WJARR

World Journal of Advanced Research and Reviews

eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(Research Article)

Check for updates

Enhancement of L. Voleti LSB technique applied to Image Steganography

Raphael George A. Mendoza *, Maurice Rubien C. Antonio, Raymund M. Dioses, Jonathan C. Morano and Mark Christopher R. Blanco

Department of College of Information Systems and Technology Management Information Technology, Pamantasan Ng Lungsod Ng Maynila, Manila, Philippines.

World Journal of Advanced Research and Reviews, 2024, 22(02), 1101–1106

Publication history: Received on 08 April 2024; revised on 15 May 2024; accepted on 17 May 2024

Article DOI: https://doi.org/10.30574/wjarr.2024.22.2.1437

Abstract

In today's world, the progress of communication technology plays a role in our everyday lives. The internet and the conversion of data into forms have significantly expanded the sharing of information leading to fast-paced growth. Despite having secure methods available, safeguarding data remains a top priority. This study aims to improve the security and durability of data transmission by combining steganography and cryptography techniques. Steganography, which involves hiding messages within another medium, and cryptography which entails encrypting messages using keys are both effective ways to ensure data security. The research delves into combinations of algorithms that integrate steganography and cryptography examining their impact on enhancing security. It categorizes methods based on technical and non-technical aspects as well as their domains. Moreover, it underscores the importance of data security in media formats such as images, videos, and audio. In analyzing message lengths noticeable character patterns were observed in both Vigenère Cipher and Elliptic Curve Cryptography. In short messages "s" was prominent in the Vigenère Cipher accounting for 26.3% of occurrences while Elliptic Curve Cryptography showed a prevalence of "t" at 3.9%. Medium-length messages continued to show the dominance of "s" in the Vigenère Cipher at 22.5% while Elliptic Curve Cryptography highlighted "p" as a character at 4.3%. Lastly, longer messages maintained the prevalence of "s" in the Vigenère Cipher at 24.3% with "v" emerging as dominant in Elliptic Curve Cryptography at 3.9%. These findings show that combining steganography and cryptography methods can greatly enhance the protection of multimedia data.

Keywords: Steganography; Cryptography; Vigenère Cipher; Elliptic Curve Cryptography

1. Introduction

In today's age the advancement of communication technology plays a role in our daily lives. The internet and the transformation of data into formats have greatly expanded the exchange of information which is growing at a rate. Despite the availability of highly secure methods, protecting data remains a top priority. Continuous efforts are being made to enhance the performance metrics and strengthen the security and resilience of these techniques. In the field of information security there are typically two categories that systems fall into: cryptography and information hiding [1,2,3]. Encryption methods are widely used to enhance the security of multimedia data. These techniques are essential in protecting forms of digital content, including images, videos, audio files and more. By deploying these methods, we create a defense against unauthorized access effectively safeguarding sensitive multimedia assets from potential threats and keeping them hidden from prying eyes [4].

Steganography is an art that cleverly hides a message within different types of digital content like images, audio, videos and more. This covert technique ensures that the message stays hidden from observers and cannot be detected within the carrier medium. On the hand cryptography acts as a strong protector of data security. It works by converting text into unreadable cipher text making it impossible for regular users to understand. This encryption process uses algorithms and mathematical operations to keep data safe, from unauthorized access or comprehension [5]. When it

* Corresponding author: Raphael George A. Mendoza

comes to Image Steganography there are algorithms available such as Least Significant Bit (LSB), Pixel Value Differencing (PVD), and Discrete Cosine Transform (DCT), these algorithms play a role in this field. The Least Significant Bit Replacement method is a used and straight-forward technique in the field of steganography, it is commonly employed to discreetly embed messages within chosen cover mediums [6].

Even though LSB gained its popularity it is susceptible to an array of vulnerabilities, particularly frequency analysis and steganalysis, which undermine its capability to guarantee the security of the concealed message [7]. Certainly, there are factors that affect LSB process. These factors include the amount of data that needs to be hidden the need, for data integrity when the "host" signal is distorted through compression and the level of protection required against interception, tampering or unauthorized deletion. As a result, both the size of the message and the encryption method used play crucial roles in ensuring the security of the message [8].

The introduction should be typed in Cambria with font size 10. Author can select Normal style setting from Styles of this template. The simplest way is to replace (copy-paste) the content with your own material. In this section highlight the importance of topic, making general statements about the topic and presenting an overview on current research on the subject. Your introduction should clearly identify the subject area of interest.

1.1. Related Works

For a time, people considered the Vigenère cipher highly secure and believed it to be unbreakable which is why it gained the nickname "le chiffre indéchiffrable " meaning "the unbreakable cipher" in French. While it wasn't truly impervious to decryption it served as an encryption method, for printing purposes until Friedrich Kasiski successfully cracked it in 1863 [9]. The Vigenère cipher is a method of substituting letters in a way that involves using alphabets for different parts of the message. It uses a matrix of 26 by 26 shifts, to the Caesar cipher. This technique is based on principles derived from Caesar ciphers. With a wider range of shifts from 0 to 25 [9]. It was named after Blaise de Vigenère, who lived during the century in France under Henry IIIs rule. The Vigenère cipher remained unbreakable until 1917 [10]. To encrypt with Vigenère each letter in the plaintext is shifted according to its index and the corresponding letter, in the password using the Vigenère square or tableau [9]. In a study conducted by [11] titled "Improving Security in Image Steganography with LSB Technique and Vigenère Cipher Algorithm " researchers explored the use of the Vigenère Cipher for encrypting messages. The Vigenère Cipher involves selecting column names from a square to encrypt the message. To begin encrypting with this cipher you choose a keyword or key phrase that is repeated to match the length of the message being encrypted. This repetition is called the keystream. For each letter in the message, you take the corresponding letter from the keyword and place it on top of the Vigenère square that corresponds to that particular letter. For example, if your keyword is 'battista' and your message is 'an example' you would have two consecutive 'b' letters from the keyword for those two letters in your message. The program efficiently combines an image file with a stego-image to hide information within it. Users can input a key along with their message, select an image file to upload and encode their message by clicking on that same image. This process generates a key and transforms the original message into ciphertext. As a result, you get a message as output while visually representing it as an encoded image with hidden text, in encrypted form (Voleti, 2021). In a study conducted by [12] and colleagues in 2013 they presented an approach titled "Improving LSB Image Steganography with Knight Tour Algorithm, Vigenère Encryption and LZW Compression." The researchers introduced a way of protecting confidential data by first encrypting it using the Vigenère encryption method ensuring that the hidden message remains secure. The results of their study demonstrate that the proposed method does not only address security and payload capacity concerns associated with basic LSB techniques but also improves the visual quality of stego images. In the study made by [13] entitled "An Efficient Least Significant Bit Image Steganography with Secret Writing and Compression Techniques" the researchers used the Vigenère cipher to encrypt and decrypt confidential files. The resulting encrypted text is then compressed using the Huffman coding algorithm. To evaluate their method the researchers tested it on three image carriers, each containing hidden messages of sizes 16kB, 32kB and 48kB. The empirical findings clearly demonstrate that the proposed technique is significantly more efficient than traditional LSB image steganography in terms of imperceptibility. This is evidenced by metrics such as Peak Signal to Noise Ratio (PSNR) Structural Similarity Index (SSIM) stego-image file size and Mean Square Error (MSE). The approach ensures data security through multiple layers of protection including encryption, compression and file embedding processes. Simulation results consistently show that the proposed method generates stego-images, with PSNR and SSIM values while maintaining lower MSE rates and file sizes compared to standalone traditional LSB steganography methods. In all test scenarios the superiority of the proposed method becomes evident through these metrics utilized in this investigation.

1.2. Vulnerability of Vigenère Cipher Algorithm

Vigenère Cipher Algorithm follows this to encode a secret message securely within an image, the algorithm starts with the secret message and a key. If the key is shorter than the secret message, duplicate it to match the length of the message. Encrypt the secret message using this key. Next, choose specific pixels from the cover image where you want to embed data. Replace the least significant bits (LSBs) of these pixels with the LSBs of the binary format of the encrypted message. Repeat this process until the entire message is encoded into the image. The outcome is a stego-image, a modified version of the original cover image that seamlessly conceals the encrypted message within its pixels. To retrieve the message an inverse LSB operation is carried out which relocates and extracts the significant bits. The outcome of this operation reveals the Secret Message. The Vigenère cipher's vulnerability lies in its short, repeated key, forming predictable patterns in ciphertexts. This key looping weakness, exploited by methods like Kasiski's, undermines the algorithm's security.

2. Proposed Method

Elliptic curves established over fields create a foundational group structure crucial for cryptographic systems. This framework comprises points on the elliptic curve, including a unique point known as the "point at infinity " symbolized as O.

An elliptic curve is a type of curve defined by an equation y^2= x^3+ax+b, with constants a and b and variables x and y. These curves have interesting mathematical properties making them well suited for use in cryptography.

A key operation in elliptic curve cryptography involves scalar point multiplication, where a point P on the curve is iteratively added to itself k times minus one to yield another point Q, known as k.P. Conversely deriving k from the given points P and Q (k.P) is known as the Elliptic Curve Discrete Logarithm Problem (ECDLP). Currently there is no algorithm of sub exponential complexity capable of solving ECDLP within a carefully selected elliptic curve group efficiently. This property positions Elliptic Curve Cryptography as an area within public key cryptography offering security comparable to traditional DLP based systems while necessitating smaller key sizes and memory requirements, like 160 bits instead of 1024 bits.

Elliptic curve cryptography is used to replace Vigenère’s index of coincidence for security. The Elliptic Curve Cryptography opens a file dialog prompting the user to select an image file, sets the initial directory to the current working directory, and specifies accepted file types (PNG, JPG, TXT). The text input by the user verifies if the passphrase is blank and then generates a key with SHA 256 encryption. The content is transformed into Base64. Secured using the ECC method.

3. Results and Discussion

The Vigenère Cipher and Elliptic Curve Cryptography (ECC) present ways of securing information through encryption, each having their strengths and weaknesses. The Vigenère Cipher, a method of encryption uses a technique that involves alphabets, for encoding. However, because it relies on keys and patterns it becomes susceptible to known text attacks and frequency analysis. Barter’s [14] observation in 2016 shows a randomness ratio of 0.042 indicating its vulnerability to cryptographic scrutiny and making it less secure for safeguarding confidential data.

On the hand ECC functions based on asymmetric encryption principles by utilizing the properties of elliptic curves within finite fields. Unlike encryption methods ECC requires two keys: a key for encoding and a private key for decoding. Shevchuks [15] research in 2020 emphasizes ECCs ability to withstand threats despite using shorter key lengths due to the complex nature of elliptic curve mathematics. Moreover, ECC ciphertexts are deliberately crafted to avoid detection patterns enhancing their security against breaches.

From a security standpoint ECC surpasses the Vigenère Cipher with its use of asymmetric encryption techniques and exploitation of curve intricacies. Its immunity against analysis and pattern recognition makes it well suited for protecting data in digital communications.

Furthermore, the unique characteristics of ECC enable a method for exchanging keys solving a challenge present in symmetric encryption methods such as the Vigenère Cipher. Through ECC individuals can send messages securely without needing to exchange keys reducing the chances of interception or unauthorized decoding.

It's important to highlight that implementing ECC involves considering management and computational resources. Even though ECC provides security its effectiveness and speed can differ based on how it’s implemented and the capabilities of the hardware.

To sum up, while both the Vigenère Cipher and ECC are used for encryption purposes ECC stands out as the option, for cryptographic uses. Its unique asymmetric structure, along with the mathematics of curves offers strong defense against security risks making it a crucial tool for safeguarding sensitive information in digital communication networks.

3.1. Frequency Analysis

Table 1 Top 5 Character Frequency of Encrypted Short Message

Algorithm	Character	Frequency (%)
Vigenère Cipher	s	99 (26.3%)
	p	48 (12.7%)
	d	48 (12.7%)
	a	47 (12.5%)
	o	46 (12.2%)
Elliptic Curve Cryptography	t	36 (3.9%)
	d	35 (3.8%)
	i	34 (3.7%)
	k	33 (3.6%)
	a	33 (3.6%)

In frequency analysis for short messages, the Vigenère Cipher prominently featured the letter "s" at 26.3%, followed by "p," "d," "a," and "o" with percentages ranging from 12.2% to 12.7%. Conversely, within Elliptic Curve Cryptography, the prevalent character was "t" at 3.9%, followed by "d," "i," "k," and "a" with frequencies between 3.6% and 3.8%.

Table 2 Top 5 Character Frequency of Encrypted Medium Message

Algorithm	Character	Frequency (%)
Vigenère Cipher	s	215 (22.5%)
	o	124 (13%)
	a	121 (12.7%)
	p	119 (12.5%)
	d	119 (12.5%)
Elliptic Curve Cryptography	p	89 (4.3%)
	v	79 (3.8%)
	x	78 (3.8%)
	n	77 (3.7%)
	j	75 (3.6%)

For medium messages, the Vigenère Cipher showcased "s" as the most frequent letter at 22.5%, followed by "o," "a," "p," and "d" with percentages from 12.5% to 13%. In contrast, Elliptic Curve Cryptography exhibited "p" as the common character at 4.3%, followed by "v," "x," "n," and "j" with frequencies ranging from 3.6% to 3.8%.

Table 3 Top 5 Character Frequency of Encrypted Long Message

Algorithm	Character	Frequency (%)
Vigenère Cipher	s	839 (24.3%)
	a	429 (12.4%)
	o	429 (12.4%)
	d	425 (12.3%)
	p	416 (12.1%)
Elliptic Curve Cryptography	v	243 (3.9%)
	h	202 (3.2%)
	n	201 (3.2%)
	e	199 (3.2%)
	p	197 (3.2%)

In long messages, the Vigenère Cipher maintained "s" as the most frequent letter at 24.3%, followed by "a," "o," "d," and "p" with percentages between 12.1% and 12.4%. Conversely, Elliptic Curve Cryptography featured "v" as the prevalent character at 3.9%, followed by "h," "n," "e," and "p," each approximately at 3.2%.

4. Conclusion

The proposed method emphasizes the effectiveness of Elliptic Curve Cryptography (ECC) compared to Vigenère Cipher when encrypting messages within the Least Significant Bit (LSB) domain. Vigenère Cipher despite being an encryption technique has weaknesses such as vulnerability to frequency analysis and known plaintext attacks. Moreover, its non-randomness ratio of around 0.042 highlights its limitations. Conversely Elliptic Curve Cryptography provides an asymmetric encryption method. By utilizing the properties of elliptic curves in finite fields ECC ensures secure communication channels even with shorter key lengths. Its ability to resist cryptographic threats is enhanced by its design to produce ciphertexts without recognizable patterns due to its mathematical structure. Hence when it comes to encrypting messages based on LSB encoding ECC stands out as the option due to its advanced security features and ability to withstand common cryptographic vulnerabilities compared to Vigenère Cipher.

Future Works

Future researchers could explore the advantages of combining Elliptic Curve Cryptography with encryption methods like RSA or AES to strengthen security measures. By harnessing the capabilities of multiple encryption techniques, it may be feasible to bolster protection against cryptographic threats even further. Also, evaluate how well the suggested methods withstand cryptographic attacks and steganalysis techniques. By testing the methods against cutting edge attacks. Researchers can confirm their efficiency and pinpoint any weaknesses that require attention.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Ahmed, D E M., & Khalifa, O O. (2014). Robust and Secure Image Steganography Based on Elliptic Curve Cryptography. https://doi.org/10.1109/iccce.2014.88

[2] Alyousuf, F Q A., & Din, R. (2020). Review on secured data capabilities of cryptography, steganography, and watermarking domain. Institute of Advanced Engineering and Science (IAES), 17(2), 1053-1053. https://doi.org/10.11591/ijeecs.v17.i2.pp1053-1058

[3] Mandal, P C., Mukherjee, I., Paul, G., & Chatterji, B N. (2022). Digital image steganography: A literature survey. Elsevier BV, 609, 1451-1488. https://doi.org/10.1016/j.ins.2022.07.120

[4] Kaur, S., Singh, S J., Kaur, M., & Lee, H. (2022). A Systematic Review of Computational Image Steganography Approaches. Springer Science+Business Media, 29(7), 4775-4797. https://doi.org/10.1007/s11831-022-09749-0

[5] Sethi, P., & Kapoor, V. (2016). A Proposed Novel Architecture for Information Hiding in Image Steganography by Using Genetic Algorithm and Cryptography. Elsevier BV. https://doi.org/10.1016/j.procs.2016.05.127

[6] Jayapandiyan, J R., Kavitha, C., & Sakthivel, K. (2020). Enhanced Least Significant Bit Replacement Algorithm in Spatial Domain of Steganography Using Character Sequence Optimization. Institute of Electrical and Electronics Engineers, 8, 136537-136545. https://doi.org/10.1109/access.2020.3009234

[7] Al-Afandy, K A., Faragallah, O S., Elmhalawy, A., El-Rabaie, E M., & El-Banby, G M. (2016). High security data hiding using image cropping and LSB least significant bit steganography. https://doi.org/10.1109/cist.2016.7805079

[8] Elharrouss, O., Almaadeed, N., & Al-Maadeed, S. (2020). An image steganography approach based on k-least significant bits (k-LSB). https://doi.org/10.1109/iciot48696.2020.9089566

[9] Aliyu, A M., & Olaniyan, A. (2016). Vigenere Cipher: Trends, Review and Possible Modifications. , 135(11), 46-50. https://doi.org/10.5120/ijca2016908549

[10] Kester, Q. (2013). A Hybrid Cryptosystem Based On Vigenere Cipher and Columnar Transposition Cipher. Cornell University. https://doi.org/10.48550/arxiv.1307.7786

[11] Voleti, L., Balajee, R M., Vallepu, S K., Bayoju, K., & Srinivas, D. (2021). A Secure Image Steganography Using Improved Lsb Technique And Vigenere Cipher Algorithm. https://doi.org/10.1109/icais50930.2021.9395794

[12] Bashardoost, M., Sulong, G. B., & Gerami, P. (2013). Enhanced LSB image Steganography method by using knight Tour algorithm, Vigenere Encryption and LZW compression. International Journal of Computer Science Issues (IJCSI), 10(2 Part 1), 221.

[13] Arroyo, J C T. (2020). An Efficient Least Significant Bit Image Steganography with Secret Writing and Compression Techniques. The World Academy of Research in Science and Engineering, 9(3), 3280-3286. https://doi.org/10.30534/ijatcse/2020/124932020

[14] Barter, A. (2016). Index of Coincidence – Cryptography

[15] Shevchuk, O. (2020). Introduction to Elliptic Curve Cryptography.