Online-Journals.org

iJIM International Journal of Interactive Mobile Technologies

iJIM | eISSN: 1865-7923 | Vol. 18 No. 16 (2024) | OPEN ACCESS

https://doi.org/10.3991/ijim.v18i16.48709

PAPER

Digital-Signature Oriented Steganography Approach against Man-in-the-Middle Attack

Gwamaka Mwakajwanga[1](✉), Othmar Mwambe[2]

[1]Tanzania Communications Regulatory Authority (TCRA), Dar es salaam, Tanzania

[2]Dar es salaam Institute of Technology (DIT), Dar es salaam, Tanzania

gwamaka.mwakajwanga@got.go.tz

ABSTRACT

Nowadays, man-in-the-middle (MITM) attacks have become a large problem due to the advancement of computational power and interactive mobile technologies. Message security is a crucial concern that ought to be managed in order to help protect vital data from unauthorized people, such as MITM. Steganography is the technique of hiding secret data within an ordinary, non-secret file or message in order to avoid detection when communicating through an unsecured network. Steganography applications play a vital role in various fields that involve classified data transfer, such as healthcare, multimedia, and the military. Hence, the application of steganography in those fields attracts MITM attacks. Thus, in an attempt to address the challenge. This study proposes a hybrid approach that integrates an image steganography technique, the Advanced Encryption Standard (AES) for message encryption, and EdDSA (Edward-Curve Digital Signature Algorithm) for signature verification to enhance steganography against MITM attacks. The proposed hybrid approach was tested and measured using image metrics (MSE, PSNR, and SSIM) and histogram visualization and verified through experimentation. The results have proven that the proposed hybrid approach is an enhanced security approach with low execution time, more payload size for hiding messages, and a high invisibility embedded message to MITM compared with other existing approaches. This study has potential limitations. It does not explore tamper resistance or algorithm robustness, and it was not tested on a public image dataset.

KEYWORDS

digital signature, steganography, steganalysis, cryptography, LSB, EdDSA (Edward-Curve Digital Signature Algorithm), Advanced Encryption Standard (AES), cyber-security, man-in-the-middle attack (MITM)

1 INTRODUCTION

In this modern era, where technology is drastically increasing, governments and non-government organizations [1] have developed many steganography tools to detect and intercept the secret of either hidden embedded messages transferred through an unsecured communication channel or network that were being hidden

Mwakajwanga, G., Mwambe, O. (2024). Digital-Signature Oriented Steganography Approach against Man-in-the-Middle Attack. *International Journal of Interactive Mobile Technologies (iJIM)*, 18(16), pp. 158–173. https://doi.org/10.3991/ijim.v18i16.48709

Article submitted 2024-02-22. Revision uploaded 2024-05-13. Final acceptance 2024-05-13.

by steganography techniques. An unsecured communication channel is communication that is done on public networks and social media applications such as Facebook or WhatsApp with the aim of defying the user into believing that there is no communication happening. Covert communication can be achieved through digital steganography, which is the art of hiding digital data in another digital medium such that the hidden data is not visible to human inspection or steganography tools [2] [3]. Application of steganography varies for many uses, such as in the military, intelligence agencies, law enforcement, activism, and it can also be applied in digital forensics to hide communication. Steganography communication contains sensitive and secret data. That's why hackers, private sector organizations, and governments are struggling to intercept and detect hidden communication through surveillance or monitoring of communication within a country with the purpose of either protecting national interest or eavesdropping on other organizations information [4] [5]. Steganography must be secured so that third parties cannot access the hidden data. Steganography techniques [6] can be applied through different computer file formats: text, image [7], video, audio, network [8], and DNA steganography.

Several recent survey studies on image steganography [1, 2, 4, 5, 6, 7, 10], have found that many image steganography methods have considered three properties (hiding capacity, robustness, and security) as performance measures. However, as the communication to transfer data happens through untrusted channels or third-party channels, there are possibilities for man in the-middle attacks. Tampering or altering of the stego image by a man-in-the-middle (MITM) can also happen during the data transfer. Therefore, they suggest that in order to ensure the security of the stego image, the design of the algorithm against MITM attacks must be considered for evaluation with other image metrics.

A MITM attack [11] is a cyber-attack in which an attacker secretly eavesdrops on the communication of two or more parties who have no idea that their communication is being altered or listened to. The purpose of the MITM may be to listen or modify the communication for his or her own interest. A MITM attack is dangerous because users can continue on with their activities for days or even weeks without noticing that something is wrong. In steganography, these men-in-the-middle perform an attack by using steganalysis techniques such as visual, statistical, transform domain, signature, and blind steganalysis.

Steganalysis tools [12] that can be used by MITM can detect embedded data in images using convolutional neural networks with a success rate of 89 percent. Even [13] can classify images that contain hidden information and those that do not contain hidden information, and the results stimulate the ability of data to be discovered by MITM. Nonetheless [14], the ensemble classifier can also be used to detect the hidden message with high accuracy compared to deep learning algorithms.

It is important to enhance security in steganography so that it increases confidence in the sender and receiver of the communication that no third party has accessed classified data. The classified data is very sensitive because of its originality. For example, in healthcare [15], steganography helps to secure patient information that is transferred across hospitals using various IOT devices and also secures [16] patient reports on DICOM images. Steganography can be used [17] to detect and protect copyright infringement on images. A prototype of covert communication [18], to be used by the military across the 5G public network, was developed. Furthermore, steganography [19] can be used to achieve authentication only for intended users by hiding the information through a CAPTCHA image.

The goal of the steganography technique is to ensure the communication remains invisible, and since the communication is conducted through an unsecured channel, the proposed algorithm must prove to the receiver and sender that the message has been

sent from a known sender and has not been altered in the middle of the communication. Therefore, the main target of this study is to provide least significant bit (LSB) steganography with double security by applying an encryption algorithm as well as a digital signature for message verification. The proposed hybrid algorithm will secure hidden messages from unintended men in the-middle like hackers and crackers who are using brute force attack and steganography tools. The hybrid approach will ensure maximum capacity, invisibility, and imperceptibility of the embedded message in the cover image.

The remainder of this paper is divided into six sections: Section I provides an introduction, and Section II provides a literature review on related works. The methodology for conducting this study is described in Section III. The findings are listed in Section IV. Section V addresses the discussion of this study, while Section VI includes the conclusion and suggestions for future work.

2 BACKGROUND INFORMATION AND RELATED WORKS

A) *Background information*

There are many steganography techniques; thus, the standard properties for a good steganography were developed [9]. Five properties of good steganography are:

- **i)** Tamper resistance: means the steganography technique should resist the breaking of its algorithm by steganalysis [10] tools used to crack the technique.
- **ii)** Robustness: the ability to withstand any condition, such as image resizing, image cropping, or image compression, should make the algorithm perform what it is supposed to do.
- **iii)** Invisibility: the hidden message shall not make anyone suspicious of its being in the stego object.
- **iv)** Capacity: the payload size of the hidden message shall be greater without affecting other properties. The larger size that can be hidden on one stego object means you will need a small number of stego objects for the whole message to be hidden.
- **v)** Imperceptibility: the difference between the object without a hidden message and the one with a hidden message shall be slightly small or not at all.

A digital signature [20] produces a unique electronic signature that can be used to sign and verify a digital file for authenticity, integrity, and non-repudiation. Digital signatures employ asymmetric cryptography, which uses two different keys: a public key for signing and a private key for verifying the signature. A private key must be kept private by a receiver so that no other user can produce the same signature without the key. There are many different digital signature algorithms, such as DSA (Digital Signature Algorithm), RSA (Rivest Shamir Aldeman) [21], ECDSA (Elliptic-Curve digital signature algorithm) [22], EdDSA (Edward-Curve Digital Signature Algorithm), and ElGama Signature Scheme.

EdDSA [23] is an asymmetric encryption algorithm that depends on a twisted Edward curve. The EdDSA signatures use the Edwards form of an elliptic curve, respectively, edwards25519 and edwards448. The internal hash function of Ed25519 is SHA-512, and the internal hash function of Ed448 is SHAKE256.

$$\text{The Ed25519 has a prime: } p = 1 \ (mod\ 4)$$

$$\text{Ed448 has a prime: } p = 3 \ (mod\ 4)$$

EdDSA can produce a high security level with a shorter key length compared to other digital signature algorithms [24]. EdDSA ensures the non-repudiation of

the sender, and even if a third party or MITM obtains a stego message, he cannot produce the same signature as the original embedded message.

Advanced Encryption Standard (AES) [25] is a symmetric encryption algorithm that uses one key for data encryption and decryption. AES is a block cipher algorithm that operates on data of 128 bits, or 16 bytes. It is considered the most secure symmetric encryption algorithm, with different encryption key sizes that range from 128, 192, and 256 bits. The AES algorithm uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys [26]. As the key size is high, the more secure the algorithm becomes, which means that in the case of a brute force attack, it can take many years for the supercomputer to crack the algorithm.

B) *Related works*

A lot of scholars have done several works in line with data security improvements in image steganography. Some aimed at ensuring the privacy and integrity of data using cryptography algorithms, while others were ensuring strong steganography algorithms so that hidden messages could not be detected. To gain a better understanding, there is a need for a critical review of related works, as presented in this section.

According to B. Karthikeyan et al. [27], they suggested using the combination of the RSA algorithm with image steganography to enhance the security of the embedded message. Their results showed that the combination led to improved data security; however, the time consumed for the encryption and decryption processes was much higher, and the approach of RSA led to a small capacity of the embedded message because most of the payload size capacity was consumed by the high key length produced by Rivest Shamir Aldeman.

In their study, V. Kalaichelvi et al. [28], they proposed a combination of both cryptography and steganography for providing security in image steganography. Using modified hill cipher algorithms helps enhance the security of the embedded message. However, a recent study paper shows that the modified hill cipher, which is based on matrix operations, has a proven vulnerability when it comes to dealing with known plain-text attacks due to its linear dependency.

In their study, M. Kataria et al. [29], they investigate the use of modern steganography techniques for secure image transmission by making use of four encryption algorithms (AES, DES, RSA, and ChaCha20). LSB and Spread Spectrum image steganography techniques are used to encode and decode cipher text into five different images. Their analysis shows that DES is less effective than AES and ChaCha20 for encryption. However, the use of RSA leads to high execution times during encryption and decryption compared to elliptic curve algorithms.

In their paper, S. Bhargava et al. [30] presented the protection of embedded messages by encrypting them using the AES algorithm on the least significant bit (LSB) steganography algorithm. Their study pointed out that the use of the AES algorithm protected the message even if the message or medium was compromised by MITM. However, this approach did not ensure integrity or non-repudiation of the message from the sender, and the use of only a single key compromises security because it depends on both sides to ensure the private key is kept safe.

D. Kumbhakar et al. [31], they proposed a way of securing e-commerce data by using Elgamal encryption and LSB steganography. They measured the performance of their proposed approach using MSE, PSNR, and SSIM. Their results showed that their approach has succeeded in securing e-commerce information.

According to A. Bahaddad [32], the security of hidden information can be done using chaotic encryption so that no man in the-middle can uncover the hidden information. They succeeded in securing the hidden information; however, chaotic encryption has challenges in terms of security and speed.

In view of the various attempts to address MITM attacks using various algorithms that ensure the security of the hidden message, a lot of scholars have proposed the use of RSA as a digital signature algorithm, but the use of RSA shows us that there is still a gap as there is a new modern digital signature algorithm giving the same level of security or even higher by using shorter key length and faster signing and verification than other digital signature algorithms. Thus, unlike previous approaches, the proposed approach in this study applies an encryption algorithm as well as a digital signature for verification.

3 PROPOSED APPROACH

In this study, a hybrid approach that applies an encryption algorithm as well as a digital signature for verification has been introduced. The proposed approach includes two sides of the communication: side one is for the sender, and side two is for the receiver. Each side will have three stages to perform, and the message between sender and receiver can be communicated on unsecured networks such as social networks (WhatsApp, Telegram), games, and other applications that do not raise suspicion. The message cannot be sent directly to the receiver, but instead the sender can use public networks, such as by posting it as a normal image, and therefore many receivers can be able to download and view it, but only the receiver with the right tools and a private decryption key can decrypt and verify the embedded message. Figure 1 shows the proposed design of a hybrid algorithm.

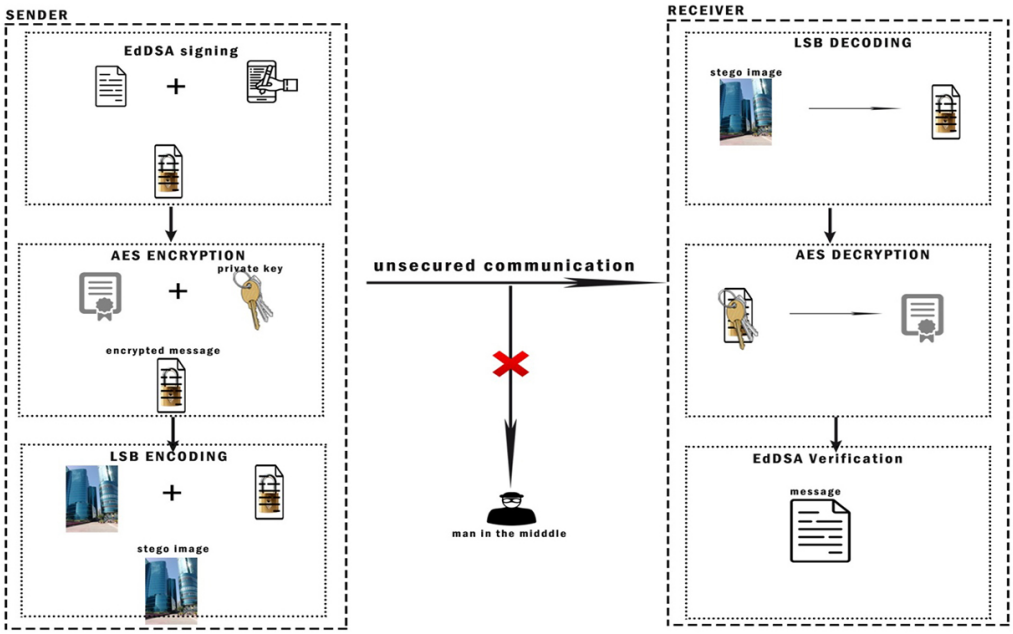

Fig. 1. Proposed hybrid algorithm flowchart

The two sides of the proposed approach are:

A) *Sender side*

1. *Message signing using the EdDSA public key.*
2. *Encryption of a signed message using an AES secret key.*
3. *LSB encodes the embedded message into the cover image.*

B) *Receiver side*

1. LSB decoding to recover embedded messages from the cover image
2. Decryption of a signed message using an AES secret key
3. Verification of the embedded message using the private key of the digital signature.

On the sender side, the transfer of images from the sender to the receiver side through an unsecure channel can be applied. Then the stego image will be received, and decoding of the hidden message from the image will be performed. The proposed algorithm has been implemented using the Python programming language and tested with randomly chosen images and a secret message to obtain results for evaluation and analysis. Below is a brief explanation of how each of the algorithms used to create a hybrid approach is functioning.

a) *EdDSA (Edward-curve digital signature algorithm)*

The digital signature Ed25519 uses a variant of the Schnorr signature based on twisted Edwards curves using the internal hash functions SHA-512 and curve25519. The Ed25519 algorithm is based on the elliptic curve defined over the prime field of

$$q = 2^{255} - 19$$

E/F_q Twisted Edward curve is given by:

$$-x^2 + y^2 = 1 - \frac{121665}{121666} x^2 y^2$$

The Ed25519 algorithm has four stages, starting with encoding, key generation, signing, and verification.

i) Key Generation

Two keys are generated in this stage, private and public key. The private key is used to generate digital signatures, while the public key is used to verify the signatures. The private key is a 256-bit integer, while the public key is a 32-byte sequence. The private key is encoded as 64 hex digits (32 bytes).

ii) Signing

iii) Verification

b) *Advanced Encryption Standard*

The encryption part has been implemented using AES-256. AES-256 encryption uses the 256-bit key length to encrypt as well as decrypt a block of messages. AES relies on the substitution permutation network principle, which means it is performed using a series of linked operations that involve replacing and shuffling the input data. The first process is the creation of round keys from a secret key by using the key schedule algorithm. Then it is followed by the encryption process, which is done on every round in four steps except for the last round, which does not have a mixColums step.

- Byte substitution (SubBytes)
- Shift rows
- Mix columns
- Add round key

Lastly, there is the decryption part with a secret key, in which the process is done in reverse of the encryption process:

- Add round key
- Mix columns

- Shift rows
- Byte substitution

c) *LSB steganography technique*

The least significant bit (LSB) is the lowest bit in a binary number; it can be the leftmost or rightmost bit. Data in images is stored using pixels, and each pixel contains the color representation of that area in RGB (red, green, and blue). Each value of the RGB has 8-bit values. The LSB technique, which is the Least Significant bit, encodes the secret message into a cover image by replacing the least significant bit of an image pixel, and by replacing these bits, there will be no greater effects on the image. For example, if the pixel has a color value of green (#00ff00), even if all the least significant bits are replaced, it will still have the same color and will have high imperceptibility to the user since it will have a value of green (#01fe00). Figure 2 shows the pixel data before performing LSB and the color after replacing its significant bit.

Fig. 2. LSB steganography technique

Performing the LSB Steganography technique to embed the encrypted, signed message into the cover image, ready to transfer on an unsecured communication channel. The main target of the proposed approach is to provide double security for the embedded secret messages by applying encryption algorithms as well as image steganography techniques. Here, the asymmetric key cryptography algorithm is used to verify the message, whereas the symmetric key, an algorithm is used to encrypt and decrypt embedded messages. So, dual security for the embedded message is achieved in this proposed work.

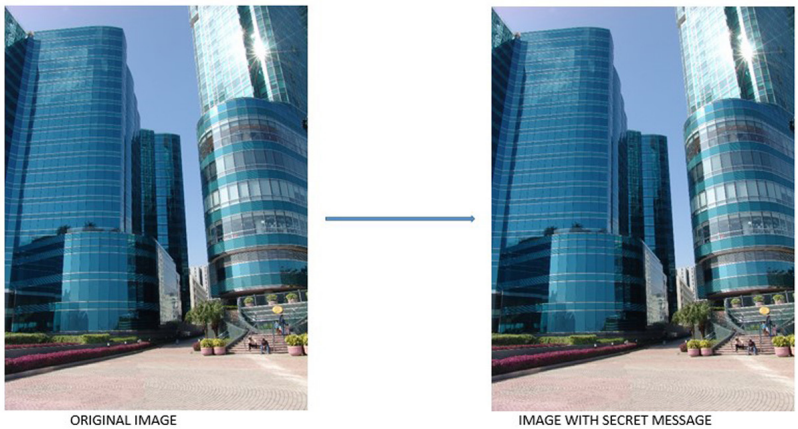

Fig. 3. Before and after decoding with LSB steganography images

4 RESULTS

In this section, the results obtained, the result analysis, and the evaluation of the proposed algorithm are revealed. In steganography, image evaluation metrics are used to measure the invisibility level, message security, and payload capacity of the proposed methods. Table 1 shows the security level of the digital signature algorithms (RSA and EdDSA) that can be obtained by using key lengths of different sizes. The most commonly used metrics in image steganography are MSE, peak signal-to-noise ratio (PSNR), structural similarity index (SSIM), and histogram visualization. In our experiment, all the evaluation metrics were conducted and the results were recorded (refers to Table 2), and apart from the evaluation metrics, the amount of time used during encryption and decryption of different message sizes (RSA and EdDSA) was recorded.

The EdDSA algorithm produces the same security level of 128 by key length of 256 bits and RSA by key length of 3072 bits. The experiment using both EdDSA and RSA was conducted to generate a digital certificate for the secret message, which had 73 bytes. The certificate generated by the EdDSA algorithm was 128 bytes long, while the certificate generated by the RSA algorithm was 512 bytes longer.

Table 1. Digital signatures algorithms strength

Security Level	ECC	RSA
80	160 bits	1024 bits
112	224 bits	2048 bits
128	**256 bits**	**3072 bits**
192	384 bits	7680 bits
256	512 bits	15360 bits

Example:
The embedded secret message.

```
TOP SECRET: The enrichment of uranium will be at full scale on July 2025.
```

Digital certificate generated after signing using EdDSA algorithm.

```
6de687dd5cbdef39d48755ed9451cdfddaf501346332eea4634c8b23358931039699d0b1d190c50092046444
cc304c9a5e8f2420aa483e8d9332109b0bbea90c
```

Digital certificate generated after signing using RSA algorithm.

```
ZoR6m1Fcq1ZH83E7ULglwGgSk3eME91C3FuA9Qaah+JtGdHy/sJi4QbFRON+wV2ETjXdx7d9CCSUOmA8XZJ8
Aw2UZneD4P5OBsdXkDGbCOvAlsQmdwHab7vHwCyT6Pup+KgYN7St0w9NY/2SrizA+jiZlju2uiPK9O6ji9X/543
Epu+KimCeTHysQdPl5Ho+1FMozKu04MoM7HnWoYU1BHQmRcmtnGmOADTvyu+DiG/uFxddRPcy4y6ckLMS
038jJQHfC9H4I3qz/1dfz5IiGs99OHJnqYkjdmwJmlmmAKzFzEV38l/YME6wXQLJmhtfm9nCmIfjBi91lBc+a3yB5
UIdzydHWrCCkl9SzeH7PzqLuDk0BUtga94XicFjKLDQB70yl/kpn8DXCURD0Ft/SiVGDDEzjbh6zowHbi9bToWz
Fn2YKRbjtQ23f+kqO8JSdU3YzHhVqS+dZ5HMlhSIvc3nCobxjBD9BPR71bqa3k8IjW2aYqmuaWuhCRwh2I/0
```

Below are the metrics used to get the results of our experiment and an explanation of how they are measured and calculated.

A) *MSE*

Mean squared error (MSE) is one of the metrics used to measure the quality of the reconstructed stego image. The cumulative squared error between the stego image and the original cover image is the Mean squared Error. For better quality images, the value of MSE has to be low indicating that the error is low. The best MSE value is 0.0. A high value of MSE in image steganography can result in attracting attention from MITM due to changes in major changes that occur in image pixels.

$$MSE = \frac{1}{MN}\sum_{J=1}^{M}.\sum_{k=1}^{N}\left(x_{jk} - x'_{jk}\right)^2$$

B) *Peak Signal to Noise Ratio*

Peak Signal to Noise Ratio (PSNR) is used to measure the image quality, method robustness, and data invisibility of the steganography method. The ratio value between the maximum quality representation of the normal image and the stego image is the PSNR. The PSNR value has to be high (100), because the higher the value, the better the quality of the reconstructed image.

Since the image pixels are changed, the value of PSNR can show how well our data is concealed, so it can hard to be detect.

$$PSNR = 10\log\frac{(2^n - 1)^2}{\text{MSE}}$$

C) *Structural similarity index*

Structural similarity index (SSIM) is used to examine the quantitative quality of a compressed image. Images can undergo changes, such as being compressed, resized, or converted to different formats, and in the process, there can be a loss of quality and fidelity between the original image and the image that undergoes changes. The assessment of SSIM Index quality is based on three factors: structure, contrast, and luminance. The values of SSIM range between 0 and 1, where the value of 0 means no match and the value of 1 means there is a perfect match between the original image and the copy of it. The SSIM between the stego-image and the original image shows how the structure of the original image has changed from the original image.

$$SSIM(x, y) = \frac{\left(2\mu_x\mu_y + C_1\right)\left(2\theta_{xy} + C_2\right)}{\left(\mu_x^2 + \mu_y^2 + C_1\right)\left(\theta_x^2 + \theta_y^2 + C_2\right)}$$

Table 2. Obtained results using python

Algorithm	*MSE*	*PSNR*	*SSIM*
LSB with EdDSA	8.51e-6	93.45 dB	0.9999999808891369
LSB with RSA	5.06e-5	85.02 dB	0.9999998834338114

D) *Histogram visualization*

Histogram metrics are useful to show distribution variables in images. Histograms are graphs that divide the entire range of measurements into a set of intervals and count how many measurements fall into each bucket (see Figure 4). A histogram of two or more images can be compared by looking at how the distribution of variables differs from one image to another. The same image shows

no difference in histogram, while the differences between the stego image and the normal image can be compared to see how they differ. The small difference in variable frequency means the image looks the same and cannot attract any attention from men-in-the-middle.

E) *Computation time*

Computation cost must be considered because lowering execution time means increasing execution speed. The execution time of the hybrid approach was recorded and compared between the proposed approach (LSB with EdDSA) and the existing approach (LSB with RSA). The computation cost in terms of time of an algorithm is calculated based on the time it takes to execute a number of inputs (n). In steganography, the computation cost is analyzed based on the time it takes to execute the LSB steganography technique on different sample images. Therefore, in our experiment, randomly selected secret message lengths are used in a test (refer to Table 3).

Table 3. Encoding and decoding execution time

Sample Images	LSB Encoding		LSB Decoding	
	EdDSA + AES	*RSA + AES*	*EdDSA + AES*	*RSA + AES*
Image 1	301.40 ms	440.70 ms	138.91 ms	140.20 ms
Image 2	291.70 ms	398.42 ms	139.50 ms	138.41 ms
Image 3	298.14 ms	479.81 ms	133.14 ms	139.80 ms
Image 4	319.20 ms	472.85 ms	139.25 ms	142.82 ms
Image 5	305.70 ms	446.00 ms	135.30 ms	140.80 ms

5 DISCUSSION

The outcomes of this study have provided insight on how the proposed approach can provide security to the hidden message. Analysis of the obtained results are compared based on properties of a good steganography:

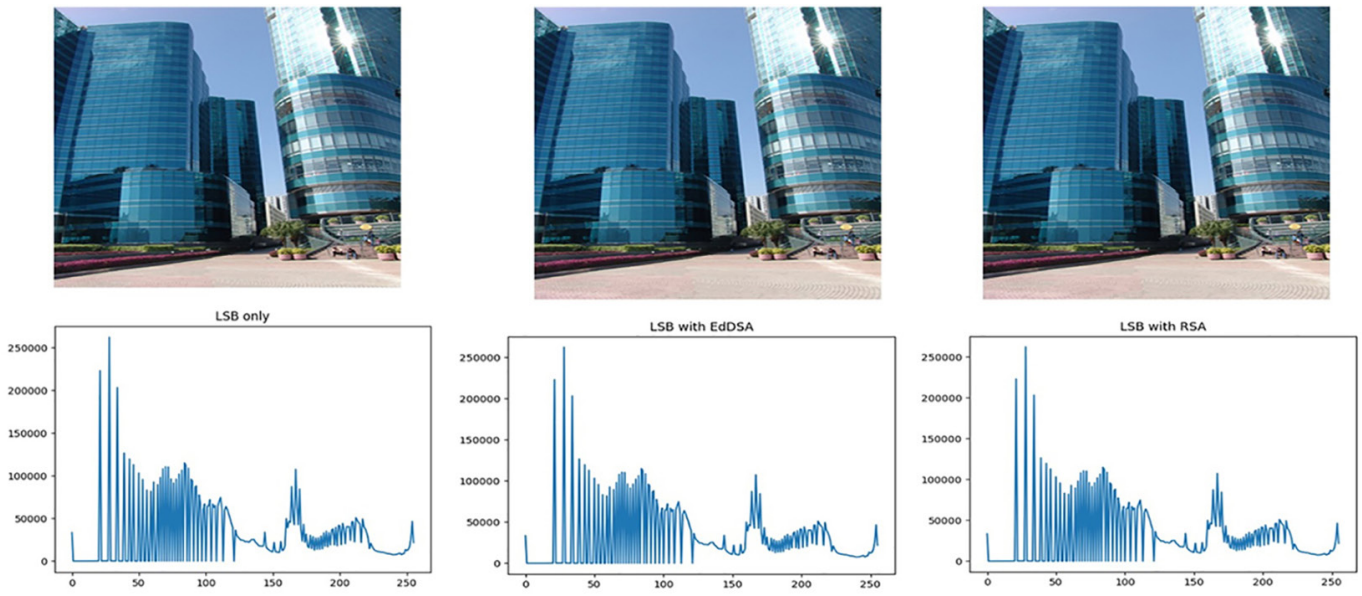

Fig. 4. Histogram visualization showing frequency of variables between images with LSB only, LSB with EdDSA and RSA

A) *Higher security*

The cryptography security level depends on the key length (see Table 1) and the amount of time an algorithm takes to crack. The EdDSA (ed25519) can produce the same level of security or even higher compared to the RSA 3072 bits with just 256 bits. The security of hidden messages in steganography is measured by evaluating the results of image metrics. One of the metrics is PSNR, and its results have shown (see Figure 5) that by using the EdDSA algorithm, the value is 93.45 dB, whereas in the LSB with RSA, the value is 85.02 dB. Since the higher the value, nearly 100, the lower the image distortion. The steganography technique should have high security on embedded data, and the proposed hybrid approach has proven that the embedded data is more secure due to enhancing it with the double security of a digital certificate of EdDSA and AES encryption. The use of two cryptography algorithms, symmetric and asymmetric, makes it difficult for man in the middle to uncover the embedded message since the message is double encrypted using the most advanced encryption algorithm but also digitally signed by the most secure and faster digital signature algorithm.

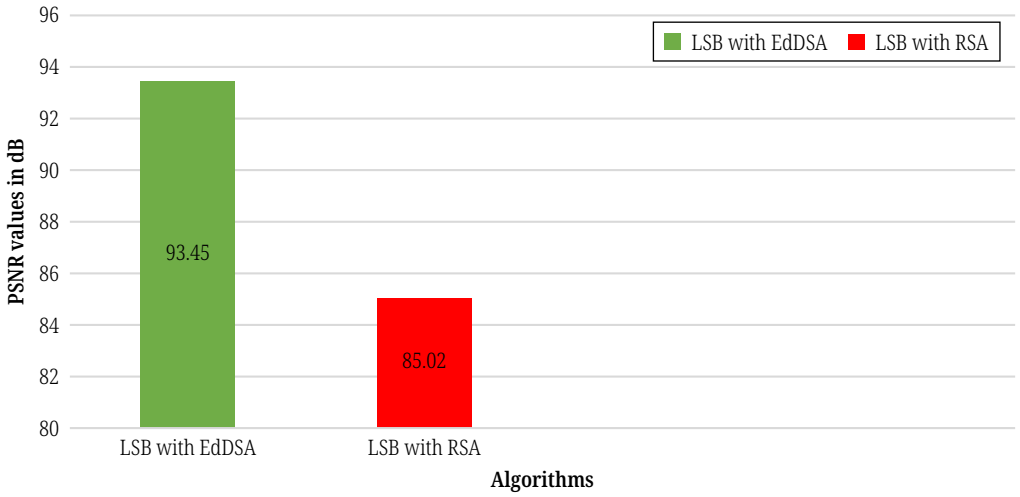

Fig. 5. Comparison chart

B) *Invisibility*

The visualization of the histogram shows that there is no difference in the frequency distribution of variables in an image between cover images encoded with LSB and cover images encoded with either LSB, EdDSA, or AES, which means the image does not attract any attention from normal human eyes compared to the slightly different image using RSA. The slight difference means there is a small distortion to the image pixels, therefore a small attention to the human eyes.

The MSE results have shown that there is a slight difference between EdDSA and RSA. The EdDSA algorithm shows that its mean squared error of 8.51e-6 is very small, approximately 0, which implies that the error can be approximately equal to zero.

Also, the SSIM results have shown that there is a slight difference between EdDSA and RSA. The EdDSA algorithm shows that the value was 0.9999999808891369, and the RSA value was 0.9999998834338114. Both are nearly 1, which is a good indicator, but EdDSA is better compared to Rivest Shamir Aldeman.

C) *Payload capacity*

As we have seen in Table 1, the same security level can be attained by RSA with a longer key length as can be achieved by a short key length with the EdDSA algorithm.

And as the security level increases, the key length of RSA increases more than that of EdDSA, which still has a shorter key length. The hidden message size on RSA is consumed more by the size of the digital signature certificate it provides, while on the EdDSA algorithm, the size is consumed by the message itself. The payload capacity of embedded messages is high in the proposed approach due to the short key length of the EdDSA compared to the RSA. The EdDSA signatures have a length of 128 bytes for Ed25519, while RSA signatures are as long as the key size, which is at least 512 bytes, which is about 4 times bigger. By considering that the payload consumption on a cover image must be low so that it does not distort the appearance and attract attention to MITM, EdDSA can produce the highest security level while saving more space for hidden messages. Therefore, this shows that the payload capacity of embedded messages using EdDSA has been raised by 75% compared to Rivest Shamir Aldeman.

D) *Computation cost*

Figures 6 and 7 are images of two graphs showing the results that have been obtained in Table 3. Figure 6 shows two lines that compare the LSB encoding when messages have been encrypted and signed using the AES, EdDSA, and RSA algorithms. Also, Figure 7 compares the time taken for LSB decoding while the messages are encrypted and verified using the AES, EdDSA, and RSA algorithms.

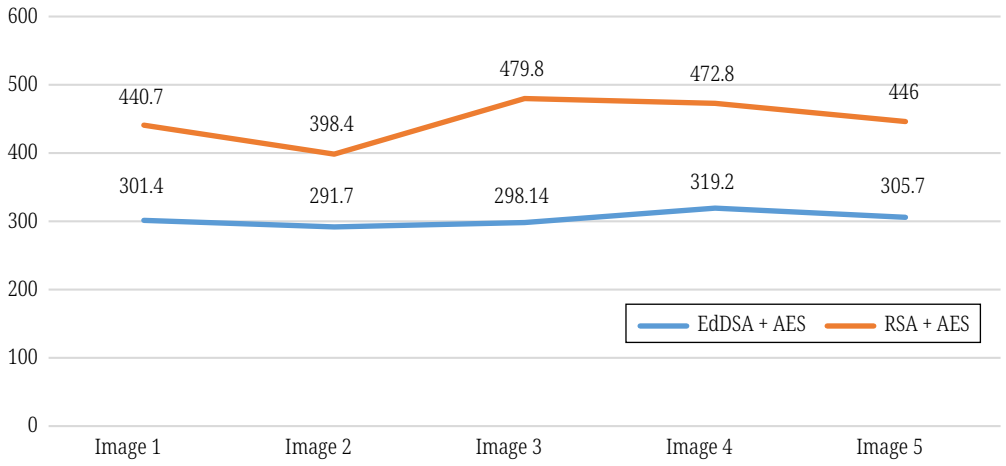

Fig. 6. LSB Encoding chart

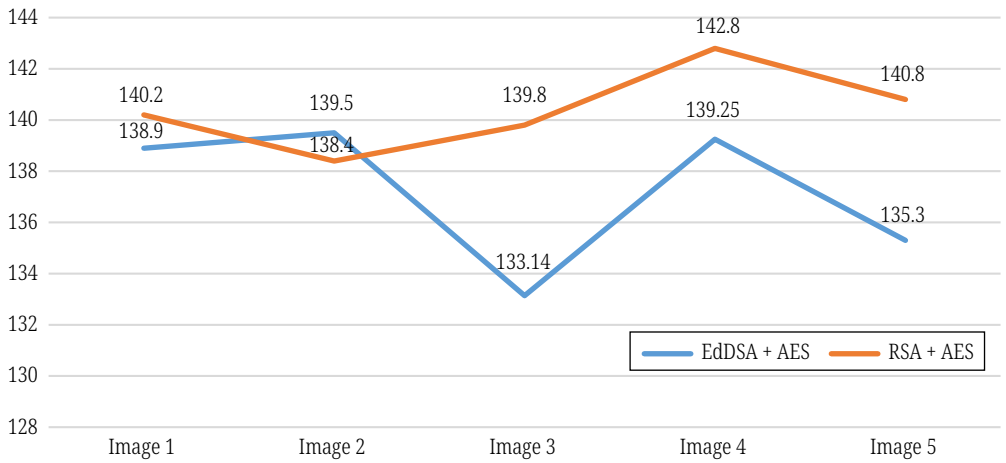

Fig. 7. LSB Decoding chart

The computation cost (space and time) should be low to have good LSB steganography. By observing the execution time taken (see Figure 6), the analysis shows that the line representing the time of LSB steganography encoding with AES encryption and message signing using the EdDSA algorithm is low on each sample image that was tested. Also, by observing the execution time taken (see Figure 7), the analysis shows that the line representing the time of LSB steganography decoding with AES encryption and message verification using the EdDSA algorithm is low on each sample image that was tested compared to the existing approach. The chart shows that on the different sample images from which the experiment was conducted EdDSA still performs better than other digital signature algorithms, such as Rivest Shamir Aldeman.

6 CONCLUSION

Our results show us that the mean squared error of 8.51e-6 is very small, approximately 0, which proves that the proposed approach has scored highly in terms of invisibility. Also, the proposed approach saved the space occupied by hidden messages by more than 75% compared to the existing approaches. Nonetheless, the EdDSA has increased execution speed by lowering execution time compared to existing approaches. Hence, the use of AES and EdDSA ensures high data security while transferring images over an unsecured network, even in the presence of man-in-the-middle attacks.

As the main objective of this study is to double the security of embedded messages in image steganography, the proposed hybrid approach algorithm based on the EdDSA algorithm and steganography technique has shown that it has enhanced the security strength of the normal LSB steganography technique by the use of digital signatures, which ensure integrity (that no one has changed the message) and non-repudiation (that the sender is who is supposed to be), and also by the use of AES, which encrypts the data so that only the user with a secret key can decrypt the message.

Even though the proposed hybrid approach has proven to enhance the security strength of hidden messages encoded by the LSB steganography technique. However, to ensure tamper resistance and algorithm robustness, more exploration is recommended. Also, the proposed approach was not tested on publicly known image datasets. Therefore, we are looking forward to working on securing steganography techniques using deep learning algorithms in order to let neural networks work on themselves against man-in-the-middle attacks.

7 ACKNOWLEDGMENT

We would like to acknowledge financial support from the Tanzania Communications Regulatory Authority (TCRA).

8 REFERENCES

[1] V. Annapurna, S. Nagaraja Rao, and M. N. Giriprasad, "A survey of different video steganography approaches against man-in-the middle attacks," in *2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 2021, pp. 1601–1607. https://doi.org/10.1109/I-SMAC52330.2021.9640974

[2] N. Subramanian *et al.*, "Image steganography: A review of the recent advances," *IEEE Access*, vol. 9, pp. 23409–23423, 2021. https://doi.org/10.1109/ACCESS.2021.3053998

[3] R. Sindhu and P. Singh, "Information hiding using steganography," *International Journal of Engineering and Advanced Technology*, vol. 9, no. 4, pp. 1549–1554, 2020. https://doi.org/10.35940/ijeat.D8760.049420

[4] N. Pattani *et al.*, "Survey on image steganography techniques," *International Journal for Research in Emerging Science and Technology*, vol. 2, 2015.

[5] D. Megías, W. Mazurczyk, and M. Kuribayashi, "Data hiding and its applications: Digital watermarking and steganography," *Appl. Sci.*, vol. 11, no. 22, p. 10928, 2021. https://doi.org/10.3390/app112210928

[6] M. Dahiya and R. Kumar, "A literature survey on various image encryption & steganography techniques," in *2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC)*, 2018, pp. 310–314. https://doi.org/10.1109/ICSCCC.2018.8703368

[7] P. C. Mandal, I. Mukherjee, G. Paul, and B. N. Chatterji, "Digital image steganography: A literature survey," *Information Sciences*, vol. 609, pp. 1451–1488, 2022. https://doi.org/10.1016/j.ins.2022.07.120

[8] A. Ganivev, O. Mavlonov, B. Turdibekov, and M. Uzoqova, "Improving data hiding methods in network steganography based on packet header manipulation," in *2021 International Conference on Information Science and Communications Technologies (ICISCT)*, 2021, pp. 1–5. https://doi.org/10.1109/ICISCT52966.2021.9670109

[9] S. Ramakrishnan, *Cryptographic and Information Security Approaches for Images and Videos.* Boca Raton: CRC Press, 2020. https://doi.org/10.1201/9780429435461

[10] D. A. Shehab and M. J. Alhaddad, "Comprehensive survey of multimedia steganalysis: Techniques, evaluations, and trends in future research," *Symmetry*, vol. 14, no. 1, p. 117, 2022. https://doi.org/10.3390/sym14010117

[11] M. Conti, N. Dragoni, and V. Lesyk, "A survey of man in the middle attacks," *IEEE Communications Surveys and Tutorials*, vol. 18, no. 3, pp. 2027–2051, 2016. https://doi.org/10.1109/COMST.2016.2548426

[12] K. Anuratha, J. M. Nandhini, D. Madhavan, A. Harini, and P. Arulmani, "Securing web user privacy with steganalysis of images using deep learning," in *2022 7th International Conference on Communication and Electronics Systems (ICCES)*, 2022, pp. 1215–1220. https://doi.org/10.1109/ICCES54183.2022.9836021

[13] O. Juarez-Sandoval, M. Cedillo-Hernandez, G. Sanchez-Perez, K. Toscano-Medina, H. Perez-Meana, and M. Nakano-Miyatake, "Compact image steganalysis for LSB-matching steganography," in *2017 5th International Workshop on Biometrics and Forensics (IWBF)*, 2017, pp. 1–6. https://doi.org/10.1109/IWBF.2017.7935103

[14] M. Płachta, M. Krzemień, K. Szczypiorski, and A. Janicki, "Detection of image steganography using deep learning and ensemble classifiers," *Electronics*, vol. 11, no. 10, p. 1565, 2022. https://doi.org/10.3390/electronics11101565

[15] H. N. AlEisa, "Data confidentiality in healthcare monitoring systems based on image steganography to improve the exchange of patient information using the internet of things," *J. Healthc. Eng.*, vol. 2022, no. 1, 2022. https://doi.org/10.1155/2022/7528583

[16] M. A. Ahmad *et al.*, "Hiding patients' medical reports using an enhanced wavelet steganography algorithm in DICOM images," *Alexandria Engineering Journal*, vol. 61, no. 12, pp. 10577–10592, 2022. https://doi.org/10.1016/j.aej.2022.03.056

[17] P. K. Kulkarni and G. Kulkarni, "A copyright protection scheme for grayscale images using wavelet transform and Arnold transform," in *2020 IEEE Bangalore Humanitarian Technology Conference (B-HTC)*, 2020, pp. 1–6. https://doi.org/10.1109/B-HTC50970.2020.9298018

[18] E. Alwan *et al.*, "Covert and quantum-safe tunneling of multi-band military-RF communication waveforms through non-cooperative 5G networks," in *MILCOM 2023 – 2023 IEEE Military Communications Conference (MILCOM)*, 2023, pp. 83–88. https://doi.org/10.1109/MILCOM58377.2023.10356300

[19] T. Kalaichelvi and P. Apuroop, "Image steganography method to achieve confidentiality using CAPTCHA for authentication," in *2020 5th International Conference on Communication and Electronics Systems (ICCES)*, 2020, pp. 495–499. https://doi.org/10.1109/ICCES48766.2020.9138073

[20] N. Cavus and N. Sancar, "The importance of digital signature in sustainable businesses: A scale development study," *Sustainability*, vol. 15, no. 6, p. 5008, 2023. https://doi.org/10.3390/su15065008

[21] X. Zhou and X. Tang, "Research and implementation of RSA algorithm for encryption and decryption," in *Proceedings of 2011 6th International Forum on Strategic Technology*, 2011, pp. 1118–1121. https://doi.org/10.1109/IFOST.2011.6021216

[22] S. Lamba and M. Sharma, "An efficient elliptic curve digital signature algorithm (ECDSA)," in *2013 International Conference on Machine Intelligence and Research Advancement*, 2013, pp. 179–183. https://doi.org/10.1109/ICMIRA.2013.41

[23] S. Josefsson and I. Liusvaara, "Edwards-curve digital signature algorithm (EdDSA)," RFC Editor, 2017. https://doi.org/10.17487/RFC8032

[24] M. Suarez-Albela, P. Fraga-Lamas, and T. M. Fernandez-Carames, "A practical evaluation on RSA and ECC-based cipher suites for IoT high-security energy-efficient fog and mist computing devices," *Sensors*, vol. 18, no. 11, p. 3868, 2018. https://doi.org/10.3390/s18113868

[25] F. J. D'souza and D. Panchal, "Advanced encryption standard (AES) security enhancement using hybrid approach," in *2017 International Conference on Computing, Communication and Automation (ICCCA)*, 2017, pp. 647–652. https://doi.org/10.1109/CCAA.2017.8229881

[26] E. Fernando, D. Agustin, M. Irsan, D. F. Murad, H. Rohayani, and D. Sujana, "Performance comparison of symmetries encryption AlgorithmAES and DES with Raspberry Pi," in *2019 International Conference on Sustainable Information Engineering and Technology (SIET)*, 2019, pp. 353–357. https://doi.org/10.1109/SIET48054.2019.8986122

[27] B. Karthikeyan, B. Bharathkumar, G. Manikandan, and R. Seethalakshmi, "A combination of RSA algorithm with image steganography to ensure enhanced encryption," in *2023 Second International Conference on Electronics and Renewable Systems (ICEARS)*, 2023, pp. 773–777. https://doi.org/10.1109/ICEARS56392.2023.10085371

[28] V. Kalaichelvi, P. V. Devi, S. Hemamalini, S. Swaminathan, and S. Suganya, "Implementation of hybrid cryptography in steganography for augmented security," in *2023 2nd International Conference on Smart Technologies and Systems for Next Generation Computing (ICSTSN)*, 2023, pp. 1–5. https://doi.org/10.1109/ICSTSN57873.2023.10151554

[29] M. Kataria, K. Jain, and N. Subramanian, "Exploring advanced encryption and steganography techniques for image security," in *2023 11th International Symposium on Digital Forensics and Security (ISDFS)*, 2023, pp. 1–6. https://doi.org/10.1109/ISDFS58141.2023.10131890

[30] S. Bhargava and M. Mukhija, "Hide image and text using LSB, DWT and RSA based on image steganography," *ICTACT Journal on Image and Video Processing*, vol. 9, no. 3, pp. 1940–1946, 2019. https://doi.org/10.21917/ijivp.2019.0275

[31] D. Kumbhakar, K. Sanyal, and S. Karforma, "An optimal and efficient data security technique through crypto-stegano for e-commerce," *Multimed. Tools Appl.*, vol. 82, pp. 21005–21018, 2023. https://doi.org/10.1007/s11042-023-14526-7

[32] A. A. Bahaddad, K. A. Almarhabi, and S. Abdel-Khalek, "Image steganography technique based on bald eagle search optimal pixel selection with chaotic encryption," *Alexandria Engineering Journal*, vol. 75, pp. 41–54, 2023. https://doi.org/10.1016/j.aej.2023.05.051

9 AUTHORS

Gwamaka Mwakajwanga is with the Tanzania Communications Regulatory Authority (TCRA), Dar es Salaam, Tanzania (E-mail: gwamaka.mwakajwanga@got.go.tz).

Othmar Mwambe is with the Dar es Salaam Institute of Technology (DIT), Dar es Salaam, Tanzania.