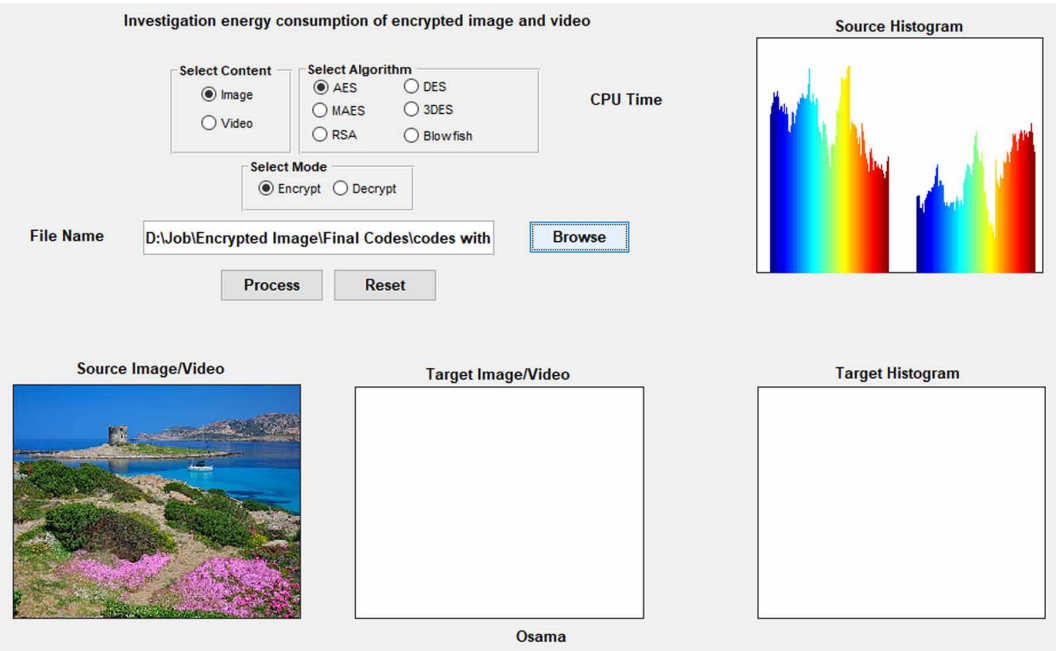


Figure 11. Select the Algorithm and Mode

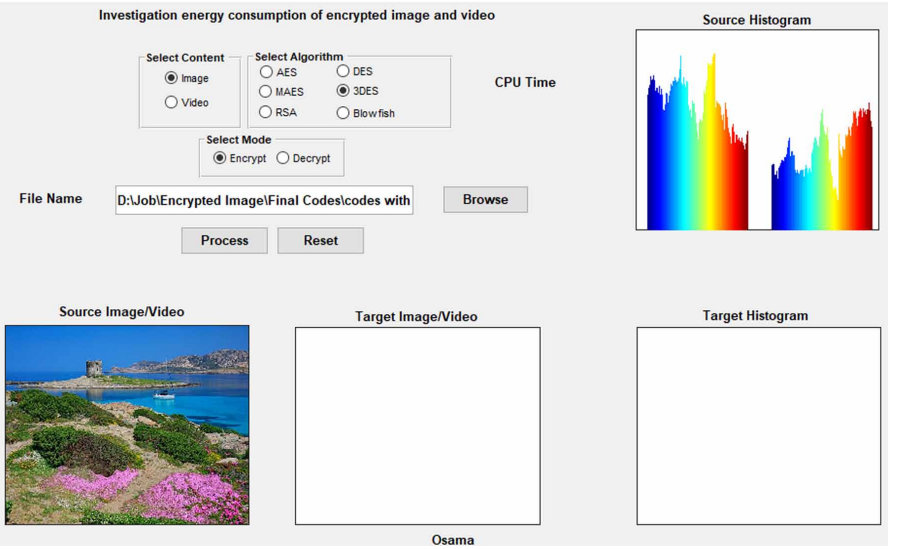
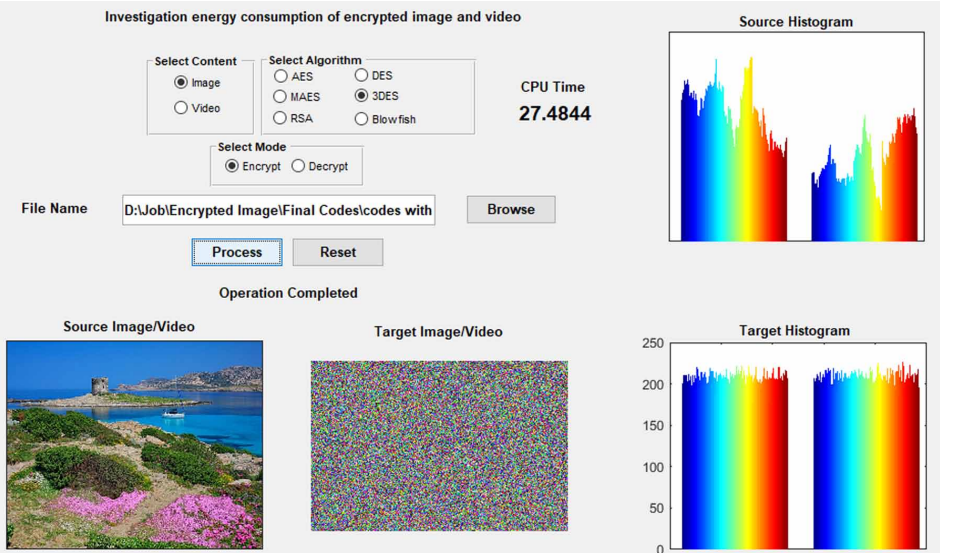


Figure 12. Start Process



application of cryptography, with several criteria. Quantitative analysis has been used to conduct multiple experiments and to evaluate the performance of the device. Where this initiative is designing the experiments, as follows:

Step 1: Attached Image/Video

At this step first select the contents, in case of image select the image content or in case of video select the video content.

Step 2: Select the Algorithm and Mode

At this step select the desire algorithm from the list using radio button. Next is to select he mode like encrypt or decrypt.

Step 3: Start Process

At this step process will begin and for encryption or decryption. This process will generate the histogram and will display the encrypted image/video with CPU time.

Compression Approach For CPU Time

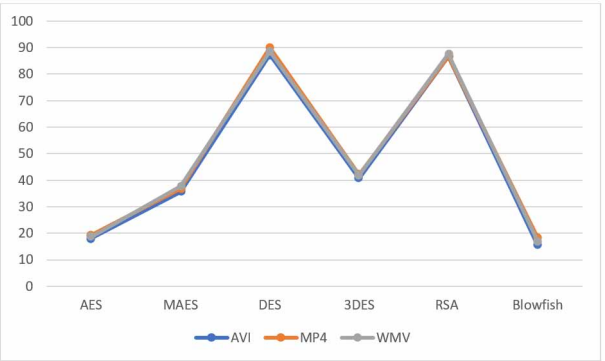
The proposed framework has been integrated with different video formats through Algorithm (AES, MAES, DES, 3DES, RSA, and Blowfish). The experiment results show in table 2 with encrypted video for different video formats but same video size.

Table 2. CPU Time for Different Image Formats

Algorithm	AVI	MP4	WMV
AES	18.0313	19.25	18.6525
MAES	35.6875	36.75	37.65
DES	87.3906	89.96	88.60
3DES	40.7188	42.18	41.818
RSA	86.5469	86.6954	87.649
Blowfish	15.5625	18.3453	17.1003

Figure 13 shows the comparison between different video formats for CPU time. The figure shows that energy consumption for AVI video is less than other video formats. However, for algorithms comparison, the Blowfish (15.5625) shows good performance with AES, MAES, DES, 3DES and RSA.

Figure 13. Comparison of different images formats for CPU Time



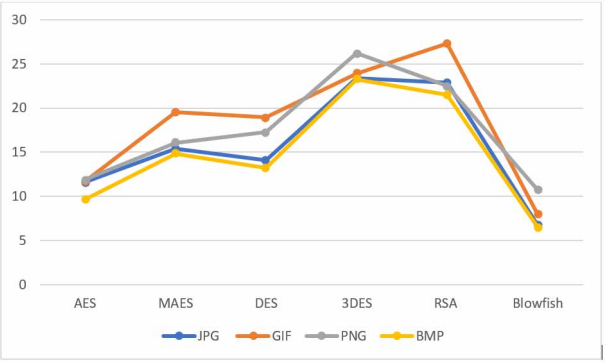
The proposed framework has been integrated with different image formats through Algorithm (AES, MAES, DES, 3DES, RSA, and Blowfish). The experiment results show in table 3 with encrypted images for different image formats but same image size.

Figure 14 shows the comparison between different image formats for CPU time. The figure shows that energy consumption for BMP image is less than other images formats. However, for algorithms comparison, the Blowfish shows good performance with AES, MAES, DES, 3DES and RSA.

Table 3. CPU Time for Different Image Formats

Algorithm	JPG	GIF	PNG	BMP
AES	11.625	11.70	11.90	9.67188
MAES	15.4063	19.49817	16.0781	14.824
DES	14.1094	18.924	17.2736	13.18
3DES	23.3594	23.899	26.23	23.2188
RSA	22.9063	27.271	22.5	21.519
Blowfish	6.78125	7.948	10.71005	6.543

Figure 14. Comparison of different images formats for CPU Time



Compression Approach for Memory

The proposed framework has been integrated with different video formats through Algorithm (AES, MAES, DES, 3DES, RSA, and Blowfish). The experiment results show in table 4 with encrypted video for different video formats but same video size.

Figure 15 shows the comparison between different video formats for CPU time. The figure shows that energy consumption for AVI video is less than other video formats. However, for algorithms comparison, the AES shows good performance with Blowfish, MAES, DES, 3DES and RSA.

The proposed framework has been integrated with different image formats through Algorithm (AES, MAES, DES, 3DES, RSA, and Blowfish). The experiment results show in table 5 with encrypted images for different image formats but same image size.

Table 4. Memory for Different Image Formats

Algorithm	AVI	MP4	WMV
AES	2.14925	2.164344	2.15433
MAES	2.16797	2.1743	2.17543
DES	2.16923	2.17543	2.17544
3DES	2.17569	2.18659	2.18548
RSA	2.17204	2.18654	2.18909
Blowfish	2.1704	2.18653	2.18776

Figure 15. Comparison of different images formats for Memory

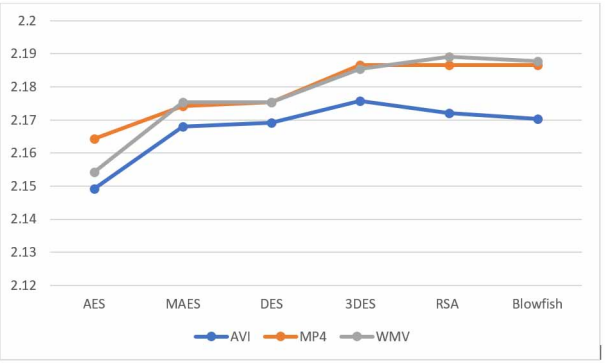
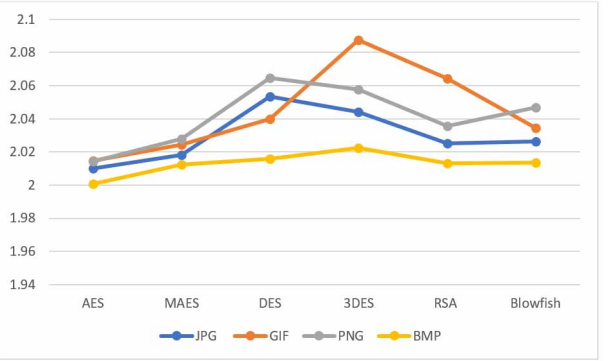


Table 5. Memory for Different Image Formats

Algorithm	JPG	GIF	PNG	BMP
AES	2.01008	2.01456	2.01452	2.00066
MAES	2.01831	2.0245	2.02785	2.01231
DES	2.0533	2.03973	2.06454	2.01578
3DES	2.04415	2.08765	2.057654	2.0223
RSA	2.02513	2.06445	2.0355	2.01334
Blowfish	2.02633	2.03466	2.04676	2.0134

Figure 16. Comparison of different images formats for Memory



CONCLUSION

Safety in the delivery of digital images and video has its significance in today's image communications, given the increasing use of images and video in the industrial process, it is important to secure sensitive image and video data from unauthorized access, and image and video safety have become a critical issue. This research also provides a study of the symmetric and asymmetric algorithm for the performance evaluation of the chosen algorithm (AES, MAES, Dec, 3DES, RSA, and Blowfish).

This research offers a high-level description of some of the most widely used encryption / decryption algorithms, such as AES, MAES, DES, 3DES, RSA, and Blowfish, and demonstrates the design of a test bed to evaluate the encryption procession overhead of various cryptographic algorithms using a basic GUI (Graphical User Interface). An easy-to-use interface is developed that allows any user to provide any type of input image / video and execute it against a set of available encryption algorithms. Each minute detail, beginning with the specifications for the execution of the proposal, has been provided in a theoretical and practical way. The primary focus is on clearly presenting the energy consumption used to encrypt the input image / video using which organizations can easily analyze the performance of different algorithms. The project also provides a graphical representation of the performance analysis for ease of understanding.

Each algorithm was applied to a particular set of parameters. It has been found from the results that Blowfish is the most secure and efficient algorithm among the symmetric encryption algorithms. The speed and power consumption of these algorithms is better than the other algorithms. The hackers cannot easily break the Blowfish algorithm before they find the correct combinations. It's more difficult to form the exact combinations of the lock. The algorithm has increased the number of loops. It takes less time to encrypt and decode an image and a video than any other algorithm.

REFERENCES

Bisong, A., & Rahman, M. (2011). *An overview of the security concerns in enterprise cloud computing*. arXiv preprint arXiv:1101.5613

Rahmati, Qian, & Zhong. (2007). Understanding human-battery interaction on mobile phones. *Proceedings of the 9th international conference on Human computer interaction with mobile devices and services*, 265-272. doi:10.5121/ijnsa.2011.3103

Dawood, A. (2019). An adaptive intelligent alarm system for wireless sensor network. *Indonesian Journal of Electrical Engineering and Computer Science*, *15*(1), 142–147. doi:10.11591/ijeecs.v15.i1.pp142-147

Saini, B. (2014). Survey on Performance Analysis of Various Cryptographic Algorithms. *International Journal of Advanced Research in Computer Science and Software Engineering*, *4*, 1–4.

Subramanyan, B., Chhabria, V. M., & Babu, T. S. (2011). Image encryption based on AES key expansion. *2011 Second International Conference on Emerging Applications of Information Technology*, 217-220. doi:10.1109/EAIT.2011.60

Krintz, C., Wen, Y., & Wolski, R. (2004). Application-level prediction of battery dissipation. *Proceedings of the 2004 international symposium on Low power electronics and design*, 224-229. doi:10.1145/1013235.1013292

Li, C., Lin, D., & Lü, J. (2017). Cryptanalyzing an image-scrambling encryption algorithm of pixel bits. *IEEE MultiMedia*, *24*(3), 64–71. doi:10.1109/MMUL.2017.3051512

Elminaam, D. A., Kader, H. A., & Hadhoud, M. M. (2009). Performance evaluation of symmetric encryption algorithms. *Communications of the IBIMA*, *8*, 58–64.

Alanazi, H., Zaidan, B. B., Zaidan, A. A., Jalab, H. A., Shabbir, M., & Al-Nabhani, Y. (2010). *New comparative study between DES, 3DES and AES within nine factors*. arXiv preprint arXiv:1003.4085.

Cheng, H., & Lerner, C. (2015). Bit allocation for lossy image set compression. *Communications, Computers and Signal Processing (PACRIM), 2015 IEEE Pacific Rim Conference on*, 52-57. doi:10.1109/PACRIM.2015.7334808

Hussain, I., Shah, T., & Mahmood, H. (2010). A new algorithm to construct secure keys for AES. *International Journal of Contemporary Mathematical Sciences*, *5*, 1263–1270.

Thakur, J., & Kumar, N. (2011). DES, AES and Blowfish: Symmetric key cryptography algorithms simulation-based performance analysis. *International Journal of Emerging Technology and Advanced Engineering*, *1*, 6–12.

Korhonen. (2011). *Predicting mobile device battery life*. Department of Communication and Networking, S-38.

Khalaf, O. I., & Abdulsahib, G. M. (2019). Frequency estimation by the method of minimum mean squared error and P-value distributed in the wireless sensor network. *Journal of Information Science and Engineering*, *35*(5), 1099–1112.

Khalaf, O. I., & Sabbar, B. M. (2019). An overview on wireless sensor networks and finding optimal location of nodes. *Periodicals of Engineering and Natural Sciences*, *7*(3), 1096–1101. doi:10.21533/pen.v7i3.645

Khalaf, O. I. (2020). Optimization of wireless sensor network coverage using the Bee Algorithm. *Journal of Information Science and Engineering*, *36*(2), 377–386.

Khalaf, O. I., Abdulsahib, G. M., Kasmaei, H. D., & Ogudo, K. A. (2020). A new algorithm on application of blockchain technology in live stream video transmissions and telecommunications. *International Journal of e-Collaboration*, *16*(1), 16–32. doi:10.4018/IJeC.2020010102

Agrawal, M., & Mishra, P. (2012). A comparative survey on symmetric key encryption techniques. *International Journal on Computer Science and Engineering*, *4*, 877.

Alam, M. I., & Khan, M. R. (2013). Performance and efficiency analysis of different block cipher algorithms of symmetric key cryptography. *International Journal of Advanced Research in Computer Science and Software Engineering*, *3*.

Marwaha, M., Bedi, R., Singh, A., & Singh, T. (2013). *Comparative analysis of cryptographic algorithms* (Vol. 16). Int J Adv Engg Tech/IV/III/July-Sept.

Murillo-Escobar, M., Cruz-Hernández, C., Abundiz-Pérez, F., López-Gutiérrez, R. M., & Del Campo, O. A. (2015). A RGB image encryption algorithm based on total plain image characteristics and chaos. *Signal Processing*, *109*, 119–131. doi:10.1016/j.sigpro.2014.10.033

Sanjay Ram, M., & Vijayaraj, V. (2011). Analysis of the characteristics and trusted security of cloud computing. *International Journal of Cloud Computing*, *1*, 61–69.

Rhee, M. Y. (2003). *Internet security: cryptographic principles, algorithms and protocols*. John Wiley & Sons.

Fotiou, N., Marias, G. F., Polyzos, G. C., Szalachowski, P., Kotulski, Z., & Niedermeier, M. (2012). Towards adaptable security for energy efficiency in wireless sensor networks. *Proceedings of the 28th Meeting of the Wireless World Research Forum (WWRF'12)*, 1-6.

Koganti, N., Tamei, T., Matsubara, T., & Shibata, T. (2013,). Estimation of human cloth topological relationship using depth sensor for robotic clothing assistance. *Proceedings of Conference on Advances In Robotics*, 1-6. doi:10.1145/2506095.2506146

Ogudo, K. A., Muwawa Jean Nestor, D., Ibrahim Khalaf, O., & Daei Kasmaei, H. (2019). A Device Performance and Data Analytics Concept for Smartphones' IoT Services and Machine-Type Communication in Cellular Networks. *Symmetry*, *11*(4), 593. doi:10.3390/sym11040593

Arora, P., Singh, A., & Tyagi, H. (2012). Evaluation and comparison of security issues on cloud computing environment. *World of Computer Science and Information Technology Journal*, *2*, 179–183.

Mandal, P. C. (2012). Superiority of Blowfish algorithm. *International Journal of Advanced Research in Computer Science and Software Engineering*, *2*, 196–201.

Seth & Mishra. (2011). *Comparative analysis of encryption algorithms for data communication.* Academic Press.

Nazir, S., Vukobratović, D., Stanković, V., Andonović, I., Nybom, K., & Grönroos, S. (2015). Unequal error protection for data partitioned H. 264/AVC video broadcasting. *Multimedia Tools and Applications*, *74*(15), 5787–5809. doi:10.1007/s11042-014-1883-8

Prasanthi, T., Balasubramanian, C., Selvi, S. K., & Kala, K. (2014). An Efficient Auditing Protocol for Secure Data Storage in Cloud Computing. *Proceedings of the World Congress on Engineering*, 2-4.

Chou, T.-S. (2013). Security threats on cloud computing vulnerabilities. *International Journal of Computer Science and Information Technologies*, *5*(3), 79–88. doi:10.5121/ijcsit.2013.5306

Stallings. (2000). *Network Security Essentials: Applications and Standards* (4th ed.). Pearson Education India.

Ding, X., Deng, Y., Yang, G., Song, Y., He, D., & Sun, X. (2016). Design of new scan orders for perceptual encryption of H. 264/AVC videos. *IET Information Security*, *11*(2), 55–65. doi:10.1049/iet-ifs.2015.0492

Apoorva, Y. K. (2013). Comparative study of different symmetric key cryptography algorithms. *International Journal of Application or Innovation in Engineering and Management*, *2*, 204–206.

Raya Basil Alothman is a researcher in the field of computer science and since 2000. She graduated from University of Mosul with a PhD in computer science in 2008, and master degree in computer science from Mosul university and B.S.c degree in computer science from Mosul university. Dr Raya Basil has publications in the field of network, image processing. She participated in many scientific conferences and symposia in different fields that serve the local community. She is now interested in the field of network security, information technology, image processing. Dr. Raya Basil Alothman started of the university of Mosul since 2000. Currently She is a member of the academic staff in the university since 2020.

Imad Saada is a researcher in the field of computer science and electronics since 2006. He graduated from Mansoura University-Egypt with a PhD in computer science in 2019, and master degree in computer science from Al-Quds university and bachelor degree in electronics engineering from Al-Quds university. Dr Imad Saada has about seven publications in the field of network routing protocols, network security, biometrics. He participated in many scientific conferences and symposia in different fields that serve the local community. He is now interested in the field of network security, sensors network, image processing. Dr. Imad Saada started in Al-Quds Open University as a technician in IT labs of the university since 2006. Currently he is a member of the academic staff in the university since 2010.