IMAGE SECURITY USING CRYPTOGRAPHIC ALGORITHMS WITH THE COMBINATION OF BASE64 ALGORITHM

A.L. Hanees[1] & S. Priyanka[2]

Correspondence: alhanees@seu.ac.lk

ABSTRACT

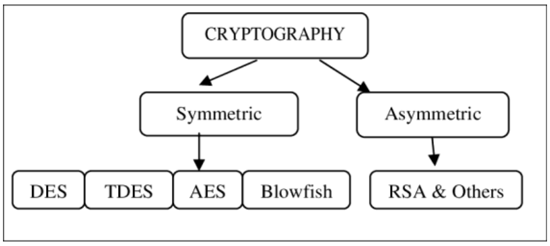
In this modern world sharing of multimedia messages became more and more popular among people. It leads them to face security threats. Here the encryption algorithms play an important role to reduce and get rid of those threats. Therefore, in this paper, a new method is proposed to increase the security and also the accuracy of image transfer. The original image is encoded into base64 string, then the encryption process and decryption process is done by one of the cryptographic algorithms on base64 string and the decrypted file is decoded in to the image. Base64 algorithm only can encrypt the image but it is less secure as anyone can access it. So that the cryptographic algorithms are used to increase the security. Also cryptographic algorithms can encrypt the image but accuracy will vary according to the algorithms. But in this proposed method both security and accuracy can be preserved. To prove that this method can work for other cryptographic algorithms five most common algorithms such as DES, TRIPLE DES, RSA, BLOWFISH, and AES are used combined with base64 algorithm individually. The algorithms are implemented in java language using IDE Netbeans. To evaluate the quality of the final image MSE, SNR, and PSNR are calculated and those algorithms are compared and analyzed using some factors such as time consumption and memory usage.

Keywords: cryptography, Base64, MSE, SNR, PSNR

1. INTRODUCTION

The security need is raised with the rapid growth of the information and communication industry. I.e. Data transfer, sharing valuable information across networks, storing data across the cloud, etc. Due to the advancement of technology in our society digital images, audios and videos are playing a major role than just plain and simple text, thus demanding serious protection of user privacy. When multimedia content is shared, it faces security threats. Here cryptographic techniques play a crucial role in information exchange. Multimedia encryption is the process of transforming Multimedia data stream (plaintext) into an unintelligible multimedia data stream (ciphertext) which helps to prevent unwanted and unauthorized disclosure of confidential information in transfer and storage. It aims to provide confidentiality, integrity, and availability.

Cryptographic algorithms can be categorized as in the following figure.



[1] Department of Mathematical Sciences, South Eastern University of Sri Lanka.
[2] Department of Mathematical Sciences, South Eastern University of Sri Lanka.

In symmetric / private-key encryption algorithms, a single key is used for both encryption and decryption. Both the sender and receiver are equivalent, and they can either encrypt or decrypt messages using that key. Private key cryptographic algorithms are generally categorized into stream ciphers and block ciphers. The most common private key algorithms are DES, Triple DES, AES, IDEA, TEA, Blowfish, etc. [2]. Public-key / asymmetric cryptographic algorithms use two keys. A public-key, that can be known by anyone and used to encrypt messages and verify signatures. A private key is known only to the receiver and used to decrypt messages, and sign (create) signatures. Therefore asymmetric cryptography is more efficient than the symmetric key cryptography because both the sender and the receiver have only one key to encrypt and decrypt all the messages in symmetric cryptography. The most common examples for asymmetric key cryptographic algorithms are RSA, ELGAMAL, and ECC, etc.[2]. In this method most common and suitable algorithms for multimedia encryption such as DES, TDES, AES, BLOWFISH, and RSA are considered.

DES: DES is a symmetric cryptographic algorithm that is the most widely used block cipher in the world. It was adopted by NBS (now NIST) in1977. DES follows the feistel structure. It encrypts 64-bit data using 56 bit key. It can be described in 2 steps.

1.1. Enciphering a 64-bit data block

An initial permutation (IP) shuffles the 64-bit input block. 16 rounds of a complex key dependent round function involve in substitutions & permutations. At last final permutation (inverse of IP).

1.2. Handling of the 56-bit key

An initial permutation of the key (PC1) selects 56-bits out of the 64-bits input, in two 28-bit halves. 16 stages generate the 48-bit sub keys using a left circular shift and a permutation of the two 28-bit halves.

TDES: Triple DES defines the use of three distinct DES keys, for a key length of 168 bits. TDES is established in order to overcome the inefficiency to protect against the brute force attacks. It has 2 methods.

1. Encrypt-Decrypt-Encrypt (EDE): It takes three 56 bit keys (k1, k2, k3) and first encrypt using key k1, next decrypt using key k2, and then again encrypt using the key k3.
2. Encrypt-Encrypt-Encrypt (EDE): It takes two 56 bit keys (k1, k2) and first encrypt using key k1, next encrypt using key k2, and then again encrypt using the key k1.

AES: As the key size used in DES is a small new method AES is established which is at least six times faster then DES. It is known to be vulnerable to exhaustive key search attacks. It performs on bytes rather than bits. AES takes 128 bits of a block as 16 bytes. These 16 bytes are arranged in four columns and four rows I order to perform as a matrix. It has 4 steps.

1. Byte Substitution
2. Shift Rows
3. Mix Columns
4. Add Round key

BLOWFISH: It is also a symmetric encryption algorithm developed by Bruce Schneier to replace DES. It also follows the Feistel structure. It uses the block size of 64-bit and key sizes range from 32 to 448 bits. Ha 2 stages.

1. Blowfish round function
2. Blowfish output operation

RSA: It is an asymmetric cryptographic algorithm which is most widely used for secure data transmission. It was published by Rivest, Shamir & Adleman of MIT in 1977. **RSA** is somewhat slow so it is rarely used to encrypt data, therefore to make it faster it is used to encrypt and pass around symmetric keys. It generates a public and private key.

This paper provides a brief idea about how the existing algorithm works to preserve security and quality when combining with the Base64 algorithm.

Related work: Paper [1] analyzed some common algorithms like DES, 3DES, AES, Blowfish, Twofish, ThreeFish, RC4 and RC6 in audio encryption and evaluated and compared using parameters like throughputs, speed, CPU time, Battery power and memory requirement.

Paper [2] Blowfish, AES, XOR, RSA algorithms are analyzed in text, image, audio, and video encryption and performance and time efficiency are evaluated. Concluded that AES is efficient than other algorithms.

Paper [3] proposed a new method that is able to shift the limit from the fourth LSB layer to the seventh LSB layer for transparent data hiding in the audio file. Here different types of audio files are used. The performance of the proposed method is analyzed using parameters such as SNR, PSNR, and MSE.

Paper [4] also proposed a new encryption algorithm for audio files based on a combination of block cipher and chaotic maps. This algorithm was performed and analysis with audio files of varies sizes of a WAV file extension. Analyzed using several factors such as keyspace analysis, statistical analysis, MSE (mean square error) analyses, PSNR (Peak Signal to noise ratio) analyses, and entropy analyses. It also proved that the algorithm is not vulnerable to brute force attacks, statistical attacks and achieve a higher level of security.

Paper [5] analyzed the algorithms such as AES, DES, 3DES, RC2, Blowfish, and RC6 in audio encryption using the parameters CPU workout and throughput. There were no significant differences between them. But the performance of blowfish is better than others when changing packet size. Different settings are provided for each algorithm.

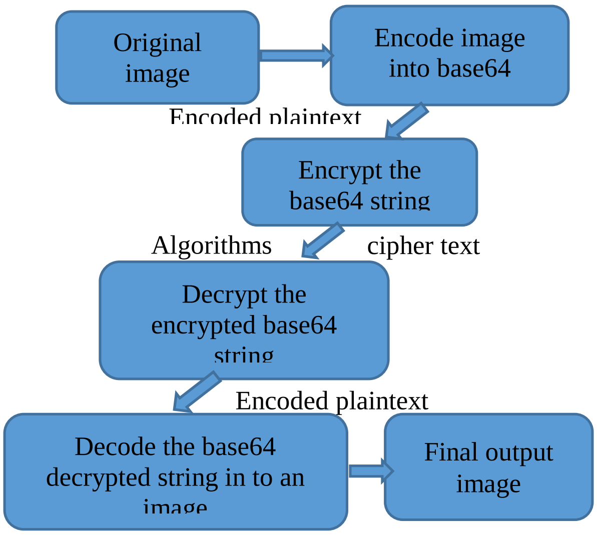
Paper [6] considered some common algorithms such as DES, TDES, AES, and Blowfish in text and other multimedia encryption and evaluated using factors such as throughputs, speed, CPU time consumption, power consumption, and security. Then concluded that AES and Blowfish gave better performance.

Paper [7] proposed a hybrid method that combines two techniques such as LSB and phase coding. The major disadvantages of the LSB have been overcome by using the phase coding to increase the robustness of the LSB. Also, the major disadvantages of the phase coding were addressed by using the whole signal and were not based only on the initial phase to increase the capacity of the embedding area of the phase coding. The efficiency is compared by determining the SNR (signal to noise ratio) value and the PSNR (peak signal to ratio) value.

Paper [8] proposed a robust audio steganography technique which consists of two steps such as randomizing and dynamically changing embedding sequence. In order to provide additional security and robustness to the proposed technique, AES is used. This technique is tested in 30 speech files and evaluated the final files using factors such as SNR and Correlation coefficients.

2. METHODOLOGY

Algorithms that suits multimedia encryption from existing algorithms are chosen. They are DES, TDES, AES, RSA, and Blowfish. Both base64 and cryptographic algorithms are implemented in java using IDE NetBeans. Four sample images were collected with different capacities while other factors are constant. Important measures such as Mean Square Error (MSE), Signal-to-Noise Ratio (SNR), Peak Signal-to-Noise Ratio(PSNR), Time consumption, Memory requirement, etc. to evaluate those algorithms are applied. Algorithms are compared with respect to the measures.



3. RESULTS AND DISCUSSION

Images with different capacities (every other aspect of images constant) such as 100kb, 500kb, 1000kb, and 2500kb are tested separately using DES, TDES, AES, BLOWFISH, and RSA with the combination of base64 algorithm. MSE, SNR, PSNR are calculated to prove that the proposed method is accurate. The time consumption and memory requirement are calculated in order to compare those algorithms.

If a vector of predictions generated from a sample of *n* data points on all variables, and X is the vector of observed values of the variable being predicted, with Y being the predicted values.

1. Mean Square Error (MSE)

MSE is the avalanche effect measure in which the total squared lapse is discovered between the original and encrypted images. Let two images, stored in X and Y vectors, is computed as follows [4]

$$MSE = \frac{\sum_1^n [x - y]^2}{M*N}$$

2. Signal-to-Noise Ratio (SNR)

Can be computed as,

$$SNR = 10 * log_{10} \frac{\sum_{i=1}^{n} X^2(n)}{\sum_{i=1}^{n} [X(n) - Y(n)]^2}$$

3. Peak Signal-to-Noise Ratio (PSNR)

PSNR is a measure describes the adjustment of image value qualities between the original and encrypted image. It can be computed as follows [4]

$$PSNR = 10*\log_{10} \frac{R^2}{MSE}$$

R^2 is known as maximum intensity.

Table 1. Quality Assessment for 100kb

100kb	**DES**	**TRIPLE DES**	**BLOWFISH**	**AES**	**RSA**
MSE	0.0	0.0	0.0	0.0	0.0
SNR	Infinity	Infinity	Infinity	Infinity	Infinity
PSNR	Infinity	Infinity	Infinity	Infinity	Infinity
TIME (ns)	472282800	391055200	264378200	203461200	14591906600
MEMORY (bytes)	4720808	12853824	4167808	4163136	371402584

Table 2. Quality Assesment for 500kb

500kb	**DES**	**TRIPLE DES**	**BLOWFISH**	**AES**	**RSA**
MSE	0.0	0.0	0.0	0.0	0.0
SNR	Infinity	Infinity	Infinity	Infinity	Infinity
PSNR	Infinity	Infinity	Infinity	Infinity	Infinity
TIME (ns)	1949942100	1271287200	851514900	916648900	542406691500
MEMORY (bytes)	2906256	27725056	21690352	21689904	589094264

Table 3. Quality Assesment for 1000kb

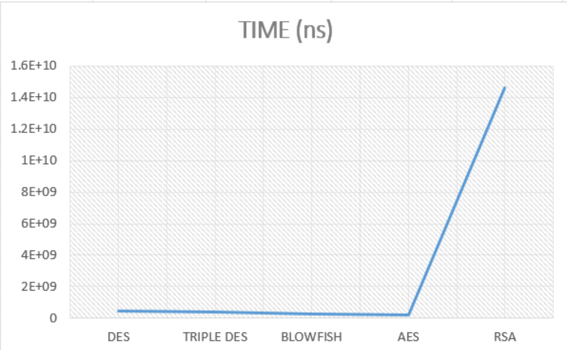
1000kb	**DES**	**TRIPLE DES**	**BLOWFISH**	**AES**	**RSA**
MSE	0.0	0.0	0.0	0.0	0.0
SNR	Infinity	Infinity	Infinity	Infinity	Infinity
PSNR	Infinity	Infinity	Infinity	Infinity	Infinity
TIME (ns)	3621980600	2179442700	1692744700	1935007100	1867248800600
MEMORY (bytes)	24917016	20150432	19584392	19331120	750716712

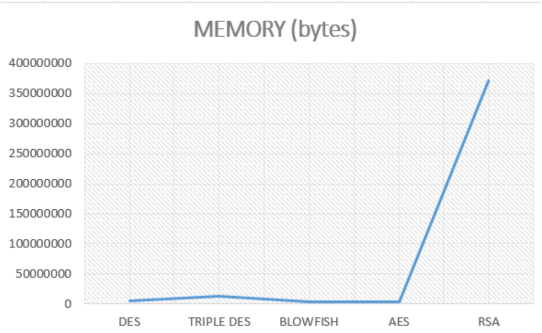
Table 4. Quality Assesment for 2500kb

2500kb	**DES**	**TRIPLE DES**	**BLOWFISH**	**AES**	**RSA**
MSE	0.0	0.0	0.0	0.0	0.0
SNR	Infinity	Infinity	Infinity	Infinity	Infinity
PSNR	Infinity	Infinity	Infinity	Infinity	Infinity
TIME (ns)	9278648900	4823236900	4439995100	4146831500	10008599005000
MEMORY (bytes)	34366344	43945632	68903928	68885760	1486948896

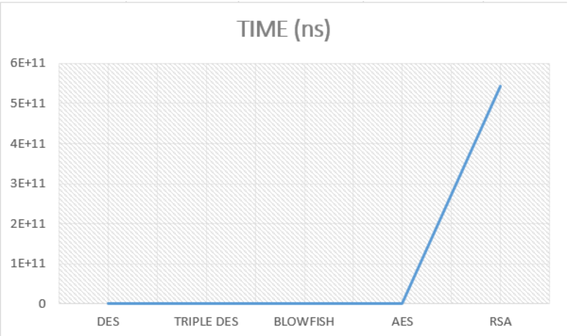
Results for 100kb, 500kb, 1000kb, and 2500kb also. Finally, results are analyzed and plotted in graphs to compare the algorithms. As the decrypted image is of the same quality as the original image value of MSE =0, SNR = infinity, and PSNR = infinity. MSE, SNR, And PSNR give the same value for all algorithms. Therefore, the graph analyzes the time and memory required.

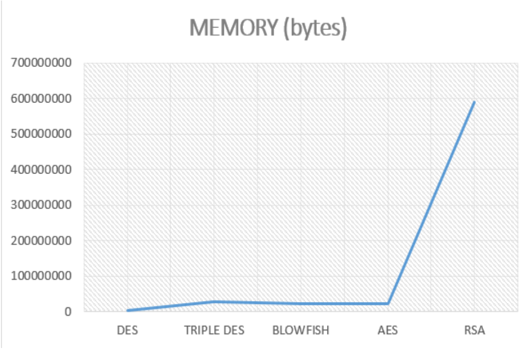
100kb



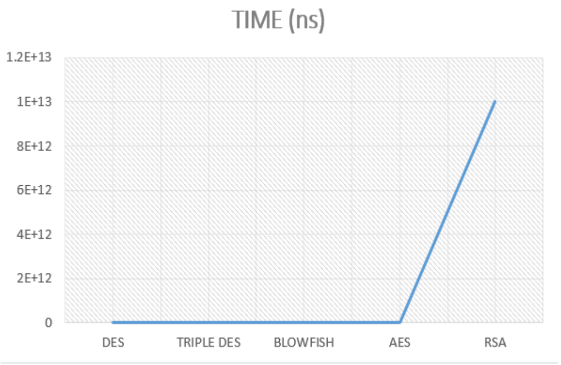


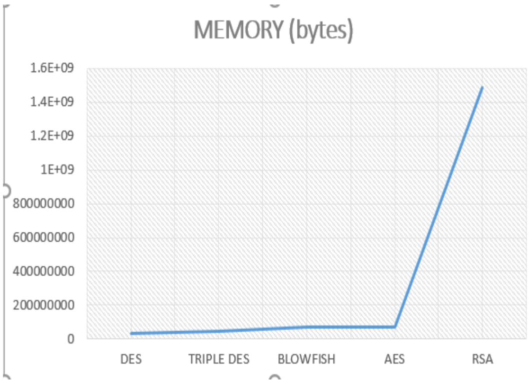
500kb



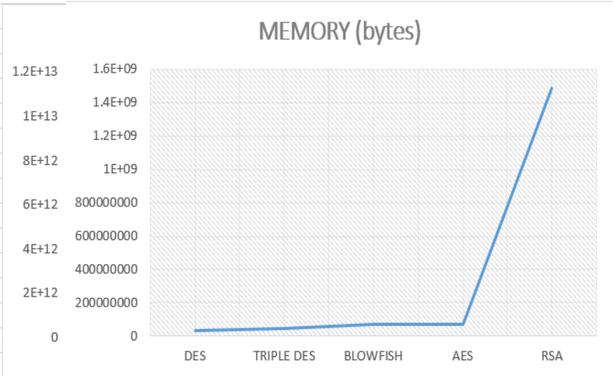


1000kb





2500kb



4. CONCLUSION AND FUTURE WORK

In this paper, it is proved that the proposed method is accurate through the MSE, SNR, and PSNR values. i.e. the original image doesn't get affected by the proposed encryption method. When the capacity of the given image increases the time consumption and memory requirement also increases. Therefore the comparison is done based on time consumption and memory requirement. As shown in the graph RSA algorithm required more time and memory. Other algorithms are almost similar in time consumption and memory usage. Anyhow it is depicted that Blowfish has good performance compared to the others in time consumption. AES shows good performance regarding time than capacity. Also DES requires less memory than others even when the capacity increases. The proposed method can be done for encrypting other multimedia messages such as audios and videos too in future in order to preserve better security and 100 percent accuracy.

REFERENCES

[1] C.Sasi varnan, A.Jagan, Jaspreet Kau, Divya Jyoti, & Dr.D.S.Ra. (2011). Image Quality Assessment Techniques pn Spatial Domain. *ISSN*, 177-184.

[2] Ch. Yaswanth, S., Ch. Hanuma, R., Gabbar, J., & M. Gowtham, R. (2015). Robust Audio Steganography based on Advanced Encryption Standards in Temporal Domain. *IEEE*, 1449-1453.

[3] Diaa Salama, A., Hatem, M., & Mohiy, M. (2010). Evaluating The Performance of Symmetric Encryption Algorithms. *International Journal of Network Security*, 213-219.

[4] Dr. Ekhlas, A. (2017). A New Audio Encryption Algorithm Based on Chaotic Block Cipher. *IEEE*, 22-27.

[5] Md, M., & Md, I. (2016). Comparison of Encryption Algorithms for Multimedia. *Rajshahi University Journal of Science & Engineering*, 131-139.

[6] Mohammed, M., & Fatma, T. (2016). The hybri technique for enhanching the audio stegonography. *modern education and computer science press*, 36-42.

[7] Mohsen, B., & Sublta, S. (2015). A new method to increase the capacity of audio Steganography based on the LSB algorithm. *Jurnal teknologi*, 49-53.

[8] Rashmi , A., & Atul, M. (2015). A Study on Current Scenario of Audio Encryption . *International Journal of Computer Applications* , 13-17.

[9] Rashmi , A., & Dr. Atul , M. (2016). Audio Encryption with AES and Blowfish . *Audio Encryption with AES and Blowfish* , 671-679.

[10] Ratinder Kaur, & V. K. Banga . (2012). Image Security using Encryption based Algorithm. *ICTEEP*, 110-112.