Data Hiding In Image Using Cryptography And Steganography

Mr.N.M.K. Ramalingamsakthivelan[1], Ms.B Ramya[2]
[1]Associate Professor, Dept of Computer Science and Engineering
[2]Dept of Computer Science and Engineering
[1, 2] Paavai Engineering College, Namakkal.

Abstract- *Over the past few decades, with the development of the information society, computer networks and related applications have become more popular. The use of the Internet and reliance on a rapidly growing global network in daily life increases the number of network machines exposed not only to external attackers, but also to internal attackers, disgruntled employees, and people who abuse their rights. for personal gain. Valuable data is always vulnerable to peak attacks in the network. Attacks can be caused by system vulnerabilities or security breaches such as system misconfiguration, user misuse, or software defects. Attackers can combine multiple security vulnerabilities into a clever attack system. Therefore, an effective security model is needed to protect sensitive information through the network. However, several approaches have been proposed to improve the security of confidential information, but each has limitations. These limitations represent problems with current security systems and have led to interest in the design and implementation of effective methods to protect confidential information. This article presents a comprehensive analysis of two popular security methods, cryptography and steganography, which outperform other standard and automated security methods.*

Keywords- Data Hiding, Cryptography, Steganography, AES, DES, DCT, DWT.

I. INTRODUCTION

Today, the use of computer networks for seamless data exchange has made tremendous progress. However, such networks are most popular for fast and easy operation for long-distance data exchange, but the security and privacy of long-distance communication remain a privacy issue. With the development of computers day by day network, a number of techniques have evolved to affect the availability, privacy and integrity of critical data, creating a serious problem for security vulnerabilities. On the other hand, many approaches have been proposed using two popular security techniques, cryptography and steganography, to improve the security of secret messages through open communication channels, but these technologies may not be safe for communication. confidential information at a distance, which creates the need for additional security mechanisms to protect confidential information. Cryptography is used to find information under the cover of steganography. This chapter presents the current state-of-the-art analysis of these two security techniques to better clarify the inadequacy of the current and traditional security methods for researchers and motivate the development of new security systems that increase the level. security.

1.1 Cryptography

Cryptography is a widely used technique that encrypts plain text to create encrypted text (cipher). Information that can be read and understood without special intervention is called plain text or plain text. The plain text encryption technique to hide content is called encryption. Encrypting plaintext results in an unreadable hash called ciphertext. Basically, cryptography examines data to ensure confidentiality and/or authenticity, and allows data to be transferred to a secure system in a way that cannot be read by anyone other than a trusted recipient [1, 2]. Cryptography and cryptography are the two main branches of cryptography. Cryptology is about keeping plaintext secrets from an eavesdropper or an enemy, while cryptography overcomes this technique to recover data or make information acceptable as authentic [3]. In general, all cryptographic processes have four main components:

- **Plain text -** Information provided. Plain text documents may contain sensitive information such as credit card numbers, passwords, bank account numbers, or payroll, employee information, or confidential formulas sent between organizations.
- **Ciphertext-** refers to plain text that is obfuscated using a mathematical algorithm. Ciphertext is the encrypted plaintext sent to the recipient.
- A **key** is a mathematical value, formula, or process that determines how a plaintext message is encoded or decrypted. Basically, it's the only way to open compressed data.

- A **cryptographic algorithm** is a mathematical formula used to decrypt the plain text to extract the encrypted text. Changing plaintext to ciphertext using a cryptographic algorithm is called encryption, and changing ciphertext to plaintext using the same cryptographic algorithm is called encryption.

Figure 1 illustrates cryptographic tactics.

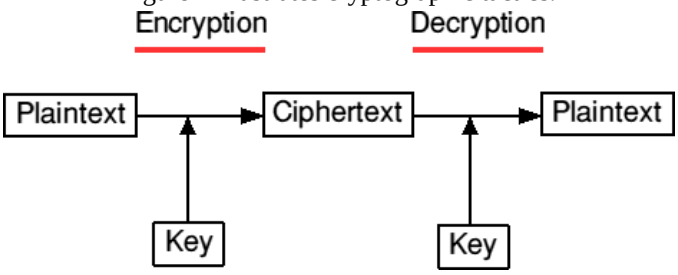

Figure 1 Cryptography

Broadly, cryptographic algorithms can be divided into two categories:

- **Stream Algorithm -** Work on plain text one byte at a time, with one byte of characters, numbers, or special characters. This process is inefficient and slow.
- **Block Algorithm** - Works on plaintext in groups of bytes called blocks (hence block algorithm or block cipher). The default block size for modern algorithms is 64 bytes, which is not large enough to work with, but large enough to prevent code breakers. Unfortunately, with today's microprocessor speeds, changing a 64-byte algorithm using brute force is an easy task.

Three types of cryptographic schemes are used in today's scenario to secure data:

1.1.1 Secret Key Cryptography (SKC)

Symmetric key cryptography schemes also use a single key for the encryption and decryption process. The Data Encryption Standard (DES) is the best example of this cryptosystem widely used by the federal government.

Figure 2 illustrates the steps in the underlying cryptographic encryption to establish secure communication.

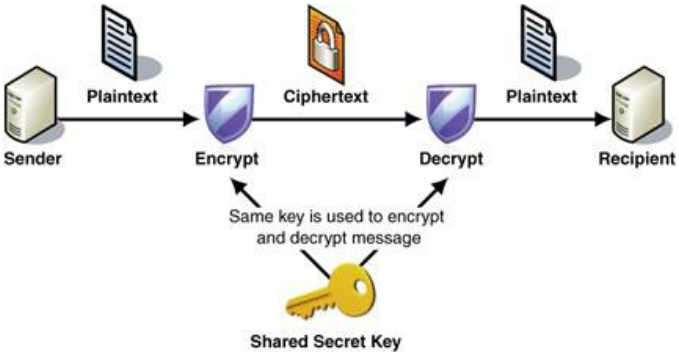

Figure 2 Symmetric / Secrete Key Cryptography

However, this mechanism improves data security, but sharing the key between the sender and receiver is a difficult problem because an unauthorized person can try all the data after receiving the secret key. So basic security for secure communication is a must with this approach.

Advantages of symmetric key cryptography

- Read quickly.
- Verifying the authenticity of the primary buyer.
- Retrieving plaintext requires the same key used when the message was encrypted.
- Weaknesses of symmetric key cryptography
- share the core of the difficult problem. If a person is allowed to ask for the secret key, they can ask for the information without any effort.

1.1.2 Public Key Cryptography (PKC)

Public key cryptography is an asymmetric scheme that uses a pair of keys, a public key for the encryption process and a corresponding private or secret key for the encryption process. Private keys cannot be removed from public disclosure. Anyone with the public key can encrypt, but not decrypt, the data. Only those with the appropriate private key can open the data. RSA, Diffie-Hellman, Digital Signature Algorithm (DSA), Public Cryptographic Standards (PKCS), Key One Exchange Algorithm (KEA) There are several examples of asymmetric key algorithms.

Figure 3 shows the steps in this algorithm.

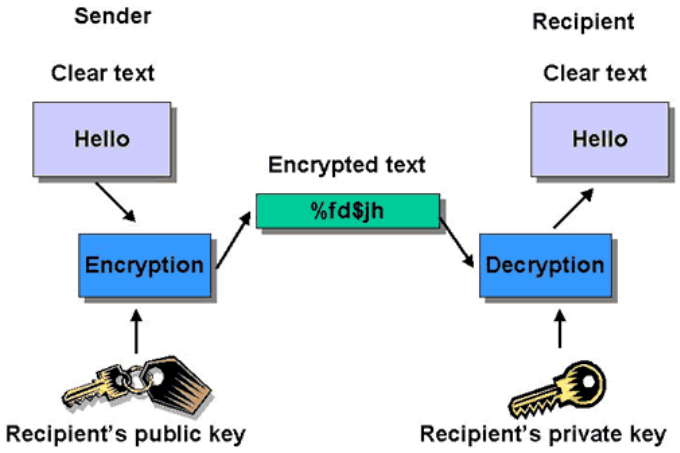

Figure 3 Asymmetric / Public Key Cryptography

Advantages of asymmetric key cryptography

- Addressing the key distribution problem of symmetric key algorithms.
- Public key cryptography is not intended to replace private key cryptography, but to complement and make it more secure.
- Increase the level of security by using a pair of buttons.

Weaknesses of asymmetric key cryptography

- The disadvantage of using public cryptography for encryption is speed: there are popular key encryption methods that are significantly faster than current key encryption methods.
- public cryptography can be impersonation-proof, even if the user does not have a private key.
- Certificate issues, most public key systems use a third party to verify key authenticity.

1.2 Hash function

Hash function uses mathematical transformation to encrypt data irreversibly. Basic program. Hash function message integrity in cryptography. The hash value provides a digital fingerprint of the message content, ensuring that the message has not been altered by intruders, viruses, or other means. Hash algorithms are efficient because the probability that two different plaintext messages will produce the same hash value is very low.

There are several popular hash functions in use today:

- Hashed Message Authentication Code (HMAC): Combines authentication and hashing via a shared secret.
- Message Digest 2 (MD2): Generates a 128-bit hash value of a byte-oriented, self-contained message designed for smart cards.
- MD4: Similar to MD2, specially designed for fast processing in software.
- MD5: Similar to MD4, but slower because more data is manipulated. A potential vulnerability in MD4 was developed after it was reported.
- Secure Hash Algorithm (SHA): Generates a 160-bit Hash value modeled after MD4 and recommended by NIST for the Secure Hash Standard (SHS).

Figure 4 shows the hash function process.

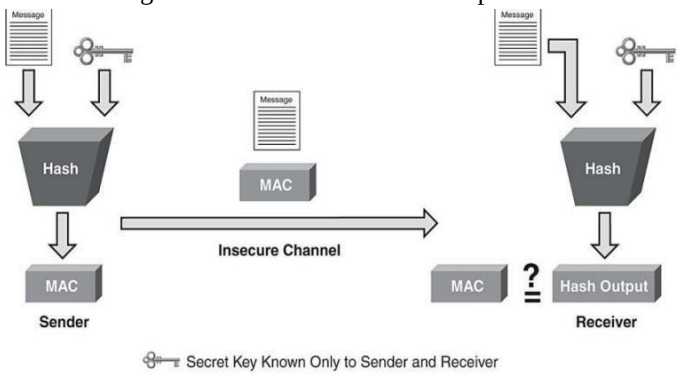

Figure 4 Hash Function

1.3 Steganography

Steganography is different from cryptography. The purpose of cryptography is to secure communication by changing data into a form that cannot be understood by the listener. Steganography techniques, on the other hand, tend to hide the existence of the message, making it difficult for observers to find out where it is message in some cases, sending encrypted data may attract attention, but invisible data may not. Accordingly, cryptography is not the best solution for secure communication; only part of the solution [4]. Steganography comes from the Greek graphy which means "cover" and "write", so Steganography means "secret writing". In steganography, a secret image is embedded in a cover image and data is transmitted in an undetectable manner. Digital images, videos, audio files, and other computer files can be used to host information.

Figure 5 shows an overview of the steganography system.

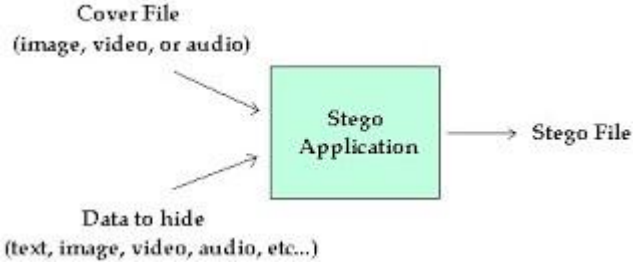

Figure 5 General Steganography Model

An object where secret information is hidden is called a secret object. A stego image is an image obtained by recording a hidden image. Hidden message can be plain text, encrypted text or image etc. it is possible Steganography techniques provide high throughput and obscure internal data.

The three main types of steganography systems are as follows

- **Image Steganography**: - To hide a secret message by converting it into a carrier image.
- **Audio Steganography:** - Secret messages are embedded in unused parts of audio because every file has some unused bits or parts where secret messages can be hidden.
- **Video Steganography:** - This technique divides the video into audio and image frames, where the video is embedded in the audio file.

Steganography techniques widely used today include:

1.3.1 Discrete Cosine Transform (DCT):

In this diagram, the image is converted from the space domain to the frequency domain. A two-dimensional DCT transformation is used. After applying quantization and IDCT to the DC coefficients, the coded latent image is coded. This method uses the JPEG compression algorithm to convert the 8X8 pixel block to 64 DCT to embed the coded secret. Since this method is used in the frequency domain, they do not significantly change the visual appearance of the image. The downside of this system is that it only works with JPEG files. DCT-encoded latent images work together at low and medium frequencies.

1.3.2 Discrete wavelet transform (DWT):

Wavelet transform (WT) transforms spatial domain information into frequency domain information. Wavelet waveforms are used in steganographic modeling because the wavelet transform divides high-frequency and low-frequency information on a pixel-by-pixel basis. Many practical experiments recommend using the wavelet transform domain for steganography due to several advantages. The search conversion application will mainly focus on the robustness and robustness of the data hiding system features.

In wavelet, frequency response and time response data can be implemented due to accurate sampling and subsampling of the image. The advantage of DWT over DCT is, firstly, there is no need to divide the input encoding into 20 blocks, the compression ratio is higher, secondly, it avoids blocking artifacts, and this allows good localization in the time and space-frequency domain. Third, the transformation of the entire image introduces a special magnification. The result is a better determination of which data is relevant for human perception, a higher compression ratio. This method compares the DCT domain with the DWT domain to provide high fidelity and good stego image quality analysis from a high signal-to-noise ratio. The peak signal-to-noise ratio is a measure of the quality of the stego-image by calculating the deviation between the stego-image and the overlay image, PSNR is the security for the higher image.

However, Steganography is closely related to cryptography to protect information from unwanted parties, but technology alone is not perfect and cannot be compromised. Once the existence of secret information is discovered or suspected, the purpose of steganography is partially defeated. The power of steganography can be enhanced by combining it with cryptography. If steganography fails to deliver the message, it is still useless because it is encrypted using cryptographic techniques.

II. CONTRACTION

The author [5] uses an algorithm based on the operation of image pixels and a 128-bit key that changes each set of pixels in a rather intelligent encryption process. The key to be used is generated independently on the sender and receiver side based on the AES key expansion process. Therefore, the entire initial key set is shared without fear. The author provides information about AES. AES provides high encryption quality with minimal memory requirements and computing time.

Cryptography and Steganography provide powerful tools for image security in communications. DES, S-box mapping, etc. There are various methods of cryptography combined with steganography for added security, but they are very complicated and involve a large number of calculations.

[8] conducted a comparative analysis of quality and size between Joint Picture Experts Group (JPEG) stegano images and Audio Video Interleaved (AVI) stegano videos. The author proposes UTF-32 encoding in the replacement algorithm and increases key strength by using stegano lossless method in AVI files. However, the load carrying capacity is low.

[9] An adaptive immutable data hiding technique is proposed for MPEG video encoding. Hidden data can be recovered without needing a goal. This technique only works in the frequency domain. It has the advantages of low complexity and low visual distortion for covert

communication applications. However, it suffers from a low load capacity.

Various technologies used in image steganography are proposed in [10]. This article presents an overview used to hide a secret message or image in the spatial and transformation domain. This paper also proposed techniques for detecting a secret message or image, i.e. steganalysis. Paper on

[11] introduced a method where the secret message is first compressed using a wavelet transform technique and then embedded into the cover image using LSB, where the bits of the secret message are embedded into the image using a random number generator. In [12], the authors give a brief overview of the above techniques used to ensure security. In this paper, it has been demonstrated that these techniques can make data more secure and robust.

In [13], the author addressed three main shorthand challenges, capacitive imperceptibility and security. This is achieved by a hybrid data hiding scheme in the enterprise LSB technique with the key permutation method. The two layers of the security system proposed in [14] by the login procedure, a username and password are required first, and after logging in, the key is used to insert the secret data. This maintains integrity and privacy. In the same way, another author used the idea of dual security in [15], the secret data was first converted into an encrypted form, and then LSB steganography technique was used to embed it in the cover object. In this way, the message is transmitted with maximum security and can be retrieved without data loss.

In [16], the author proposed a technique using LSB steganography and cryptography, where secret information is encrypted using RSA or Diffie Hellman algorithm before embedding into the image using the LSB method. The time complexity increases with the proposed technique, but high security is achieved at this cost. In [17], the authors proposed an optimal steganography based on discrete wavelet transform (DWT). Experiments show that the peak signal to noise ratio (PSNR) generated by the proposed method is better. In the same context, a new image steganography technique proposed in [18] is proposed, which combines integer wavelet transform (IWT) and discrete cosine transform (DCT), which embeds the secret image in the frequency domain of the cover image with high matching quality.

In [19], the authors used a different approach to hide the imagei.e. Corner Hide (HBC) algorithm is used to place the key in the corners of the image. All keys in the corners are encrypted by generating pseudo-random numbers. Then the hidden image is transferred. The receiver should know all the keys that are used in the corners when encrypting the image. Reverse Data Hiding (RDH) is used to get the original image and the original image is created when all the corners are unlocked with the correct secret keys used to hide the image.

In the paper [20], the method proposed by the authors provides information hiding inside the image by replacing the LSB and MSB technique in that the proposed works are as follows first find the key i.e. public key and private key according to the RSA algorithm access and encrypt secret messages this algorithm is the most popular and proven asymmetric key cryptographic algorithm, RSA methodology, and encryption of secret information. The secret information is encrypted, and then the encrypted ASCII value is converted to binary, the information is encrypted, and then the MSB and LSB bits are replaced with information. At the same time, the pixel image is converted into binary form. The image is used as a wrapper for embedding encrypted information. This process is completed by a least significant bit (LSB) encoder, which replaces the least significant bit of the pixel values with encrypted information bits. There was one disadvantage in this, which is certainly the increasing time requirement of the entire process.

In the paper [21], the authors proposed a scheme by including a mixture of cryptography and steganography in the confidentiality of data before secrecy by increasing the level of security. It is used for the secure exchange of private information between administrations. In this, the author suggests two security steps, the first is the encryption process and the second is steganography, which increases the level of security for data hiding. In the first stage, the message is transmitted and is first transformed into an encrypted image using a first encryption process. In a second phase, this ciphertext is to be converted into a transition text using a second encryption process. The intermediary ciphertext or information created the hidden text inside the cover image using steganography to hide the presence of the secret, and this resulting steganographic image is transmitted to the receiver over the network. So in this paper scheme of dual encryption and steganography, it is proposed that the encryption process is fully dependent on the key, the encryption process uses RSA algorithm and the steganography technique is used for image embedding, steganography uses the

III. CONCLUSION

This article presents the state-of-the-art research work on two popular approaches to information security, namely cryptography and steganography. However, both

techniques provide security for classified information. Where cryptography modifies information settings so that only the authorized recipient can obtain a text message, steganography hides the complete information in a cover medium so that no one can easily identify it. any message is hidden in the content presented, but no standalone approach is that good for practice. Therefore, a new advanced technique for data security is needed to ensure greater security of information when communicating over an unsecured channel. Future work can be done in a way to combine the concepts of cryptography and steganography to ensure more security of the secret message.

REFERENCES

[1] Menezes, Alfred, Paul C van Oorschot, Scott A. Vanstone, "Handbook of Applied Cryptography. CRC Press", October 1996, ISBN 0-8493-8523-7.

[2] William Stallings, "Cryptography and Network Security: Principles and Practices", Pearson Education, Third Edition, ISBN 81-7808-902-5.

[3] W. Stallings, Cryptography and Network Security: Principles and Practice. Prentice Hall, 2010, vol. 998.

[4] Nagham Hamid, Abid Yahya, R. Badlishah Ahmad & Usamah M. Al-Qershi "Image Steganography Techniques: An Overview" International Journal of Computer Science and Security (IJCSS), Volume (6):Issue (3): 2012

[5] B. Subramanan "Image encryption based on aes key extension" in IEEE Applied Second International Conference on New Applications of Information Technology, 978-0-7695-4329-1/11, 2011.

[6] Manoj Kumar Ramaiya, Naveen Hemrajani, Anil Kishor Saxena, "Security Improvisation in Image Steganography Using DES", 3rd IEEE Trans. IACC International Conference -2013, Page(s): 1094 – 1099.

[7] Manoj Kumar Ramaiya, Naveen Hemrajani, Anil Kishor Saxena, Monika Sharma "Image Stenography: Self Extraction Mechnanism", UACEE International Journal of Advances in Computer Science and its Applications-IJCSIA Vol -3 Issue -2,ISSN 2250-3765 Pg -145-148, 2013.

[8] R. Kavitha and A. Murugan, "Lossless Steganography on AVI File Using Swapping Algorithm", International Conference on Computational Intelligence and Multimedia Applications, pp. 83-88, Sivakasi-Tamil Nadu, December 2007

[9] Yueyun Shang, "New Invertible Data Hiding in Compressed Videos or Images", Third International Conference on Natural Computing (ICNC 2007), Vol. 4, pp. 576-580, Haikou, August 2007.

[10] S.Ashwin, J.Ramesh, K.Gunavathi, "Novel and Secure Encoding and Hiding Techniques Using Image Steganography: A Survey", IEEE Xplore International Conference on Emerging Trends in Electrical Engineering and Energy Management, December 2012, p. 171-177.

[11] Humanth Kumar, M.Shareef, R.P. Kumar, "Securing Information Using Steganography", IEEE Xplore International Conference on Circuits, Power and Computing Technologies, March 2013, pp. 1197-1200.

[12] Vipula Madhukar Wajgade, Dr. Suresh Kumar, "Stegocrypto – A Review of Steganography Techniques using Cryptography", International Journal of Computer Science & Engineering Technology, ISSN: 2229-3345, Vol. 4, 2013, pp. 423-426.

[13] Marghny Mohamed "Data hiding by LSB substituting using genetically optimal permutation key" in International Arab journal of e-technology, vol.2, no 1,11-17, January 2011.

[14] Rosziati Ibrahim and Teoh Suk Kuan, "A Steganography Algorithm for Hiding a Secret Message Inside an Image," Computer Technology and Application, vol. 2, pp. 102-108, 2011

[15] K. Sakthisudhan, P. Prabhu, "A dual steganographic approach for secure data communication" International Conference on Modeling, Optimization and Computation, Elsevier, Procedia Engineering, vol. 38, pp. 412-417, 2012

[16] Shailender Gupta, Ankur Goyal and Bharat Bhushan, "Information Hiding Using Least Significant Bit Steganography and Cryptography" International Journal Modern Education and Computer Science, vol. 6, pp. 27-34, 2012

[17] T. Narasimmalou, Allen Joseph .R, "Optimized Discrete Wavelet Transform based Steganography", IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT), 2012.

[18] NedaRaftari and Amir MasoudEftekhariMoghadam, "Digital Image Steganography Based on Assignment Algorithm and DCT-IWT Combination", Fourth International Conference on Computational Intelligence, Communication Systems and Networks, 2012.

[19] Hemalatha M., Prasanna A., Dinesh Kumar R., Vinoth kumar D., "Image Steganography using HBC and RDH Technique", International Journal of Computer Applications Technology and Research, Vol.3, 2014, pp. 136- 139.