Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 00 (2023) 000–000

Procedia Computer Science

www.elsevier.com/locate/procedia

8th International Conference on Computer Science and Computational Intelligence (ICCSCI 2023)

Time-Based Steganography Image with Dynamic Encryption Key Generation

Kevin Wijaya[a], Bryan Lansky[a], Cecilia Ariani Dewi[a], Rojali[a], Ghinaa Zain Nabiilah[a]

[a]*Computer Science Department, School of Computer Science, Bina Nusantara University, Jakarta, Indonesia 11480*

Abstract

The rapid advancement of technology has necessitated stronger protection measures for data exchange. Encryption, coupled with robust keys, is an effective method to safeguard sensitive information. This study aims to improve the security of key levels by implementing a combination of steganography and encryption. The approach involves using two keys, one in the form of a normal string and the other based on the insertion time. These keys are combined to create a new, stronger encryption key. The secret messages are then encrypted using this new key and inserted using the Least Significant Bit method in steganography. This integrated approach aims to provide a higher level of protection for data during transmission and storage

Keywords: Cryptography; LSB; AES; Image; Time Key Encryption

1. Introduction

At the time when the internet was unpopular, information exchange was done using written media, such as sending letters or writing memos. This process often requires quite a long time to reach the destination, especially over long distances. Within the appearance of the internet network, the information exchange gets more rapid, easier, and more efficient. Humankind is now able to use email, chat, or any social media to do instant information exchange without being limited by distance. Besides, with an internet network, worldwide information access becomes easier as it is accessible with the internet.

However, internet network usage also comes with a security risk to watch out for, like private information leak /cyber-attack which destroys security and information integrity exchanged through the internet. Therefore, we as an

internet network user shall understand the role of information security and implement the right security act to protect our privacy. To prevent information / data leak, the cryptography protocol, a security practice to send a message as well as keeping the secrecy of the message.

The Advanced Encryption Standard algorithm may be done to protect sensitive or confidential data / information. AES is a symmetrical cryptography, which is used to encrypt and decrypt data efficiently. This algorithm uses the same encryption key to encrypt and decrypt data. One of the advantages of the AES Algorithm is the data processing efficiency and speed for every device type. Therefore, AES is highly common to use as a security standard to protect confidential and important data. AES gives assurance for unauthorized parties to be banned from reading secret data, so that it is the right choice for our information security.

Steganography is a method to hide confidential messages on a certain media so that unauthorized people are unable to see. Secret information is inserted into a media such as an image, video, audio, or other types of document by modifying pixel / bit value. There are also a lot of algorithms/steps to enhance the security of messages / information. Steganography is usually used for communication security and secret message / data hiding [11].

Time-based encryption offers tighter access control for sensitive data by limiting decryption to specific time periods. This ensures that unauthorized or premature access is prevented until the specified time. It is particularly useful when sharing confidential information, as the recipient can only access the data after a certain time limit, providing additional rules for accessing sensitive information. This feature is beneficial in situations where compliance or legal requirements necessitate delayed access. Overall, time-based encryption enhances security and control over sensitive data by limiting access and providing time limits for stakeholders to read hidden files.

2. Literature Review

In the world of cybersecurity, there is the science of cryptography and steganography, where encryption and decryption are important parts of cryptography. There are many types of encryptions, such as Advanced Encryption Standard, Blowfish, Chaotic map, and many more. Each algorithm has its own strengths and weaknesses. Steganography also has many techniques for embedding data, including Least Significant Bit, Pixel Value Differencing, modulus function, Discrete Wavelet Transform, and others. The selection of embedding techniques is also important, just like encryption, it must be tailored to the specific needs.

Steganography may seem like watermarking media, but as Omar Elharrouss, Noor Almaadeed, and Somaya Al-Maadeed stated, there are differences between the two [5]. Therefore, it is important to distinguish between them and choose the appropriate technique by comparing existing algorithms, as stated by D Darwis N B Pamungkas and Wamiliana [7]. Additionally, steganography techniques can be developed, as demonstrated by Endang Ratnawati Djuwitaningrum, who improved the LSB technique from changing only 1 bit per pixel to 6 bits per pixel to increase capacity [8].

Not only cryptography and steganography play a critical role in data security, but also the system design and the creation process. For example, Imam Prayogo Pujiono and Eko Hari Rachmawanto created a new key obtained by combining several n keys [2], while Sarah Kareem Salim, Mohammed Majid Msallam, and Huda Ismail Olewi combined two images using LSB and Blowfish [3]. Furthermore, Sahera A. S. Almola, Najat H. Qasim, and Hamid Ali Abed Alasadi merged a secret image with a cover image [1].

All these aspects are important for ensuring data security. However, there are also aspects of data transmission, as described by Acqueela G Palathingal, Anmy George, Blessy Ann Thomas, and Ann Rija Paul who used cloud as a data transmission medium [9]. As for password security, it can be improved by encrypting passwords using keys known only to the user, as discussed in Hamdan Dian, Riza Arifudin, and Alamsyah's article [10]. According to Zahraa Salah Dhaief, Raniah Ali Mustafa, and Amal Abdulbaqi Maryoosh [6] and Ashwak ALabaichi, Maisa'a Abid Ali K. Al-Dabbas, Adnan Salih [4], it is also important to hide the communication flow by applying random patterns to avoid detection.

3. Method

3.1. Cryptography

Cryptography derives from Greek, kryptós which means "secret" and γράφειν which means "to write". Combine those two words together, and then it means secret writing. So, cryptography means expertise / knowledge regarding communication procedures between 2 parties or more based on a well designed security protocol so that unauthorized parties are unable to find out.

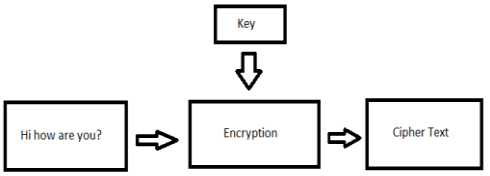


Fig. 1. Encryption.

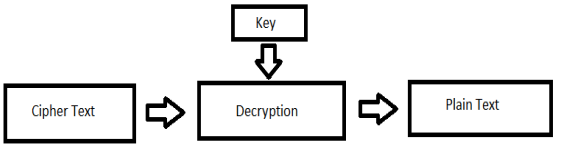


Fig. 2. Decryption.

In the encryption process shown in Figure 1, a message is entered into an encryption algorithm with the help of a key to produce a unique and unreadable ciphertext. Encryption was done to generate Cipher Text.. Next is when Cipher Text is changed to a readable format called decryption. The decryption process starts by taking Cipher Text to be decrypted using the same key. In the decryption process shown in Figure 2, a ciphertext/message resulting from encryption is entered into a decryption algorithm. The decryption algorithm is the inverse of the encryption algorithm to transform the ciphertext back into its original form.

3.2. Advanced Encryption Standard (AES)

Basically AES works by taking a message to be encrypted and do a partition to small blocks of data to be encrypted separately. After all blocks of data are encrypted, the encryption results of every block are merged back together to become an encrypted message. This process resembles the merge sort algorithm which works by doing a partition, sorting, and finally merging.

AES uses a symmetrical key, which means the same key will be used for the encryption and decryption processes. AES also have a few encryption modes to choose from, based on the requirements such as :

- ECB (Electronic Code Book)
- CBC (Cipher Block Chaining)
- CFB (Cipher Feedback)
- OFB (Output Feedback)
- CTR (Counter)
- GCM (Galois/Counter Mode)

One most common encryption mode is CBC (Cipher Block Chaining), where every block of data is encrypted using the same key, however the encryption result is influenced by the previous block as the name suggests, chaining. Types of AES are divided into three by the length of the used key, which are 128, 192, 256. Each key has different rounds, AES 128 has 10 rounds, AES 192 has 12 rounds, and AES 256 has 14 rounds.

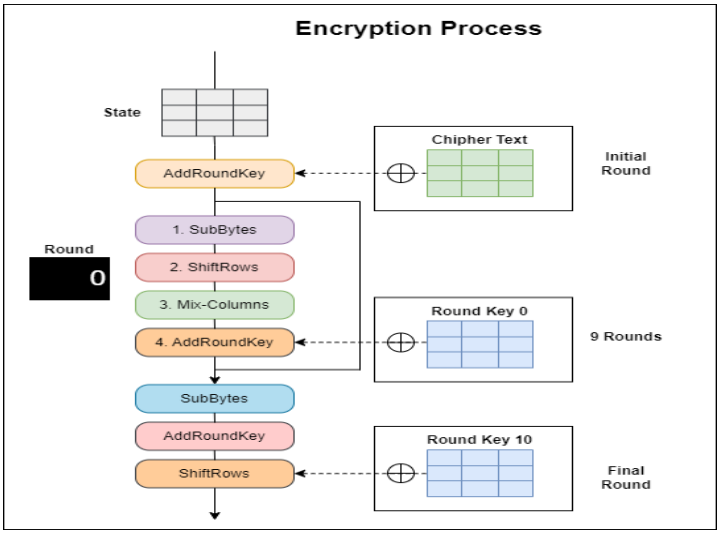


Fig. 3. AES Encryption.

The encryption process consists of several steps, namely Sub-Bytes, ShiftRows, MixColumns, and AddRoundKey, as shown in Figure 3. This process is repeated for 10 rounds, consisting of 9 rounds and 1 final round.

1. Sub-Bytes : a non-linear substitution step where each byte is replaced with another value from table (Figure 4).

	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xa	xb	xc	xd	xe	xf
0x	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1x	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2x	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3x	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4x	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5x	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6x	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7x	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8x	cd	0c	13	ed	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9x	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
ax	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
bx	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
cx	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
dx	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
ex	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
fx	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Fig. 4. S-Box.

2. ShiftRows : a transposition step where the last three rows are shifted to the left by the number of levels of that row.
3. MixColumn : a linear mixing operation which matrix multiplication of the matrix generated in the previous stage with a multiplication matrix called the dot product.
4. AddRoundKey : each byte of the state is combined with a byte of the round key using XOR operation.

3.3. Image Media

Image or picture is a combination of dots, lines, planes and colors representing the visuals of an object in 2D. An image can be made from various acts or tools such as painting, cameras, and image processing software applications. In the computer world, an image or picture holds the meaning of a group of zeros and ones that is called the binary language. The binary language then is parsed by a computer program, producing a complete picture shown in a monitor visible to the human eye.

There are a few image format variations in a computer which are JPG, JPEG, PNG, and BMP. Each of these image format has its own strengths and weaknesses, which determines the purpose / usage.

- JPG/JPEG (Joint Photographic Experts Group). This format has a relatively small size due to data compression without ruining the quality of the picture (Lossy Compression). Due to high compression rate, it results to this type of image having the blur effect in images with a lot of details.
- PNG (Portable Network Graphics). This format is suitable for images with a lot of details, resulting in the image having a bigger size than JPEG.

- BMP (Bitmap). This format has simplistic data and the image quality generated is great especially for a highly detailed image, but the weakness is the size will be too big as a result of no data compression. If compression is done, the image quality will be ruined.

The resolution of an image is represented by the amount of pixels x pixels, for example 300x300, then the image has 90000 pixels. The bigger the resolution / dimension, the bigger the image file size becomes. Each pixel has various bit depths, which are 8, 16, 24, and 32 bits, meaning that each pixel may need 1 until 4 bytes to produce that 1 pixel color. If the bit depth of a pixel is high, that shall give more color variations. As the example 8-bit produces 256 color variations, 16-bit produces 65.536 color variations, 24-bit produces 16.777.216 color variations, and then 32-bit produces 4.294.967.296 color variations.

The 24-bit format is widely known as RGB (Red, Green, Blue), where the first byte is used by red, the second is used by green, and the third is used by blue. Those three basic colors are combined into one producing new colors such as brown, purple, and etc. The 32-bit format a.k.a ARGB (Alpha Red Green Blue), is the enhanced version of RGB with an additional feature called Alpha Channel. Alpha Channel is equal to opacity, the component responsible for managing the transparency of a pixel, 0 value implies a transparent pixel and 255 implies a completely not transparent one. In this research, the image file used is in format PNG with the bit depth of 32(ARGB).

3.4. Dataset

BOSSbase, which stands for "BOutique of Speech and Signal Processing database," is a well-known and commonly used image database in the field of steganography research. It contains color images in JPEG format that are utilized as cover objects for concealing secret messages using steganographic techniques. The database is thoughtfully curated to provide a diverse and representative collection of images that are suitable for evaluating the performance of steganographic algorithms. BOSSbase includes a wide range of images with varying image quality factors, such as compression levels, resolutions, and color depths. This enables researchers to simulate real-world scenarios where steganography may be applied and assess the effectiveness of their steganographic methods in different conditions. The database comprises both natural images, which are real-world images, and synthetic images, which are artificially generated, covering a wide range of image content, including landscapes, objects, and textures.

3.5. Steganography

The word steganography derived from the word steganos, meaning hidden / covered. Steganography is a study of the arts of hiding a message in a certain media so that the sender and receiver exclusively knows it. The steganography science has been existing since thousands of years in Greece, and at that time steganography was done using the human media. Specifically the hair of the slaves were shaved bald, then a secret message was written. The slaves then were sent to the message receiver when their hair had grown, which made the message unnoticable to other parties. Steganography isn't always described with complicated implementation, a simple example is : when we make a word file with words whose colors are changed into white; that is a simple steganography implementation. Another example is writing using a pen with invisible ink, and only visible using a flashlight upon the sentences.

In the computer world, steganography can be implemented into a lot of file types such as image, audio, and video. There are also tons of ways to insert secret messages into the files mentioned above, one of it is Least Significant Bit (LSB). LSB is an insertion method into the last bit of a byte. Initially the message is converted into bytes so that every bit inside is acessible. According to the previous chapter, 1 pixel may have 32 bit depths or 4 byte, in the last byte which is the blue part is where 1 bit of the message is inserted. The effect of LSB makes the ARGB value either increase or decrease by 1, however this is not a problem. The change occuring in the image is insignificant, even hard for a human's bare eyes to realize. Despite the advantages of using LSB, there is also a disadvantage; the amount of messages able to be inserted are limited.

The amount of messages which fit for insertion is based on the size of the image, the bigger size it has, the more messages can be inserted or it has linear correlation. However the implementation of this algorithm can be optimized. The standard one can only hold 1 bit of secret message per byte, the optimized version can hold more so that the amount of messages inserted can double up.

1.LSB Insertion	2. LSB Extraction
Character = A = 01000001	
Pixel 1 = 125 = 0111 1101, replace with 0 = 0111 1100	Pixel 1 = 0111 1100, takes the last bit = 0
Pixel 2 = 234 = 1110 1010, replace with 1 = 1110 1011	Pixel 2 = 1110 1011, takes the last bit = 1
Pixel 3 = 123 = 0111 1011, replace with 0 = 0111 1010	Pixel 3 = 0111 1010, takes the last bit = 0
….	….
Pixel 7 = 150 = 1001 0110, replace with 0 = 1001 0110	Pixel 7 = 1001 0110, takes the last bit = 0
Pixel 8 = 190 = 1011 1110, replace with 1 = 1011 1111	Pixel 8 = 1011 1111, takes the last bit = 1
	Character = 01000001 = A

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

Mean squared error (MSE) is a calculation to measure the number of errors in a statistical model. This calculation computes the average of the differences between the observed and predicted values. When a model has no error, the MSE is zero. Likewise, as errors increase, the MSE value will also increase.

$$MSE = \frac{1}{m\,n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

Information:
m = Width
l = Length
K = Result media
I = Original media
(i,j) = Pixel Coordinate

PSNR (Peak Signal-to-Noise Ratio) is one of the measurement methods used to measure the quality of images or videos by comparing the original image with the resulting image. PSNR is calculated by measuring the ratio between the maximum media value and the level of noise present in the resulting image. The PSNR value is measured in decibels (dB), and the higher the PSNR value, the better the quality.

$$PSNR = 10\,.\log_{10}(\frac{MAX_I^2}{MSE})$$
$$= 20\,.\log_{10}(\frac{MAX_I}{\sqrt{MSE}})$$

Information:
MAX_I = Maximum Pixel Value

After calculating the MSE in a model to find the level of error, the value is then used in PSNR calculation to ultimately obtain a PSNR value. This value is then used to determine criteria with qualitative values based on the table below.

Table 1. PSNR Value.

Distortion Level	PSNR Value
<20 dB	Very poor
20 dB - 25 dB	Poor
25 dB - 30 dB	Fair
30 dB – 35 dB	Good
35 dB – 40 dB	Very Good
>40 dB	Excellent

3.7 Length of Key and Time Key

Time can be used as a good key because it has a selected punctuality probability of 0.0694%.

$$\frac{1}{(24*60)} * 100\% = \frac{1}{1440} * 100\% = 0.0694\%$$

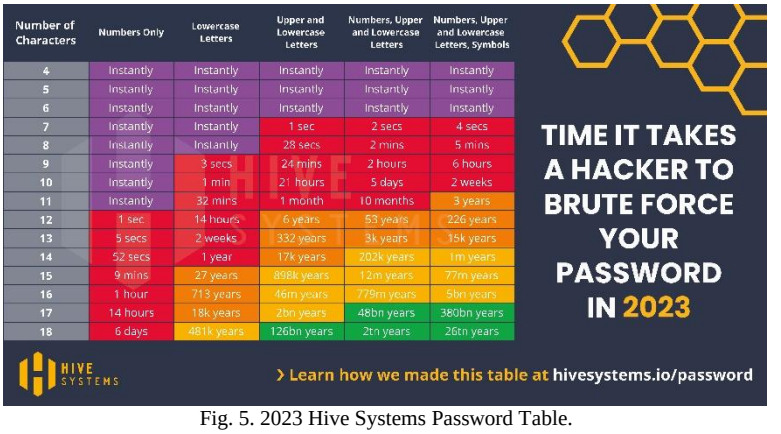


Fig. 5. 2023 Hive Systems Password Table.

The table above shows the time required by a hacker to crack a password using brute force techniques. Based on the data provided, the longer and more varied the used characters, the longer the time needed.

4. Result and Discussion

This program focuses on the implementation of a time key encrypted with a user key to create a third key, namely the message key, using the AES (Advanced Encryption Standard) encryption method. The aim is to create multiple layers of security to make it difficult to be hacked. The implementation is developed using Java programming language with JDK Java 18. The program is divided into 4 Java classes, which are:

- Steganography, which contains methods to insert and extract messages in a cover image.
- AES, contains methods to encrypt messages using the Advanced Encryption Standard algorithm.
- Time serves as a helper class to retrieve the current time in hours and minutes.
- Steganography App serves as the main code that will be executed first.

4.1 Flow Chart

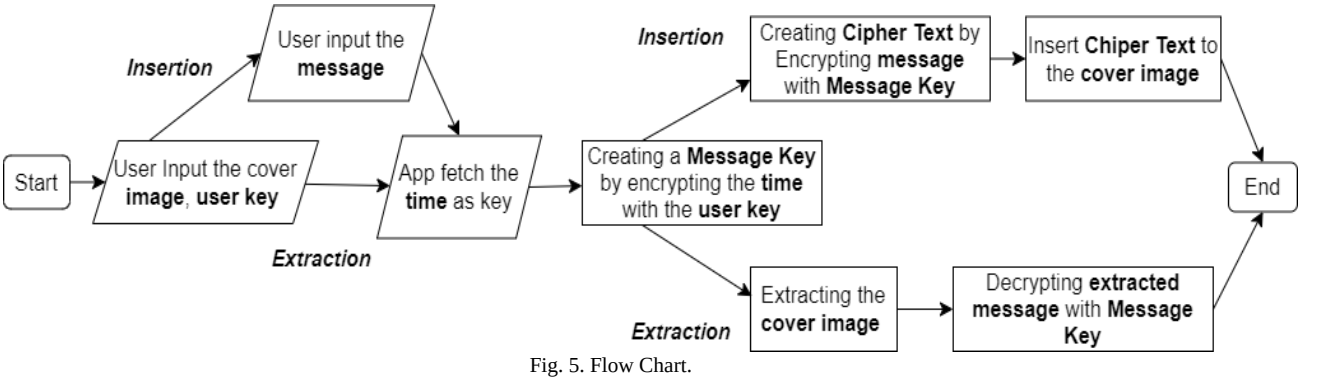


Fig. 5. Flow Chart.

Insertion

1. The user inputs the Cover image, user key, and message.
2. The application will fetch the time as the time key.
3. Application encrypts the time with the user key to create a third key, which is the message key.
4. The user's input message will be encrypted using the message key to produce the cipher text.
5. The cipher text is then embedded into the Cover image.

Extraction

1. The user inputs the cover image and user key.
2. The application retrieves the time as the time key.
3. Application encrypts the time with the user key to create a third key, which is the message key.
4. The cover image is extracted to retrieve the secret message, and then decrypted with the message key.
5. The decrypted result is displayed.

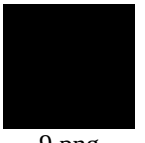
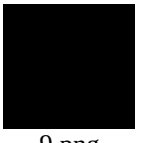
4.2 Result

Table 2. Experiment Result

Image Name	Encryption Key	Time	Message Key	Secret Message	Cipher Text
1.png	river	14:25	QdcwMwy13nh mufHwyik0wQ==	Hi there, are you okay?	8+Vtf7lNx1nnOXiqnGBrsePy1u5qsDf LZEm/giZVKuk=
2.png	house	14:25	8hQ4llmal6Ve1y 2Jrk8TOg==	I Can't See My Forehead	W+YP0KHbKRfpnU3HZp9ItAW0buv Xq5IGzCwn/vAHZtM=
3.png	treeAndLeaf	14:25	ojsfnSCi0OYu/w2 4gKPnQQ==	Well Maybe It Is Stupid, But It's Also Dumb	zmBqP8n7wjj9QjQ1NJfpSNQ28y0R 1U4CiKxMXspwc4vgBLpGaTJVykb NTC0knvJi
6.png	weAreBinusian	14:25	L+plFy71A0jp24d 33uCiYA==	No, This Is Patrick!	eWxLjFFaTWydSL/aAMlanfrTJQ lslmch2vxcwXMhNXE=
7.png	webarebear	14:25	PZLEOF0zPB/WK EQ5O09mNw==	Sometimes we have to go deep inside ourselves to solve our problems	ZH9H8tZSIGd7jHRV3s2TwtPIDGIW fxijTc7CZ0JY3pijOLOjOx+XAEYlh Umw7NQhKr9XsvslXs+rqM3lKZT/ D3qgdJVgowzehakCt8IH2LQ=
9.png	deepblack	14:25	YCRGaE8mW4sgs fLhiJ7hpA==	Dumb people are just blissfully unaware of how dumb they are	6pWKAF21wJhfDb1wfio2+RA3zgtS JuSwLXla6BFfQi0cwEFC6GxF1XY 3U//t1nFiYI4txv+Q1l+JYsfgxUV2 Ag==
10.png	beaglepuppy	14:25	kDcvBEsWdDFHA we8M239DA==	I'm so loyal, I haven't bathed in weeks!	mcpeC4k1+mgbqCpiJR6jr4LQ6eBU wqxDDFv4lXO6HmMDAMXsaXDJz Ejo/Y88oB06
12.png	tailung	14:25	ts4FiJENj87vx8k2 xftdTA==	You cannot stop the unstoppable	K9nlMc7YKVxdXPEGWHis+/15cy8 jwMTOpaDaqqKPisg=

Table 3. Experiment Result

Cipher Text	Before	After	Previous Size	Afterward Size	Insert Time (ms)	Extract Time (ms)	PSNR Value (dB)
8+Vtf7lNx1nnOXiqnGBrsePy1u5 qsDfLZEm/giZVKuk=	 1.png	 1.png	59.9 KB	56.2 KB	338	116	79.32
W+YP0KHbKRfpnU3HZp9ItAW 0buvXq5IGzCwn/vAHZtM=			86.7 KB	82.0 KB	335	121	78.9

	2.png	2.png					
zmBqP8n7wjj9QjQ1NJfpSNQ28y0R1U4CiKxMXspwc4vgBLpGaTJVykbNTC0knvJi			113 KB	110 KB	344	172	77.89
	3.png	3.png					
eWxLjFFaTWydSL/aAMlanfrTJQlslmch2vxcwXMhNXE=			10.4 KB	10.1 KB	345	118	77.1
	6.png	6.png					
ZH9H8tZSIGd7jHRV3s2TwtPIDGIWfxijTc7CZ0JY3pijOLOjOx+XAEYlhUmw7NQhKr9XsvslXs+rqM3lK/D3qgdJVgowzehakCt8IH2LQ=			1.70 MB	1.69 MB	500	144	81.95
	7.png	7.png					
6pWKAF21wJhfDb1wfio2+RA3zgtSJuSwLXla6BFfQi0cwEFC6GxF1XY3U//t1nFiYI4txv+Q1l+JYsfgxUV2Ag==			538 bytes	795 bytes	331	114	73.4
	9.png	9.png					
mcpeC4k1+mgbqCpiJR6jr4LQ6eBUwqxDDFv4lXO6HmMDAMXsaXDJzEjo/Y88oB06			119 KB	50.2 KB	339	117	73.91
	10.png	10.png					
K9nlMc7YKVxdXPEGWHis+/15cy8jwMTOpaDaqqKPisg=			156 KB	65.9 KB	329	118	76.54
	12.png	12.png					
Original message is 5279 characters, inserted cipher text is 7041 characters			55,9 KB	69,9 KB	386	118	55,92
	Lena.png	Lena.png					

5. Conclusion

Based on the analysis conducted on a series of cryptography processes, including embedding and extracting using AES (Advanced Encryption Standard) and Least Significant Bit, it can be concluded that:

1. There are two keys used to create a new key that will be used to encrypt the secret message, namely the regular string key and the time key taken directly at the time of the insertion process.
2. The extraction and decryption process takes less than 1 minute due to the time format (hour: minute).
3. Using the AES encryption algorithm causes the encryption key for the secret message to become longer. This also affects the encrypted message itself, resulting in a much longer cipher text. For example, the image Lena.png has a secret message of 5279 characters, but after encryption, it becomes 7041 characters.

4. The number of characters that can be embedded in the image is equal to (picture width * picture height)/8, but it does not mean that the number of characters can be directly inserted according to that formula due to the reasons mentioned in point 3 above.

This research is focused on the use of layered keys which results in a slightly longer process and longer keys. Suggestions for future authors are:

1. The process of LSB (Least Significant Bit) can be further enhanced, such as by providing a certain pattern so that the insertion is not done sequentially.
2. This research uses the PNG format as the dataset, and it is expected that other formats can also be used as the data source.
3. The program can only execute images with a bit depth of 32, and it is expected to improve the embedding algorithm so that images with a bit depth of 8, 16, 24, and above 32 can also be processed.

References

[1] Almola, S. A., Qasim, N. H., & Qalasadi, H. A. (2022). Robust Method for Embedding an Image Inside Cover Image Based. Informatica, 46, 53-60.
[2] Pujiono, I. P., & Rachmawanto, E. H. (2023). The Implementation of Improved Advanced Encryption. Journal of Applied Intelligent System, 8(1), 69 – 80.
[3] Salim, S. K., Msallam, M. M., & Olewi, H. I. (2023). Hide Text in An Image Using Blowfish Algorithm and Development of Least Significant Bit Technique. Indonesian Journal of Electrical Engineeering and Computer Science, 29(1), 339-347.
[4] ALabaichi, A., Al-Dabbas, M. A., & Salih, A. (2019). Image Steganography Using Least Significant Bit And Secret Map Techniques. International Journal of Electrical and Computer Engineering (IJECE), (10)1, 935-946.
[5] Elharrouss, O., Almaadeed, N., & Al-Maadeed, S. (2020). An Image Steganography Approach Based on K-Least Significant Bits (K-LSB). IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), (pp. 131-135). Doha, Qatar.
[6] Dhaief, Z. S., Mustafa, R. A., & Maryoosh, A. A. (2020). Hiding Encrypted Text in Image using Least Significant Bit image Steganography Techniqu. International Journal of Engineering Research and Advanced Technology (IJERAT), (6)8, 63-75.
[7] Darwis, D., Pamungkas, N. B., & Wamiliana. (2021). Comparison of Least Significant Bit, Pixel Value Differencing, and Modulus Function on Steganography to Measure Image Quality, Storage Capacity, and Robustness. Journal of Physics: Conference Series, 1-11.
[8] Djuwitaningrum, E. R., & Apriyani, M. (2018). Text Message Steganography Techniques Using Least Significant Bit Method and Linear Congruential Generator Algorithm. JUITA, (4)2,79-85.
[9] Palathingal, A. G., George, A., Thomas, B. A., & Paul, A. R. (2018). Enhanced Cloud Data Security using Combined Encryption and Steganography. International Research Journal of Engineering and Technology (IRJET), (5)3, 1856-1859.
[10] Dian, H., Arifudin, R., & Alamsyah. (2019). Security Login System on Mobile Application with Implementation of Advanced Encryption Standard (AES) using 3 Keys Variation 128-bit, 192-bit, and 256-bit. Scientific Journal of Informatics, (6)1, 34-44.
[11] Aditya, Y., Pratama, A., & Nurlifa, A. (2010). Literature Review for Multiple Steganography Methods. Seminar Nasional Aplikasi Teknologi Informasi 2010 (SNATI 2010), 32-35.
[12] Bossbase [Online Dataset]. (2020). https://www.kaggle.com/datasets/lijiyu/bossbase
[13] Animal [png] (2003). https://pngimg.com/images/animals/
[14] Binus University School of Computer Science BINUS UNIVERSITY [png]. https://socs.binus.ac.id/2013/02/21/logo-binus-socs/
[15] W, Ashly. (2022). Image [png]. https://www.oberlo.com/media/1603954479-toa-heftiba-0wajhfk7q9o-unsplash.jpg?fit=max&fm=webp&w=1824
[16] Vanish. Image [png]. https://www.vanisharabia.com/media/2448/color-meanings-and-moods.jpg?width=1140&height=489&center=0.5,0.5&mode=crop&format=webp&quality=70
[17] Hive Systems Password Table Use. (2023). https://www.hivesystems.io/password