International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 8 Aug 2023, pp: 428-437 www.ijaem.net ISSN: 2395-5252

Hybridization of Cryptography and Steganography to Achieve Secret Communication

[1]Molta Eli Danlami, [2]Lavi Linus Raymond, [3]Tashara Solomon
Modibbo Adama University, P.M.B 2076, Department of Computer Science, Adamawa State Yola, Nigeria

Date of Submission: 10-08-2023 Date of Acceptance: 20-08-2023

ABSTRACT: The combination of cryptography and steganography is a technique for transferring message in secure manner; hence we will employ this hybrid technique. First the model will be divided into two parts which is the Encode section and the Decode section. The message will be divided into two and then we will encrypt the first part of the message using blowfish algorithm and the second part using AES algorithm respectively. Python is chosen as main programming language to implement the hybridization of cryptography and steganography to achieve secret communication. Peak Signal to Noise Ratio (PSNR) will be used as quality assessment metric for determining the quality of a reconstructed image, the result obtained from hiding of the cipher text in the developed model is the output image (stego image). Encryption has a higher execution time over steganography across all the various message sizes; the wide margin is as a result of the use of two encryption techniques to increase the cryptographic strength of our model. This research work was successful in developing a new model for securing cloud data that employs the use of Blowfish, Advanced Encryption Standard (AES) and the Discrete Cosine Transformation (DCT). By utilizing the use of two cryptographic techniques and steganography, the difficulty of breaking the system by an attacker is increased.

KEYWORDS: Hybridization, Cryptography, Steganography, Communication

I. INTRODUCTION

Cryptography and steganography commonly work together to safeguard data confidentiality, integrity, and availability, which are crucial computer security issues. Cryptography and steganography use open network communication to send secret communications, such as documents, photos, or other data, to the receiver with the secret key. Computer Science uses cryptography and steganography for access control and information confidentiality. Many daily applications use them. Cryptography and steganography methods are being requested more for fast Internet development.

[1].Cryptography is the study of mathematical methods for data secrecy, integrity, entity authentication, and data origin authentication. Cryptography refers to the science of secret writing. Cryptography makes third-party data illegible. Symmetric (secret-key) and asymmetric (public-key) network security protocols use cryptography. Symmetric algorithms cypher and decipher plaintext using the same key. Asymmetric algorithms use public-key cryptosystems to exchange keys and quicker secret key algorithms to protect stream data. Public-key encryption methods use a pair of keys, one of which are public and encrypts data for a recipient who has the secret key. Key exchange is needed for private and public keys. Steganography conceals information. Thus, steganography differs from cryptography, where the message is visible but its meaning is hidden. Steganography hides data in innocent media. Steganographic findings can hide in media, network traffic, or disc space. Data can be used to hide information in different ways. Information Hiding has fascinated researchers for years. Digital forensic investigations face intriguing information concealment methods. Information can get through firewalls.

[2].Cryptography and steganography are extensively used methods for encrypting or concealing messages. Steganography conceals a message while cryptography encrypts it. If these methods are utilised separately, the intruder may discover the message. Thus, we propose combining them with higher security levels to create a highly secure data hiding system.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 8 Aug 2023, pp: 428-437 www.ijaem.net ISSN: 2395-5252

As data value and quantity rise, so does the relevance of information and communication networks for society and the global economy. Meanwhile, those systems and data are increasingly exposed to unauthorised access, use, misappropriation, change, and destruction. Millions utilise computers for banking, shopping, military, student records, etc. Many of these apps require us to protect messages from unauthorised individuals. Internet technology is growing fast. Internet is increasingly essential. With more internet users and faster access, everyone can get and share information. Popular internet networks are hazardous. Thus, confidentiality and information security are crucial, especially for sensitive messages. Steganography, cryptography, and watermarking solve these issues, making research in this area more intriguing.

[3].Communication is crucial to modern existence. Internet expansion and use have forced humans into the digital realm and digital communication. Data must be concealed when going through channels. Communication security is essential. Cryptography and steganography conceal crucial information. Covert communication with steganography is powerful. It obfuscates the meaning. Cryptography obscures messages. Many ways have been developed to encrypt and decrypt data to secure communication using cryptography. Unfortunately, keeping a message's contents and existence secret is sometimes vital. Steganography implements this. It's unseen communication. Hiding information in other information hides its existence. Digital data and networks are employed for steganography on computers today. Steganography hides the existence of a message, while cryptography hides its contents.

II. LITERATURE SURVEY

In today's world, communication is a need for everyone. However, in order for information to be exchanged via a communication channel, that channel must be secure, which means that no one can monitor that information. Therefore, we need a secure communication channel where no one may discover its presence. Steganography is utilised for it. Steganography is a method for concealing the existence of interparty communication. There are numerous choices for safe communication in daily life, including the phone, email, and others. But occasionally, it isn't secure to a certain extent. There are two methods that can be utilised to send data securely. These methods include steganography and cryptography. People come up with creative procedures for secret communication for a long time. In that direction, it gets so bad that no one who should know is able to analyse the data detection and recognise the presence of this data.

A variety of computerised material, including audio, video, images, and protocols, employ steganography to store information. But occasionally it will be defenceless against various types of assault. Digital steganography is employed for it. To confirm the sender's ownership of the copyright, digital steganography embeds the secret information in another piece of computerised data using a secret identifier.

[4].A method for obscuring communication between persons transferring information is steganography. People may access a wealth of information on the internet. Additionally, this knowledge is spread from person to person across the internet. However, attackers occasionally target the message. Therefore, if we convey the message in an image, music, video, or other multimedia file for security reasons, no one will be able to tell that the message is hidden within the multimedia file. Consequently, we can obtain data security utilising this. Because the message is hidden behind the image's background, even if an attacker were to gain access to our multimedia file, they would still be unable to obtain our original information. Attacker cannot thus readily obtain the original communication (Janki, 2015).

The main objective of cryptography is to let two parties to share private information, even if that communication is only possible through a channel that is being watched by an opponent. Replacement Cyphers. When was the last time you made an internet purchase? Recall all the images of accessories and gadgets you looked at? But what if they weren't truly meant for you? What if the trousers you were admiring were in fact extremely precise designs for military facilities? You would not be aware.

History of Steganography and Cryptography

[5].Steganography'spredecessor, cryptography, must first be understood in order to fully comprehend it. Information can be secured with cryptography by being converted into cypher text, an unintelligible form. This unreadable format needs to be decoded using a secret key. The development of cryptography has accompanied humankind through numerous stages.

Using unconventional hieroglyphics in an inscription, an ancient Egyptian scribe used cryptography as early as 1900 B.C. Hebrew scribes employed ATBASH, a reversed alphabet simple solution cypher, between 500 and 600 B.C. Julius Caesar employed a straightforward substitute with the standard alphabet in official communications

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 8 Aug 2023, pp: 428-437 www.ijaem.net ISSN: 2395-5252

between 50 and 60 B.C. Numerous forms of cryptography have been used throughout history. Quantum cryptography is the most advanced kind of encryption available today. Combining physics and encryption, quantum cryptography creates a new cryptosystem that cannot be broken without the sender and recipient being aware of the attempted and unsuccessful intrusion. Steganography has evolved and thrived on its own throughout the lengthy history of encryption. Greek words steganos (covered or secret) and -graphy (writing or drawing) are the roots of steganography. Steganography is the practise of concealing information by enclosing messages in other, ostensibly unimportant messages, pictures, or noises.

Around 440 B.C., the first steganographic method was created in ancient Greece. A primitive form of steganography was used by the Greek tyrant Histaeus, which included shaving a slave's head, tattooing the message on the slave's scalp, waiting for the slave's hair to grow out to reveal the secret message, and sending the slave on his way to convey the message. To read the message, the recipient would need to have the slave's head. The reply would be steganographically identical from the recipient.

Another early type of steganography was used about the same time. This technique featured Demerstus, who warned the Spartans in writing of impending Xerxes assaults. A fresh layer of wax was applied once the message had been carved into the wax tablet's wood. This tablet that appeared to be empty was successfully delivered with its secret message. Early 1600s saw the advent of steganography when Sir Francis Bacon utilised a different typeface to represent each piece of the encoding. Over time, steganography continued to advance to new levels. Steganography is widely employed in times of war. Both the British and American forces employed numerous kinds of invisible inks during the American Revolutionary War. For the hidden text, Invisible Ink used everyday items such as milk, vinegar, fruit juice, and pee. These messages have to be read with heat or light.

Microdots were first used by the Germans during World War II. The D1.1 microdots were complete paperwork attachments that were scaled down to the size of a period, including images, plans, and other content. Secret messages were also transmitted using null cyphers. Unencrypted transmissions that contain real messages hidden in the text are known as null cyphers. It was difficult to decipher hidden messages in the seemingly benign messages. Fishing freshwater bends and saltwater beaches rewards everyone who is feeling anxious, as shown by the following example of a harmless message with a null cypher. Resourceful fisherman typically enjoy seeing skilled leapers and acknowledge that swordfish are always more intimidating. Each word's third letter can be used to decode the following message: Send money, weapons, and attorneys. Techniques for Stenography in the Digital Age, the goal of both steganography and cryptology is to conceal communications in a particular medium. However, they differ significantly in that steganography relies on concealing the mere existence of a message whereas cryptography relies on hiding the meaning of the message. Surprisingly, steganography achieves this with little of its unique characteristics. This feat is made possible by the Internet's immense scale and the volume of data it contains; for this reason, it can be a particularly effective technique of protecting data transport.

The Caesar Cipher

The Caesar cypher is among the most well-known older encryption techniques. Gaius Suetonius Tranquillus, a Roman historian who lived between 70 and 130 CE, said that Julius Caesar employed this cypher to encrypt military messages by moving all of the plain text's characters three spaces to the right. The message Attack at Dawn, for instance, becomes "Dwwdfndwgdzq." The 'A' in the ordinary text is, as you can see, shifted three letters to the right to form a 'D' in the cypher text. Then, in the cypher text, the t from the ordinary text is moved three letters to the right to create a w. All of the plain text's letters go through this process. None of the shifts in our case extended past the letter z. What would happen if the letter Y was moved to the right three positions? The procedure would go around the entire alphabet, beginning with letter a. As a result, in the cypher text, the letter y would be changed to the letter b.

Cryptanalysis

[7].Caesar's cypher can actually be cracked in just 26 tries for the shift vector, and this can be done very quickly even by a human. Be aware that Eve must test the first few characters in each shift because, if she guesses incorrectly, the first few letters will probably result in nonsense. This is not the case with the simple substitution cypher; there are 26! > 1026 potential keys, which is an excessive quantity even for a recent PC. Even such a cypher text can be easily deciphered, though. The key idea is that straightforward substitutions do not change the fundamental

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 8 Aug 2023, pp: 428-437 www.ijaem.net ISSN: 2395-5252

properties of the underlying natural language, in this case, English. Eve can therefore make the following argument. The most common characters in a typical English text (which is what the message is supposed to be) are 'e', 't', 'a', 'o', and 'n'. Even their frequency may be calculated with ease (you can open a lengthy pdf file and count the occurrences of these letters by "bare" hand, or you can locate online tables that tell them). You can also take into account the trigrams "the," "and," and "ing," as well as the bigrams "the," "he," "an," "re," and "er." The point is that, for example, no matter which letter stands for 'e,' it will stand for 'e' always, and since 'e' is the most frequently occurring letter in English, this unknown character will be somewhat frequently in the cypher (and almost certainly the most frequently, if the cypher is long enough). If we count the frequently occurring letters, bigrams, and trigrams given the cypher text, we may have reasonable guesses on the substitution. This also holds true for other frequently occurring letters, bigrams, and trigrams. As soon as some of the text is made clear, we can determine more substitutes. We are able to recover the text after some trial and error. Even though it might appear difficult, this works remarkably quickly. As a historical aside, we mention that Arab intellectuals were aware of cryptanalysis and letter frequency counts in the 14th and 15th centuries. The usage of more complex cryptosystems than straightforward replacement cyphers at the same period shows that frequency analysis-based cryptanalysis was already known in Italian states.

Codebreaking

The most significant type of covert intelligence now used in the globe is codebreaking. Compared to spies, it generates a lot more accurate information, and this intelligence has a significant impact on how governments choose to implement their policies. A chronicler, however, has never existed. One is sorely needed. Even though it has been estimated that cryptanalysis prevented a year of fighting in the Pacific, history only briefly mentions it. Despite Britain's belief that it was crucial enough to send 30,000 people to the task, Churchill's epic history of World War II has been stripped of every single mention of Allied communications intelligence with the exception of one (and that is based on the American Pearl Harbour probe). There is no published history of World War II intelligence. All of this creates a skewed perception of what actually occurred. Additionally, just like other fields of human endeavour, cryptology can profit from understanding its key trends, notable figures, mistakes committed, and lessons learned.

Steganography

Johannes Trithemiu coined the term "steganography" for the first time in 1499. Stegano + Graptos are the two words that make up the term "steganography." Stegano, which means "Covered," and Graptos, which means "Writing," exactly translate as "cover writing." Steganography is thus defined as covered writing. Steganography is a unique method of obscuring data on a medium so that hackers won't suspect anything.

[8].The essential idea of steganography is that the message being transmitted must not be visible to the untrained eye. In order to prevent hackers from reading the message, the sender in this case embedded the message within the text, image, video, or audio file. This method is quite old and not new. The most popular Steganographic techniques employed by spies include the use of invisible ink and microdots. Design messages were once written on wax-coated wooden tablets. To expose the message, they tattooed the messenger's head, allowed his hair to grow back, and then saved it once more when he reached his contact point. Three essential elements are often needed for steganography: a carrier object, secret data, and a steganographic method. Steganography has a wide range of practical uses, including the safe exchange of sensitive information among defense organizations and between national and international governments, the security of online financial transactions, and the protection of military and intelligence organizations. The following elements of image steganography are generally of concern: Performance, Security, and Capacity.

This study focuses on a security issue. Additionally, despite the fact that a variety of carrier file types can be utilized in steganography, this research concentrates on image steganography because images are the most often used on the internet.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 8 Aug 2023, pp: 428-437 www.ijaem.net ISSN: 2395-5252

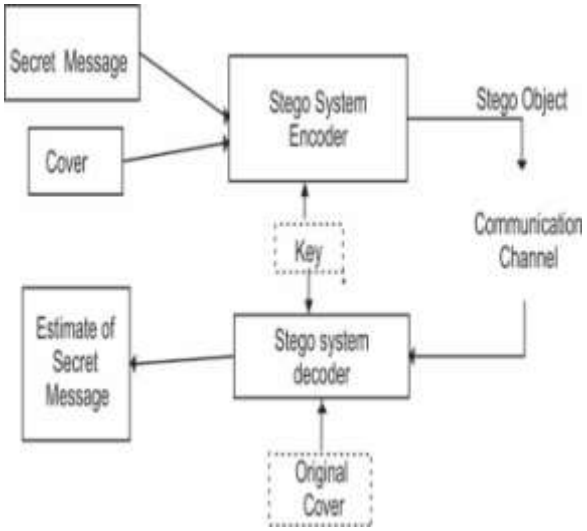

Figure 2.1: A typical steganography technique

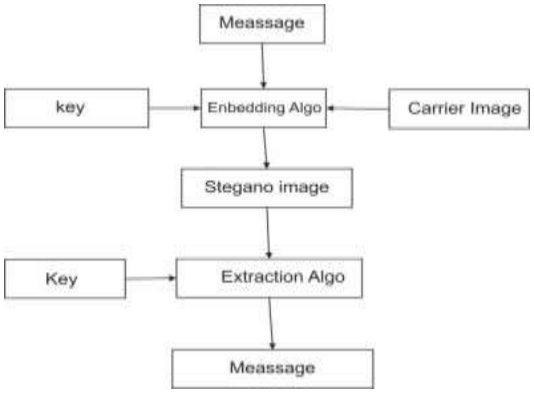

Figure 2.2 Basic Models for of Steganography for Embedding and Extracting Message.

Using steganography in text: In this, formatting is used to first embed the message to be conveyed in a text file. Line-shift coding, word-shift coding, feature coding, etc. are all used in the format. The rooted content is lost when text is reformatted, making the approach ineffective. Steganography used to hide messages in photographs is called image steganography. Due to the fact that hardly any changes are noticeable, this method is the most common. Less Significant Bits (LSB) replacement, in which the LSBs of the cover image pixel are changed to disguise the payload, is one of the frequently used techniques for embedding payload in cover images. Additional data can also be hidden in edges.

Audio steganography: This modifies audio files to include secret messages. The methods include echo hiding, phase coding, and LSB manipulation. Video steganography is a technique for concealing data or files in digital video formats. Hidden information is carried by video. The information in each of the video's images that is invisible to the human eye is often hidden using discrete cosine transformations (DCT). H.264, Mp4, MPEG, AVI, and other video formats are used for video steganography.

Cryptography

By transforming the text into a disgusting form, cryptography ensures that only the intended recipient can remove the discomfort and read the original secret message. The study of utilising mathematics to encrypt and decrypt data is known as cryptography. The practise of writing in secret, or cryptography, scrambles the message such that it cannot be deciphered. The term "cryptography" relates specifically to the technique used to hide the contents of messages; it is derived from the Greek words "Kryptos," which means concealed, and "graphikos," which means writing. Understanding how to change a message such that it cannot be

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 8 Aug 2023, pp: 428-437 www.ijaem.net ISSN: 2395-5252

read without the right method and key is known as cryptography.

[9].The development of cryptography has accompanied humankind through numerous stages. In his time, Julius Caesar employed the conventional alphabet substitution procedure for official communications. Today's encryption has advanced to a new level, and quantum cryptography has also been developed. A novel cryptosystem that cannot be broken without the sender and recipient is created by quantum cryptography, which integrates cryptography and physics.

Three different mechanisms are employed in cryptography: - Symmetric key encipherment, also known as secret key cryptography, uses the same key for both encryption and decryption. Public key cryptography, also known as asymmetric key encipherment, uses two separate keys, one of which is used for encryption and the other for decryption. The usage of hash functions for digital signatures is widespread.In many applications, using a hash function for message authentication has become the norm. Hash code is the output of the hash function.

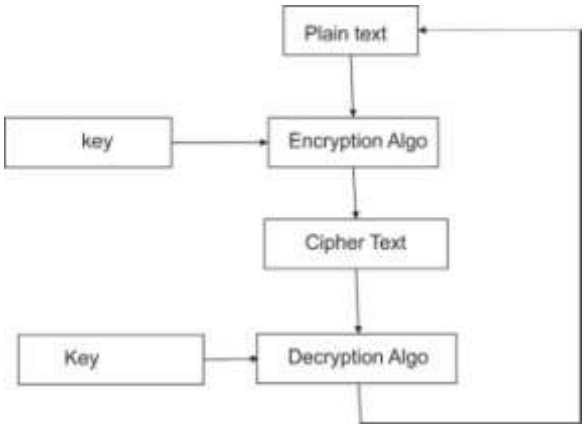

Figure 2.4: Basic Encryption and Decryption Process of Cryptography

Cryptography refers to the act of secret writing through the enciphering and deciphering of encoded messages. It is evidenced in situations where communication is established between two parties over an insecure medium which can be easily eavesdropped.

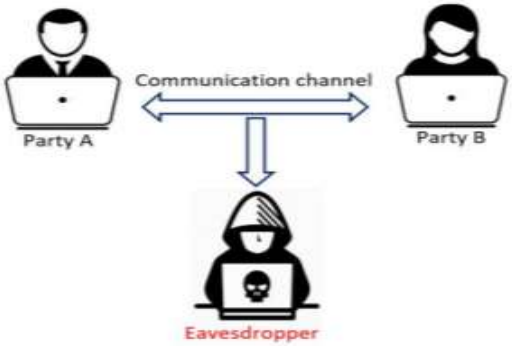

Figure 2.5 a basic pictorial of the encryption system.

Blowfish Algorithm

In 1993, Bruce Schneier created the Blowfish algorithm as a unique alternative to already-existing encryption algorithms including AES, DES, and 3 DES, among others (Archisman, 2020). Blowfish is a symmetric square encryption algorithm that was conceptualised using, Quick: It encrypts data at a rate of 26 clock cycles per byte on typical 32-bit microchips. Lessened: It requires less than 5K of RAM to continue operating. Important: It makes use of a 32-bit extended XOR lookup table. Secure: The key length is configurable and ranges from 128 bits to 32 448 bits by default. It is appropriate for applications like correspondence join or an updated record scrambled where the key is not frequently changed. The performance of blowfish is superior to other algorithms because it is unpatented and royalty-

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 8 Aug 2023, pp: 428-437 www.ijaem.net ISSN: 2395-5252

free. It has undergone extensive analysis, and it is gradually gaining acceptance as a reliable encryption technique. According to Monika and Jasmine (2014), blowfish is not copyrighted, has a free licence, and is publicly accessible for all usage. BLOWFISH is widely used because:

i. It has undergone extensive testing and been determined to be secure.
ii. It is quick because it makes use of the built-in instructions on modern microprocessors for simple bit-shuffle operations.
iii. It was made available to the whole public.

Advance Encryption Standard (AES) Algorithm

The symmetric key block cypher Advance Encryption Standard (AES) was created in 1998 by Joan Daemen and Vincent Rijmen. Any combination of data and a key length of 128, 192, or 256 bits is supported by the AES algorithm. AES permits a data length of 128 bits that can be divided into four fundamental operating blocks. These blocks are regarded as an array of bytes that are arranged in a 4 by 4 matrix that is also known as the "state" and is subject to rounds that perform various modifications. The number of rounds utilised for full encryption is variable N = 10, 12, and 14 for keys with lengths of 128, 192, and 256, respectively. The permutation and substitution network used in each round of AES is suitable for both hardware and software implementation.

Another cryptographic algorithm that can be used to protect digital data is AES. AES, which can encode and decode data in bits of 128 bits (16 bytes), is an iterative, symmetric-key square figure that can use keys of 128, 192, and 256 bits. Symmetric-key figures scramble and translate data using the same key, in contrast to open key figures, which employ many keys. The amount of bits in the encoded data that piece figures return is equal to the amount in the original information data. A circle structure is used in iterative figures to perform stages and replacements of the data information repeatedly. Electronic data encryption is governed by the Advanced Encryption Standard (AES). In 1997, the U.S. government acquired, and it is currently in use everywhere. The same key is used by both the sender and the receiver because AES is a symmetric-key algorithm. The Rijndael algorithm, a symmetric block cypher that can process data blocks of 128 bits with key sizes of 128, 192, and 256 bits, is described in this AES standard. Rijndael makes use of the input, output, and cypher key. It only accepts inputs and outputs with a block size of 128 bits or less.

III. METHODOLOGY

Cryptography and Steganography Model

The combination of cryptography with steganography is a way to securely convey messages; so, we use this hybrid technique. The model is first separated into two sections: the Encode section and the Decode section. The message will be divided into two parts, the first part will be encrypted using the blowfish algorithm, and the second part will be encrypted using the AES algorithm, implying that the encryption is hybrid because we are using two different encryption techniques for our cryptography just to enhance the security of the message. Finally, we will embed the message in an image using the DCT steganography technique, to obtain the stego-image. This stego picture is also transmitted to the receiver. So, even if an attacker sees the image, which is very difficult to detect the presence of a message in the image because it is secured with DCT steganography, the attacker will be unable to obtain the original message in a number of tries because the message itself is encrypted using two different encryption techniques solely to enhance security and confidentiality. To recover the original message, the receiver performs a reverse operation.

Encode

For the encoding first the message will be written then the message will be split into two halves the first section will be encrypted with key generation cipher using Blowfish Algorithm while the second part will be encrypted with key generation cipher using AES Algorithm, after that the two cipher text will be added together to become one cipher. Furthermore an image will be selected for hiding the encoded text, next we will use DCT to store the encoded message in the image and then encode the image, and lastly we transmit the encoded image.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 8 Aug 2023, pp: 428-437 www.ijaem.net ISSN: 2395-5252

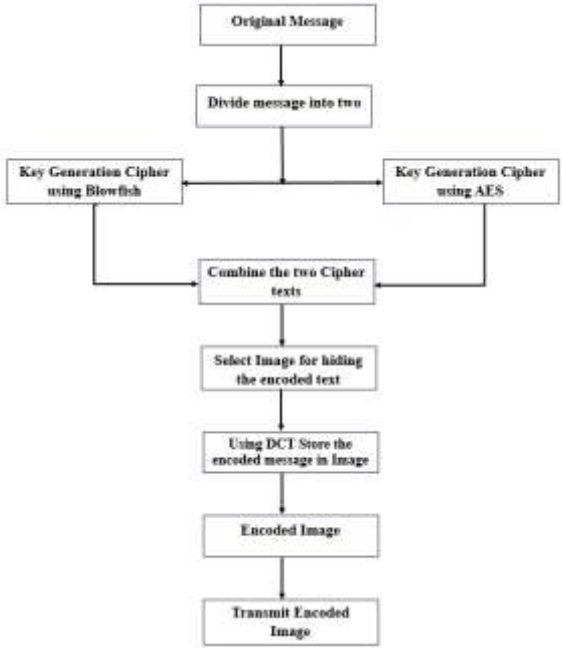

Figure 3.1 Proposed Model for Encoding the Hybrid Technique.

Decode

To decode the message is to reverse the encode process in order to retrieve original message. To decode the message on the receiving side first we the encoded image then we extract the cipher text using DCT^1, after getting back the cipher text we then divide it into two, then we decode the first part using symmetric key using Blowfish and the second part we decode the message using symmetric key using AES, after that we add the message together and from there we will obtain our original message.

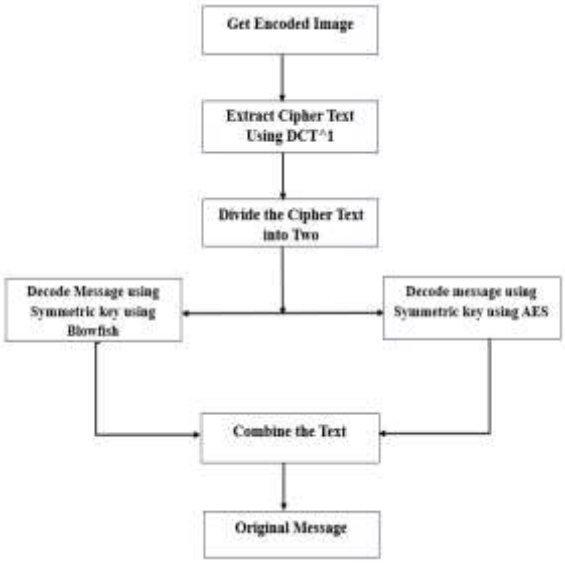

Figure 3.2 Models for Decoding the Hybrid Technique.

[10].The goal of cryptography is to ensure the secure and genuine transport of information while protecting conversations from prying eyes. It takes the plaintext message and changes it into ciphertext, which is incomprehensible. The key enables the user to decrypt the communication, allowing them to read it. The strength of an encryption is determined by the level of randomness, which makes it more difficult for anyone to guess the key or algorithm input. The

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 8 Aug 2023, pp: 428-437 www.ijaem.net ISSN: 2395-5252

integrity and validity of the conveyed communication will be achieved through the use of cryptography.

Blowfish

With blowfish symmetric encryption, data is encrypted and decrypted using the same encryption key. The encryption algorithm uses the sensitive data and the symmetric encryption key to transform the sensitive data into ciphertext. In this study, blowfish will be used to encrypt the first half of the message, creating a cypher text. The blowfish uses a single encryption key to both encrypt and decrypt data. Data encryption. Data encryption happens through a 16-round Feistel network, with each round consisting of a key-dependent permutation and a key- and data-dependent substitution. Blowfish utilises the same secret key to encrypt and decrypt messages, it is a symmetric encryption technique. Blowfish is a block cypher, which means that during encryption and decryption, a message is divided into blocks of a specific length. Blowfish uses blocks of 64 bits in length; messages that aren't a multiple of eight bytes must be padded. The two components of Blowfish are key-expansion and data encryption.

Advance Standard Encryption

AES is a symmetric encryption method since it uses the same key for both data encryption and decryption. Additionally, it employs numerous rounds of the SPN (substitution permutation network) method to encrypt data. The impenetrability of AES is a result of these encryption rounds, which are impossible to break through due to their sheer number. AES encryption keys come in three lengths. Different key combinations are possible for each key length. This encryption technique has a variable key length, but a fixed block size of 128 bits (or 16 bytes). Because of current technology, there is no excuse not to employ 256-bit AES encryption because the resource difference is so negligible. The second part of the message will be encrypted using AES which produces a cipher text also.

The art of steganography involves concealing a hidden message within (or even on top of) an otherwise public communication. Steganography is used to conceal and deceive. It is a type of covert communication in which the messages are concealed using any media. The art and science of concealing secret communications in cover messages so that no one but the sender and the intended recipient is aware of their presence. Since it doesn't require encrypting data with a key or scrambling data, it isn't a type of cryptography. It is actually a method of data concealment that can be used in cunning ways. Steganography is a technique that permits concealment and dishonesty, in contrast to cryptography, a science that generally promotes privacy. Picture steganography is the practice of concealing data by using the cover item as the picture. Images are frequently employed as a cover source in digital steganography because they contain a large amount of bits in their digital form. Although there are numerous methods for concealing information within an image, we employ the discrete cosine transform (DCT) technique.

Discrete Cosine Transform

JPEG compression uses the Discrete Cosine Transform Technique (DCT) and DCT coefficients. It divides the image into components with varying degrees of importance. It changes a signal or image's frequency domain from the spatial domain. It can divide an image into high, middle, and low-frequency components. In the low-frequency sub-band, which contains the majority of the visual information in an image, much of the signal energy is found, and high-frequency components of the image are typically eliminated through compression and noise attacks. So that the visibility of the image is not impacted, the secret message is encoded by changing the coefficients of the middle-frequency sub-band.

Testing

Different bits of data will be passed as the message in order to test the system and also different categories of images will be used and also check the compression and the distortion of the image in order to make sure the stego image looks exactly like the original image.

Programming language and libraries

Based on the context of the project, the language Python is chosen as main programming language to implement the combination of steganography with encryption to facilitate covert communication. Python is selected because of the ease of use and thousands of available libraries to be used to implement the needed algorithms. Regarding libraries, the first one is the input parse library which will be used to receive the text message from the user. Then, symmetric-key encryption will be carried out using the blowfish library. It supports a variable-length key of 4 to 56 bytes and has an 8-byte block size. It is quick, cost-free, and has undergone extensive analysis. Another library will be use is the pycrypyto library which will be used to implement AES encryption.

Using the "scipy library" method, we may compute the discrete cosine transform by choosing different kinds of sequences, and then use this method to return the changed array.

IV. CONCLUSION

This research work will be successful in developing a new model for securing cloud data that employs the use of Blowfish, Advanced Encryption Standard (AES) and the Discrete Cosine Transformation (DCT). By utilizing the use of two cryptographic techniques and steganography, the difficulty of breaking the system by an attacker is increased. An attacker may not easily discern that an image is carrying a message on it and by the time he does, he will realize it has been encrypted.

From the results presented, it can be noticed that the system is able to execute fast and can also hide a message in a cover image without creating high distortion. It can therefore be concluded that the proposed model is a strong competitor for providing secret communication and hence has achieved the set aim and objectives.

REFERENCES

[1]. Vishnu, S. B., & Helen, K. J. 2015.A Study on Combined Cryptography and Steganography. International Journal of Research Studies in Computer Science and Engineering, 2(5) 45 49

[2]. Setiadi, D. I. M., Rachmawanto E. H., & Sari, C. A. 2017. Secure Image Steganography Algorithm Based on DCT with OTP Encryption. Journal of Applied Intelligent System, 2(1,) 1-11

[3]. Rinsa, &Ayshamol, V. H. 2018. Security Enhanced Steganography in DCT Domain using Reversible Texture synthesis and AES Encryption. International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, 7(7), 18-20.

[4]. Janki, G. 2015. Image Steganography Based on Transform Domain, Blowfish and AES for second level security. COMPUSOFT, An international journal of advanced computertechnology, 4 (6), 1852-1856

[5]. Alan, S., Roger F., & Craig, L. 2020. The Rise of Steganography.An Overview of Steganography for the Computer Forensics. http://www.garykessler.net/library/fsc_stego.html

[6]. Chuck, E. 2016. Modern Cryptography: Applied Mathematics for encryption and information security. McGraw-Hill Education, 978-1-25-958809-9 Communications, pp. 1{22, 2016.

[7]. Peter, M. 2008. Introduction to mathematical cryptography. Budapest semesters in DNA steganography using hyper elliptic curve cryptography," Wireless Personal And Networking (WiSPNET), International Conference on. IEEE, pp. 2308{2312.

[8]. Mohammed, A. S. 2018. Image Steganography Techniques - A Review Paper.International of Computer Science & Information Technology, 2(3). 28-30. DOI 10.17148/IJARCCE.2018.7910

[9]. Khalid, I. R., &Manisha, M. 2015. Study of Cryptography and Steganography system. International Journal of Advanced Trends in Computer Science and Engineering, 4(8), 13685-13687

[10]. Dipti, K. S., &Neha, B. 2020. Proposed System for data hiding using Cryptography and Steganography. Bell System Technical Journal, 8(5), 1-10