RES MILITARIS Social Science Journal

ADVANCED IMAGE ENCRYPTION STRATEGIES FOR IOT ENVIRONMENTS

[1]S.S.Rajakumari,[2]A.GuruRaja

[1]Associate Professor ,[2]Assistant Professor

Department Of ECE

St. Johns College of Engineering & Technology, Errakota, Yemmiganur

ABSTRACT

It is crucial to pay attention to the security of information sent via these Internet of Things (IoT) applications due to the fast advancements in the industry and the growing reliance on this technology in residential and financial applications. For critical communications sent via IoT apps, this study suggests a novel encryption mechanism. The suggested approach offers four distinct layers of protection for the secret communication, which is a picture in this instance. By using Conformal Mapping on the hidden picture, we can see the top level. Level 2 involves encoding the first level's output picture using the RSA encryption and decryption technique, and Level 3 involves concealing the message within the cover image using the Less Significant Bit (LSB) method. The last layer of protection is the GZIP compression of the stego image. After the steganography procedure, the image's quality was evaluated using the peak signal-to-noise (PNSR) metric. It seems like the findings are satisfactory and show promise. As a result, this approach is proposed as a means to transmit covert messages via critical IoT applications.

Security for the Internet of Things, RSA Encryption, Image Encryption, LSB Hiding.

I. INTRODUCTION

In recent times, the Internet of Things (IoT) has become a significant subject of debate in research and its practical applications. The Internet of Things (IoT) is a framework in which everyday objects have the capability to detect and interact with other devices over the internet. Currently, there are many factors that provide a favorable atmosphere for the expansion and growth of IoT. These factors include the universal accessibility of broadband internet to all users and its comparatively cheaper connection costs. Furthermore, it is possible to connect several sensors and devices to it (JEMAI, SADEK, SALIM, & TALBI, 2017). The Internet of Things (IoT) encompasses a variety of devices that are interconnected with certain limitations. These devices often work together to achieve certain objectives, and as a result, they may be used in a variety of ways, such as monitoring and gathering data, as well as accessing and processing it. This technology undergoes constant development in several domains, such as smart houses/buildings/cities, environmental and traffic monitoring, and health and patient monitoring (often referred to as mHealth) (Noura et al., 2018) (Kharchenko, Kolisnyk, Piskachova, & Bardis, 2017). The ideas of mobile networks, traditional internet, and sensor networks have seen significant advancements due to the Internet of Things (IoT), since all entities are interconnected via the internet. When ensuring the integrity, confidentiality, and authenticity of data, it is important to also address its security and privacy (JEMAI et al., 2017) (Kuzminykh, I; Carlsson, 2018). The primary challenges encountered while implementing IoT systems are their increased susceptibility to a wide range of passive and active threats compared to older options. Passive attacks severely compromise data confidentiality by intercepting and retrieving the content of sent packets. Active attacks compromise the integrity and validity of data by manipulating packets via insertion, deletion, or modification. Encryption is a

recommended approach for preventing these attacks. (Want and Dustdar, 2015).

II. LITERATURE SURVEY

The emergence of steganography and cryptography was a direct response to the multitude of assaults and risks faced by smart phone technology. Steganographic methods have been used throughout the years to ensure the secure safeguarding of data transmission. The name steganography, as stated by Dengre, Gawande, and Deshmukh (2013), has its origins in ancient Greek. It is derived from the words "Stegano," meaning anything that is concealed or hidden, and "Graphia" or "Graptos," meaning the act of writing or recording something. According to Alotaibi and Elrefaei (2015), in order for steganography to achieve its intended objective, certain approaches must be used. Steganography may use a combination of spread spectrum methods, transform domain techniques, and replacement and insertion techniques. Nevertheless, substitution, injection, and propagation are identified as the most significant approaches in the field of steganography. The replacement process involves replacing discrete segments of the carrier file with the concealed message in order to evade detection by the unauthorized individual. Injection is a method that prevents suspicion when a file is added to the cover media. On the other hand, propagation involves using cover objects but utilizes an invisible data production engine to imitate a file, such as music, sound, or text.

The writers in (Kyei, Panford, Hayfron-acquah, Student, & Lecturers, 2019) use optimal techniques of steganography and cryptography. The Least Significant Bit (LSB) technique is used to insert or embed messages into a cover object. The research utilizes RSA, an asymmetric cryptography technique, for its cryptographic purposes. The integration of both the Least Significant Bit (LSB) insertion method and the RSA technique in their system renders it one of the most exceptional apps for guaranteeing data security and confidentiality on Android smart devices. Steganography is the practice of concealing confidential information inside an item, specifically a picture (M & Hussain, 2014). In picture steganography, the concealment of data is often achieved by manipulating the intensity of pixels. Therefore, it has been observed that photographs are the most prevalent and often used cover items in the field of steganography.

The objective of the authors in (Apau, B., & Twum, 2016) was to maintain consistent file size output after embedding, while significantly lowering the size of the file to be embedded. The first objective is achieved by re-encoding and recreating the original movie using video encoding methods. Afterwards, the Least Significant Bit (LSB) is used to embed the file into a transformed frame. The RSA and Huffman code compression methods are used to achieve a significant payload capacity. The analytical findings suggest that the process of embedding files into cover movies preserves the properties of both the original video and the steganographic video. The compression levels were determined to be higher than typical, namely over 20%.

III. CONFORMAL MAPPING IN IMAGE PROCESSING

Conformal mappings are mathematical functions that maintain the angle and shape of a very small object, but not necessarily its size, as shown by equation 1 (Frederick & Schwartz, 1990).

$$w = f(z) \qquad (1)$$

In more precise terms, a map is said to be conformal (or angle-preserving) at z0 if it maintains both the oriented angles between curves passing through z0 and their orientation or direction. Complex analysis yields a significant family of conformal maps, which may be used as an illustration.

$$f: U \rightarrow C \qquad (2)$$

If U (as defined in equation 2) is an open subset of the complex plane, then the derivative of the function exists and is non-zero at every point in U, except for zero. If f is anti-holomorphic, meaning it represents the conjugate of a holomorphic function, the angles are retained but their orientation is inverted. The Riemann mapping theorem states that every non-empty, open, and simply connected subset of the complex plane C may be bijectively mapped to the open unit disk centered at P using a conformal map. The symbol "P" denotes a specific point located on the plane. The open unit disk is defined as the set of locations whose distance from P is less than 1. If U is an open subset with a simple connectivity in the complex plane C (excluding the whole C), it implies the existence of a bijective or one-to-one mapping (f) from U to the open unit disk D. (Sharon and Mumford, 2006).

$$f: U \rightarrow D \qquad (3)$$

where

$$D = \{z \in C : |z| < 1\}$$

Since f is a bijective map in equation 3, it is conformal.

A conformal map of an extended complex plane, which is equivalent to a sphere, is defined as a Mobius transformation. In other words, it is a transformation that results in a rational function of the form (Ganguli, 2004).

$$f(z) = \frac{az+b}{cz+d} \qquad (4)$$

With respect to the conjugate, it maintains the angles but inverts their orientations. Figure 1 depicts the graph of the conformal mapping.

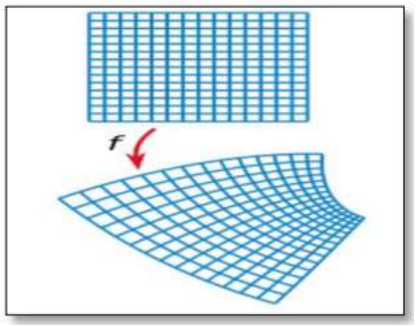

Figure 1 Conformal mapping graph

The intricacy of the changes used to establish relationships between various fish species may vary. Figure (2) displays instances of transformations that depict the various forms of fish.

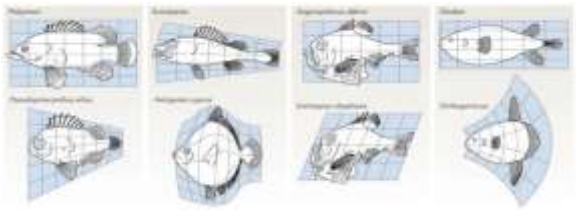

Figure 2. Transformation examples, These images are taken from (Arthur, 2006)

RSA Cryptosystem

In 1978, R. Rivest, A. Shamir, and L. Adleman published an academic essay introducing a public-key cryptographic system that encompasses key generation and public-key ciphers. Their security relies on the assumed intricacy of factoring numbers into their prime components. The RSA cryptographic scheme, derived from the initials of the founders' last names, has shown its effectiveness to date. The cryptographic uses of this technology include banking, e-mail security, and online e-commerce. In addition to its practical uses, it is mostly used for encrypting short data fragments, namely for key transmission, as well as for digital signatures and certifications over the internet (Deen, El-Badawy, & Gobran, 2014). The RSA algorithm is a kind of asymmetric cryptography that involves the use of two sets of keys for encrypting and decrypting communications. This is essential to guarantee the integrity and protection of accurate

information. The generation of such keys involves intricate mathematical calculations, which yield the public and private keys. The sender is provided with the first key to encrypt the communications, while the recipient is given the private key to decode the encrypted messages covertly (Apau & Adomako, 2017). The RSA method is based on performing exponentiation over integers modulo a prime in a finite (Galois) field. It utilizes integers that are composed of 1024 bits. Oleiwi, Alawsi, Alisawi, Alfoudi, and Alfarhani (2020).

Steganography

Steganography is the practice of concealing data inside seemingly harmless carriers in order to hide the existence of the data. Steganography, an ancient art, has had a resurgence due to the advent of computer technology (Kamble, Engineering, Gaikwad, & Engineering, 2013). Computer-based steganographic approaches include hiding digital information inside other data in a manner that is undetectable to the original data (Khalid Obayes, 2013). This kind of information may be sent by textual communication or as a binary file. Additionally, other details about the cover or the owner can be included, such as digital watermarks or fingerprints. Steganography is founded on the idea that artifacts such as bitmaps and audio files might hold excessive and unnecessary information. Steganography significantly decreases the likelihood of detecting secret communications. The encryption of the communications provides an additional level of security, since the message must be deciphered if it is found. Steganography may be seen as similar to cryptography, since both are used to introduce aspects of secrecy into communication (Kamble et al., 2013). Cryptography approaches aim to obfuscate communications in such a way that only those with proper authorization can comprehend them if intercepted (Amin, Salleh, Ibrahim, Katmin, & Shamsuddin, 2003). In recent years, several steganography approaches have been suggested for concealing secret messages inside multimedia artifacts, such as photographs. Regarding the latter, there are several methods by which covert messages or information are concealed in a manner that prevents any modifications to the original photos from being detected. Several widely used strategies comprise:

- Least Significant Bit insertion (LSB).
- Masking and filtering.
- Transform techniques.

LSB insertion is a straightforward method of embedding information in picture files. It involves simply embedding the message bits into the least significant bit plane of the cover image, following a predictable pattern. The modulation of the least significant bits does not produce any noticeable variations to the human eye, since the change in amplitude is quite little. LSB offers numerous advantages, such as its ability to easily embed message bits in the least significant bit planes of a cover-image. Additionally, the resulting stego-image appears identical to the cover-image due to the minimal change in bit amplitude, resulting in a higher level of perceptual transparency. Khalid Obayes, in the year 2013.

Compression

Data compression may be classified into two categories: lossy compression and lossless compression. The loss of information is often unacceptable owing to the valuable nature of data (Nitu, Kumar, & Rishi, 2019). Illustrative instances include the realm of medical imaging, fingerprint data, and computer programming. Furthermore, lossless data compression is particularly advantageous when it comes to text. Hence, it is essential to compress the data in a manner that ensures the complete retrieval of all the data upon decoding the compressed data. Therefore, lossless data compression is often favored over lossy compression. Reversible compression, often known as lossless compression, ensures that the decoded data is an

exact replica of the original data (Shah & Sethi, 2019). The suggested approach used GZIP to compress the cover picture as the last stage, after the hiding of the secret image inside it (the stego image).

There are two distinct variations of GZIP. GZIP utilizes a hybrid LZ77 and static Huffman encoder to compress real-time data. Meanwhile, GZIP utilizes a mix of the LZ77 and dynamic Huffman algorithms to compress non real-time data. The Static Huffman algorithm encodes the data by giving a fixed-length code to each symbol in a single operation. The static Huffman encoder does not analyze the frequency distribution of the data. Therefore, the data is encoded in an efficient manner, however there is a trade-off in terms of compression ratio (Oswal, Singh, & Kumari, 2016). The dynamic Huffman encoder performs a somewhat challenging job of encoding symbols (Patel, Katiyar, & Arora, 2016). The encoding process assigns varying length codes to symbols based on their frequency, with more frequent symbols receiving shorter codes and less frequent symbols receiving longer codes. Consequently, the desired compression ratio is attained (Shah & Sethi, 2019) The reference comes from a study conducted by Balakrishnan and Sahoo in 2006.

Peak Signal to Noise Ratio (PNSR)

PSNR is a commonly used statistic in steganography to assess the quality of stego pictures. A stego picture will have improved quality as the value of PSNR increases. The cover picture, denoted as C, has a size of M × M, while the stego image, denoted as S, has a size of N × N. The pixel values of C range from (0, 0) to (M-1, M-1), while the pixel values of S range from (0, 0) to (N-1, N-1). The Peak Signal-to-Noise Ratio (PSNR) is computed using the method described by Khalid Obayes in 2013:

$$PNSR = 10log_{10}\left[\frac{MAX^2}{MSE}\right] \quad (5)$$

Where

$$MSE = \frac{1}{NM}\sum_{x=1}^{N-1}\sum_{y=1}^{M-1}(c(x,y)-s(x,y))^2 \quad (6)$$

IV. PROPOSED METHODOLOGY

This study presents a suggested technique for transferring an encrypted picture with the aim of achieving a high level of security throughout the transmission process. Figure (3) depicts the general overview of the picture transmission and reception process, which has two steps: transmitting and receiving. The processing occurs in these two stages, as shown below.

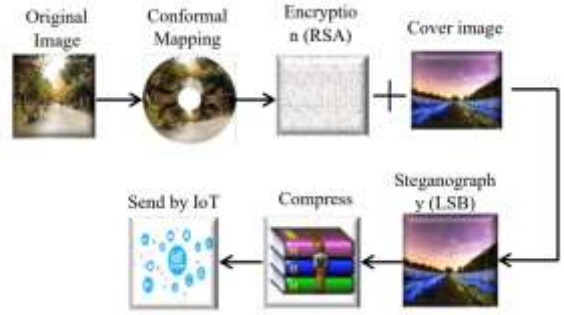

Figure 3 Sending phase in IoT

Sending phase

The transmission procedure involves many sequential processes, namely: conformal mapping, encryption, steganography, and picture compression.

1. Conformal Mapping

During this stage, the initial picture underwent processing to generate a new image that had the same properties as the original image, but had a distinct visual look. Figure (4) illustrates the sequential process of transforming the original picture into a processed image via the use of the conformal mapping technique.

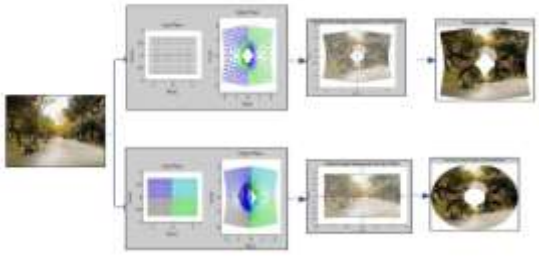

Figure 4 Converting the original image according to geometric models

2. Image Encryption

The picture was encrypted using the RSA technique. The process relies on the use of two keys represented by prime integers (p, q) and the mathematical computation of values for each component (E, N, M). Figure (5) displays the values of p = 11, q = 13, and E = 7. Additionally, we provide the picture to be encrypted and the location where the new image will be saved after the encoding process. The input is a jpg picture with a resolution of 512 pixels in width and 502 pixels in height. The execution time was just 12 seconds, and the result of the encryption process is a text file, which facilitates both concealment and transmission of the picture inside the IoT ecosystem.

Figure 5 Image encryption by (RSA)

3. Steganography

The Least Significant Bit (LSB) technique is used to conceal the text file that was produced in the preceding stage. The picture format (bmp) is used as the cover for the text file. Figure 6 displays the characteristics of the cover picture. In this phase, the problem of the size of the encrypted picture is resolved by ensuring that the text occupies a lesser space compared to the cover image. This, in turn, simplifies the process of concealing the text inside the image. The dimensions of the generated pictures are also maintained and sent to the compression algorithm.

Figure 6 Steganography step

4. Compress Image

The GZIP method is a significant compression technology used for compressing data on websites. This method is used for processing the picture that is produced during the concealment phase.

Received Phase

The compressed picture is sent over the Internet as the first stage in the reception process. Their order is shown in Figure (7). This text provides a detailed description of the process of receiving:

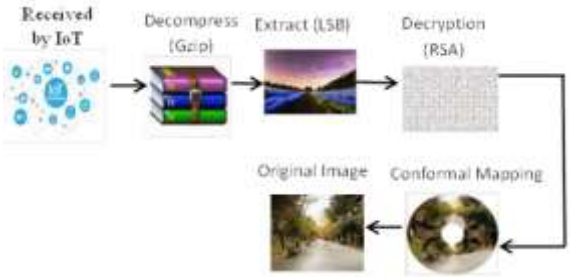

Figure 7 Receiving phase

1. Decompress

The GZIP function was used to decompress the received image. This process produces the cover image. T is considered to be important as it may fool the intruder by not being able to identify the hidden file inside the cover image.

2. Extraction

In the Steganography step, the LSB algorithm was used to hide the original image in the cover image. In the process of extracting the original image from the cover image, we also used the same algorithm, the input for this step is a BMP image and the output is a text file of type (txt).

3. Decryption (RSA)

In this step, the TXT text file is received and decrypted by the RSA algorithm. First, the values of D, N are entered, which are calculated based on the values of P, Q as inserted during the transmission process (encryption step). The decoding process results in a jpg type image. This step is the basic step in accessing the image to be secured. Figure (8) shows the decrypting execution step.

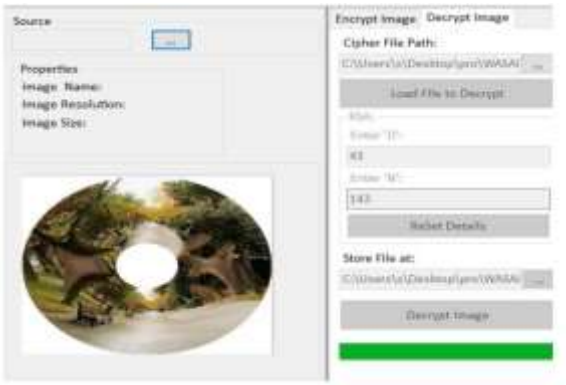

Figure 8 Decoding the text file to obtain the encrypted image type jpg

V. EXPERIMENTAL RESULT

To test the proposed method, four images of different sizes were used, three of which are jpg type and one is bmp type. Table (1) shows the basic characteristics of these images, such as their dimensions, type, and size. Picture 4 differs as the initial processing was not performed on it (conformal mapping). The rest of the images underwent the initial processing of conformal mapping, which in turn changed the appearance of the image (white spaces are added). These changes are not exploited in the encryption process, as this effect is clearly observed at the time of implementation. The encoding of the images is the least possible in the fourth image (4s).

As for the size of the image resulting from combining the encrypted image with the cover image in the process of concealment, it was the least for image 4, which is 136 KB. In the process of compression, image 3 presented the best performance despite the convergence of the results. It is worth noting that the parameter values of (PSNR and MSE) were represented by 8-bit pixels for each sample. The results execution appears to be perfect, as shown in Table (1).

Table 1 The table shows the main characteristics of the images with the implementation results of the proposed method

	Image Characteristics			Result execute				
	Dimension	Image Type	Size	Encryption time	Steganography	Size after compression	MSE	PSNR
Image1	502×512	BMP	3.12 MB	12s	Type: .txt Size: 436 KB	2.73 MB	9.6	38.59
Image2	612×516	PNG	208 MB	6s	Type: .txt Size: 219 KB	2.76 MB	3.29	42.99
Image3	616×512	JPG	40.3 MB	14s	Type: .txt Size: 494 KB	2.68 MB	11.32	37.62
Image4	225×225	JPG	12.3 KB	4s	Type: .txt Size: 137 KB	2.75 MB	2.75	43.77
Cover Image	1280×853	BMP	3.32 MB	-	-	-	-	-

VI. CONCLUSION

Upon acquiring the data and evaluating the level of distortion in the stego picture using the PNSR measure, the findings seem to be quite encouraging. Several conclusions may be inferred. The implementation of four tiers of protection resulted in a very secure and trustworthy means of communication. Conformal Mapping used in the first stage introduced distortion to the covert picture, resulting in a somewhat unclear appearance while maintaining the original characteristics of the image. However, this technique requires more processing time. The security of RSA is further enhanced by including a second degree of protection dependent on the number of prime factors. Furthermore, the decoded photos do not include any missing data, in addition to the consideration of security. Additionally, the process of converting an image to a text file and then compressing it using GZIP is a very efficient method for enhancing the speed of downloading and receiving images on web sites.

REFERENCES

1. Alotaibi, R. A., & Elrefaei, L. A. (2015). Steganography in Arabic Text Using Zero width and Kashidha Letters. International Journal of Computer Science & Information Technology (IJCSIT), 6(4), 1–11.

2. Amin, M.M., Salleh, M., Ibrahim, S., Katmin, M.R., & Shamsuddin, M.Z.I. (2003). Information hiding using steganography. 4th National Conference on Telecommunication Technology, NCTT 2003 - Proceedings, (June 2015), 21–25. https://doi.org/10.1109/NCTT.2003.1188294
3. Apau, R., & Adomako, C. (2017). Design of Image Steganography based on RSA Algorithm and LSB Insertion for Android Smartphones. International Journal of Computer Applications, 164(1), 13–22. https://doi.org/10.5120/ijca2017913557
4. Apau, R., Hayfron-Acquah, J.B., & Twum, F. A Modified High Capacity Video Steganography Technique Based On Spatial Domain Method, Asymmetric Cryptography and Huffman Code Algorithms. Communications, 5(10), 53-60. https://doi.org/10.5120/cae2016652390
5. Arthur, W. (2006). Series on Historical Profiles — TIME LINED ' Arcy Thompson and the theory of transformations. Genetics, 7(1958), 7–12.
6. Balakrishnan, R., & Sahoo, R. K. (2006). Lossless compression for large scale cluster logs. 20th International Parallel and Distributed Processing Symposium, IPDPS.
7. Balakrishnan, R., & Sahoo, R.K. (2006). Lossless compression for large scale cluster logs. In Proceedings 20th IEEE International Parallel & Distributed Processing Symposium. https://doi.org/10.1109/IPDPS.2006.1639692
8. Deen, A.E.T. El, El-Badawy, E.S.A., & Gobran, S.N. (2014). Digital Image Encryption Based on RSA Algorithm. IOSR Journal of Electronics and Communication Engineering, 9(1), 69–73. https://doi.org/10.9790/2834-09146973
9. Dengre, A.R., Gawande, A.D., & Deshmukh, P.A.B. (2013). Effect of Audio Steganography based on LSB insertion with Image Watermarking using AVI video Cryptography : International Journal of Application or Innovation in Engineering & Management (IJAIEM), 2(6), 363–370.
10. Frederick, C., & Schwartz, E.L. (1990). Conformal Image Warping. IEEE Computer Graphics and Applications, 10(2), 54–61. https://doi.org/10.1109/38.50673
11. Ganguli, S. (2004). Conformal Mapping and its Applications. IEEE Transaction on Medical Imaging, 23(8), 1–4. https://pdfs.semanticscholar.org/1bed/474a4649f8344f1c56ee0972593e816ca01b.pdf
12. Jemai, A., Sadek, F., Salim, M., & Talbi, M. (2017). A lightweight Encryption Algorithm applied to a quantized speech image for Secure IoT. Proc. of the Sixth International Conference on Advances in Computing, Electronics and Communication - ACEC 2017, (February), 1–6. https://doi.org/10.15224/978-1-63248-138-2-01
13. Kamble, P., Engineering, S., Gaikwad, V.S., & Engineering, S. (2013). Steganography Techniques: A Review. International Journal of Engineering Research & Technology (IJERT), 2(October).
14. Khalid Obayes, H. (2013). Suggested Approach to Embedded Playfair Cipher Message in Digital Image. 3(5), 710–714.

15. Kharchenko, V., Kolisnyk, M., Piskachova, I., & Bardis, N. (2017). Reliability and Security Issues for IoT-based Smart Business Center: Architecture and Markov Model. 2016 Third International Conference on Mathematics and Computers in Sciences and in Industry (MCSI), (June 2020), 313–318. https://doi.org/10.1109/mcsi.2016.064