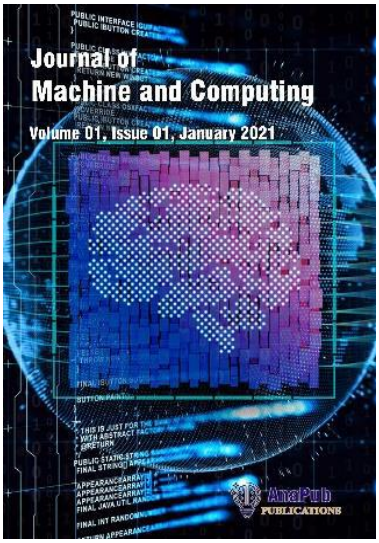
Journal Pre-proof



Enhancing Data Protection and Covert Communication in Cloud Environments with Isogeny-based Cryptography and Spread Spectrum Steganography

Shivaramakrishna D and Nagaratna M

DOI: 10.53759/7669/jmc202505023

Reference: JMC202505023

Journal: Journal of Machine and Computing.

Received 26 May 2024

Revised form 02 September 2024

Accepted 16 November 2024

Please cite this article as: Shivaramakrishna D and Nagaratna M, “Enhancing Data Protection and Covert Communication in Cloud Environments with Isogeny-based Cryptography and Spread Spectrum Steganography”, Journal of Machine and Computing. (2025). Doi: https:// doi.org/10.53759/7669/jmc202505023

Enhancing Data Protection and Covert Communication in Cloud Environments with Isogeny-based Cryptography and Spread Spectrum Steganography

D.Shivaramakrishna [1], Dr M.Nagaratna [2]
Department of Computer Science and Engineering, Jawaharlal Nehru Technological University, Kukatpally, Hyderabad - 500 085, Telangana, India [1,2]
University College of Engineering, Science & Technology, Hyderabad[2]

devallashivaramakrishna@gmail.com[1], mratnajntu@jntuh.ac.in[2]

***Abstract*— The rise of cloud computing has changed how individuals and organizations store and communicate data, but it additionally caused significant concerns about information security and confidentiality. In order to improve data protection and allow covert communication in cloud environments, this research suggests a unique approach that combines spread spectrum steganography with isogeny-based cryptography as a solution to these problems. The main goal is to make it less difficult for two users, User 1 and User 2, to communicate private data that is kept in a cloud infrastructure through safe and covert data transfer. This technology depends on isogeny-based cryptography, which creates safe channels of communication between users by taking use of the mathematical features of isogenies of elliptic curves. Additionally, this technique provides protection from quantum assaults, consequently boosting data security. Spread Spectrum Steganography (SSIS), the second element, is used to secretly include shared secrets inside digital images. To protect secrets, SSIS encrypts, duplicates, interleaves, and employs pseudorandom noise sequences as carriers. The noise in the stegoimage is then removed with a filter to approximate the original image. By performing this, the stegoimage is made integrate in with the original, thereby hiding the secrets. Users 1 and 2 can safely share information by combining spread spectrum steganography and isogeny-based cryptography, reducing potential risks associated with parties that are unreliable. Spread spectrum steganography provides the covert hiding of transmitted secrets inside digital images, while isogeny-based cryptography provides secure communication channels. These methods are combined to build an effective structure for private and secure data sharing in cloud services. This novel method solves important concerns about data security, secrecy, and covert communication, and thus makes a significant addition to the developing field of cloud computing security.**

Keywords*— *Cloud Computing, Covert Communication, Spread Spectrum Steganography, Isogeny-based Cryptography, Data Security

I. INTRODUCTION

Cloud computing is the means of interacting with distant computer systems in order to retrieve and update stored data with the assistance of any hardware linked to the Internet, including portable hardware. Taking into consideration, the aspect of innovation and improvements that will drastically shift the lives of individuals, a relatively recent invention is the cloud computing [1] [2]. This is because through the application of this technology one can be able to access the computing facilities and resources [3]. The term cloud is another name which people use interchangeably with cloud computing [4]. Cloud computing may be used for a number of purposes through the use of the internet, it may be used for storage. Optimization of resources indicates that through sharing the cloud computing may benefit from reliability and efficiencies of scale. Also, there could not be now a general definition of cloud computing [5] [6]. The following are the five characteristics of cloud computing that were proposed by National Institute of Standards and Technology: On demand self-service, network-accessible resources, resource pooling, rapid provision and elasticity, and service-oriented. Cloud computing has been growing in speed on how it stores information but its safety keeps on being a concern [7].

When data is moved to a cloud-based storing provider, this poses a safety issue since the data owner is not in control of the data anymore. In cloud computing there is a major issue on the security and protection of data that is stored in the cloud. That is the main problem with the cloud; everyone, including intruders and foreign hackers, may easily access unprotected information. Employee at any part of the company have easy access to information whether intentional or accidental [8]. In certain situations, it is possible to achieve unauthorized entry into systems using a number of methods. There is the problem of vulnerability of cloud servers to viruses and malwares. Out of all the methods of information protection cryptography and steganography are the most effective. Some of the challenges that are associated with cloud computing are a major one being the security of the information being transmitted [9].

Any mention of data security must also mention cryptography, which plays a critical role in preventing unauthorized access to information, change or interference of the information and interception of the data. Genuine

cryptographic techniques have emerged as crucial in an increasingly more digital society where data are processed and stored. The study explores the area of security of information by Cryptography, including its basic concepts, methods of encoding, key control and its emerging role in protecting modern technology. In its most elementary form, cryptography is the science and the skill of maintaining secret given information by encoding with the aid of mathematical principles and methods [10] [11] [12]. It works based on number of basic principles such as non-repudiation, authenticity, privacy and integrity [13] [14]. While, there are four basic tenets of computer security and their brief explanation is as follows: The principle of authenticity proves the identity of the originator or the recipient of the information, the principle of confidentiality prevent information from leaking to unknown persons, the principle of integrity prevents information from being altered in transit or even when stored and the principle of non-disclosure prevents persons from refraining their behaviors or financial dealings [15] [16]. Cryptography's baseline is cryptography [17]. It involves for using an encryption algorithm and an encrypted key which makes the plaintext (which is intelligible data) into ciphertext (which is non-interpretable data). Asymmetric key encryption entails one public and private key where the public key is used to encrypt the message while the, private key can be used to decrypt the message Symmetric key encryption entails the use of the same key for both the encryption and decoding processes [18].

The key contributions of the paper are given as follows:

- The proposed hybrid security architecture that utilizes spread spectrum steganography and isogeny-based cryptography combination addresses security and confidentiality issues in cloud computing by enhancing data protection and enabling covert communication.
- In order to create safe communication channels between users, the study makes advantage of the mathematical principles of isogenies between elliptic curves. This cryptographic method makes data transmitted in cloud settings more secure by defending against quantum assaults.
- The study secretly incorporates communicated secrets inside digital images using spread spectrum steganography. The stegoimage has been modified to appear virtually identical to the original by SSIS, offering a high level of privacy for the concealed secrets.
- Even in unreliable conditions, the approach allows User 1 and User 2 to securely communicate data. Isogeny-based cryptography creates safe channels, while spread spectrum steganography makes sure that the shared secrets remain concealed, reducing the risks carried about by unreliable parties.

The rest of the section is organised as shown below. Section 2 illustrates literature works on cloud data security and covert communication. Section 3 gives the Problem Statement. Section 4 covers the proposed technique for Enhanced data protection in cloud infrastructure. Section 5 illustrates the performance measures and gives the outcomes and contrasts the approach's effectiveness to existing approaches. Section 6 provides the conclusion.

II. Related Works

The area of cloud computing is quickly developing. Individuals can utilize it to obtain the capabilities of their computers as required, including data storage and processing strength, without having to manage it. In order to address current safety and confidentiality problems, such as loss of information, Information manipulation, as well as information stealing, the work intends to provide an information safety framework that utilizes both steganography and cryptography for information within cloud computing. In order to determine the problem and ascertain its exact cause, researchers looked into a number of investigations on existing security features of cloud computing principles. The work employs an innovative scientific investigation methodology. The issue recognition, specifications gathering, artifact creation and expansion, demonstrations, and evaluation phases are all included in the conception of the scientific investigation process. The method was developed utilizing the design process and a programming language called Python, and the histogram, tables of data, and procedures were utilized to express arguments about how it operated. The four phases are sharing information, information restoration and backup, steganography, and information encryption for maintaining and securing information. By defending the integrity of information, privacy, and security against intruders, the proposed approach cloud-based information, redundant systems, adaptability, effectiveness, and protection. However, it needs to strengthen the pairing and offer more protection for multimedia information [19].

In the cloud setting, services are shared amongst every server, subscribers, and individuals. Since security is the main problem in handling information and transmission since information in its original format can be obtained, abused, and demolished, internet service providers have trouble to ensure file security [20]. In the context of cloud computing, security in the cloud is a major problem. Numerous research projects are being suggested in order to protect the environment of cloud computing. Cryptography is employed to solve the security problem and attain the CIA feature. Conventional symmetrical and asymmetrical patterns have certain drawbacks. To address this, a novel hybrid approach with high levels of information safety and privacy will be introduced. In the article, a hybrid method is constructed by combining ECC with Blowfish. The suggested technique offers beneficial confidentiality and security of user information when effectiveness of the combined approach is contrasted to the mixed approach currently in use. Mixed cryptography is employed to overcome the disadvantages of both asymmetric and symmetric encryption techniques. However, it has an issue in the Key Distribution Process which can be solved by Steganography.

The most innovative and practical method for organizing and using enormous quantities of information is through the cloud. Maintaining information that is obtained and processed through the internet as opposed to being maintained remotely on a device is the idea behind cloud computing. Cloud computing

can manage a lot of information on request since it executes applications via the internet [21]. Cloud computing makes it simple to utilize internet preservation in the data era, which advances communications and technology. Effective information protection is necessary for cloud computing since it makes every piece of information accessible and enables anything to be operated remotely. It is crucial to remain in mind that a variety of security issues, including those involving information safety, information privacy, integrity of information, as well as information authentication, may occur. Cloud security must be updated and improved regularly in order to address all issues. With the use of cryptography and steganography, information safety has been established and improved. Steganography may be employed to encode information throughout communication, and cryptography may be employed to hide information exchanged from unknown individuals. The most efficient technique for protecting information used in cloud communications is steganography. The most reliable method to conceal information, including images, sounds, and video content, is using steganography. However, employing image information concealing is the optimum and safest way. The most significant secure way of protecting information stored in the cloud is steganography since it manages duplicated information and hides information. The steganography approach is deemed more reliable when Pseudo-Random Numerical Generation is utilized. The steganography approach can be employed with PRNG technology.

In the past few years, information has become essential to all parts of human existence. The last few decades have seen a tremendous increase of information due to the creation of several applications. The innovation that can be utilized for maintaining those enormous volumes of information is cloud computing. The technological advancements' fast evolution renders it even more crucial. Therefore, protecting information from intruders has become crucial in order to maintain its authenticity, privacy, security, confidentiality, and processing processes [22]. In the investigation, an innovative compact cryptographic technique for improving information safety was suggested. The technique may be utilized to protect applications that utilize cloud computing. Sixteen bytes keys is required to encode the information. To increase the level of sophistication of the encryption, it was influenced by feistal and replacement permutation structure approaches. The method uses logical procedures to implement Shannon's concept of confusion and dissemination. The measurement of the secret code and the number of rotations is also adjustable. In comparison to the encryption technologies that are commonly employed in cloud computing environments, the empirical findings of the proposed technique demonstrated a high degree of protection as well as a noticeable increase in measurements of cipher implementation duration and safety measures.

Cloud computing is a cost effective and elastic paradigm for accessing resources for storing and processing data and it brings about several security threats which include data loss, manipulation and theft. For these problems, a novel security model integrating steganography with cryptography is developed as a solution. This framework incorporates both techniques that would help to improve the data protection and privacy within clouds. The steps of the present study included analysing current security measures, proposing a new synergistic cryptographic configuration of the ECC with Blowfish algorithm, and using them with steganography to solve the key distribution issues. The framework is intended to preserve consistency, privacy and security of the data with regard to multiple media types. This approach seeks to enhance safety of data held in cloud computing through employment of sophisticated cryptographic systems and steganography, that could be achieved using conventional techniques.

III. Problem Statement

Due to the rapid growth of the cloud computing industry, many serious issues have been discussed that are related to privacy and security of information in the cloud settings. Such concerns involve questions related to data loss, alteration and deletion. The idea of this work seeks to design a comprehensive information security solution involving both steganography and cryptography to any information in cloud computing to overcome the challenges highlighted above. Since these are the general causes of the problems, existing security strategies in cloud implementation have been primarily studied [23]. While the digital mode the large quantity of information managed and maintained in remotely, the study underlines information safety in the cloud infrastructure as critical importance, to eradicating these security issues that involve solutions of the Isogeny-based Cryptography and Spread Spectrum Steganography.

IV. Isogeny-based Cryptography and Spread Spectrum Steganography

The suggested approach comprises of two fundamental components, namely Isogeny-based Cryptography and Spread Spectrum Steganography which seem to work hand in hand with the aim of protecting and concealing the flow of information from one User in the blockchain, namely User 1 to the other User 2. User 1 and User 2 have to exchange some sensitive data which are stored in the cloud infrastructure. This information has to be accessed from the cloud by User 1 and then passed on securely to User 2. In this component, primarily to ensure secure Users 1 and 2 communications, a third party is not involved, whereas, the isogeny-based cryptography is applied to create such connection. The public-private key pair is generated with the help of isogeny-based cryptography wherein the use of isogenies between elliptic curves is employed mathematically. There is another key which is unique to each user called public key and another unique one which is called private key.

Although the public keys make encryption of data possible, the cryptographic procedures on information can be performed by the users through use of the private keys. The formation of elliptic curves and its corresponding isogeny forms the first step of the process. These are the keys that isogenies work with when encrypting the information. Through sharing of such kind of isogenies, Users 1 and 2 are in a position to establish secure

communicating channels. Every party contributes some of their isogenies data that has to be guaranteed that the information disclosed is valid. The exchange happens sequentially.

The computational complexity of getting the private keys is reduced by leverage on this method's steps and users may also verify information given by the other party without revealing their secrets any further. Still, the isogeny-based encryption strengthens protection of the transmitted data by offering resistance to quantum attacks. That goes to the Steganography after that, and then it receives the encrypted message. The last step is the Spread Spectrum Steganography (SSIS) procedure, which is used for hiding the messages in the completely inoffensive 'sheep' material. In this particular scenario, SSIS helps in the integration of the traded secrets within the constructed digital images. These are the basic steps of the procedure: encodation of secrets, use of error-correcting codes to encode information redundantly and integration of all information in order to get prepared for the actual embedding. Padding provides a way of making sure that the size of the image and the actual message have the same size.

In the next step, the noise sequence is modulated using encoded message such that the secrets is further masked with noise. When the original image and the noise are put together, what is termed as a Steg image is formed. This means that in order to recover the secrets it is not necessary to have the original image at hand. For the preliminary assessment of stego image, a filter is applied on the image to obtain an approximate cross section of the noise content in the image. The extent of accuracy of this approximation depends with the filter that is used; a filter that works well ensures that the secrets are retrieved well. As a result of this procedure, the Steg image is less concealed, making the Steg image to have a perception like the original image. Spread spectrum steganography develops an additional layer of concealment which unmakes possibility for the aggressor to come to the hidden image's information. The two cryptographic techniques known as isogeny-based cryptography and spread spectrum steganography are employed to allow the sharing of secrets of User 1 and User 2 in order to minimize the dangers involved in dealing with the-third parties. Spread spectrum steganography ensures that no one other than the sender and the receiver will ever know that there are secrets being transmitted hidden in digital images while isogeny-based encryption ensures that passageways created for communication are secure. Altogether these methods can provide reliable private and secure way for transferring data between Users 1 and Users 2 in the worst-case scenario. The Block Diagram of Cryptography and Steganography is illustrated in; Figure 1.

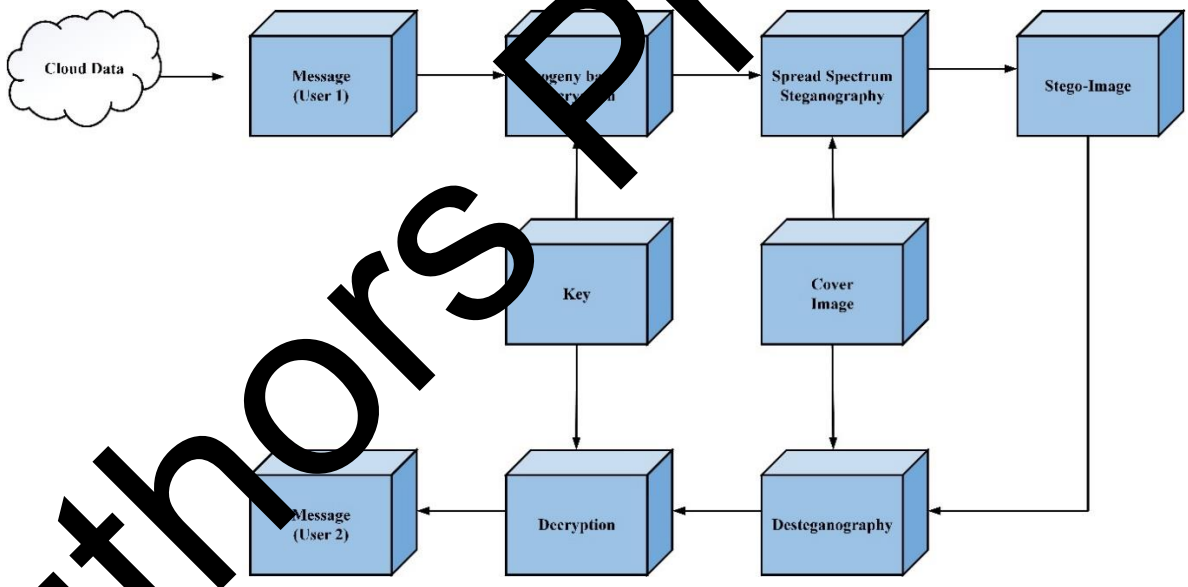


Fig. 1. Block Diagram of Cryptography and Steganography

As for the Users 1 and 2, they become owners of highly significant secret information – encrypted digital assets, private keys [illegible] ving the digital tokens or, in other words, cryptocurrency, secret codes, and key words. Both users require engaging into an information exchange, which is actually swapping of each other's secret information and have to be accessible to a secured digital communication platform. Nevertheless, a certain barrier remains, thanks to which even User 1 and User 2 cannot have a feeling of confidence in the other party at first glance. While User 1 is sharing the information with another User 2 there exists a real threat of the fact that User 2 might cease responding to the communication and ignore the terms of the agreement. The problem of identifying a suitable and credible third party is merely pushed to another layer of the solution: to accomplish the transaction through the services of an experienced and reputable third party.

The following fundamental question shall be addressed in this study; Can Users 1 and 2 engage in this trade independently without the help of a competent third party? This is because User 1 and User 2 want to pass on confidential data that is contained in a cloud architecture. This information has to be accessed from the cloud by User 1 and securely communicate to User 2. Being based on the protocols and possible susceptibilities of the cloud service providers upon which the integrity, confidentiality and availability of the data depend on, the cloud environment poses special security concerns and challenges. Solving these problems, especially if a need to simultaneously ensure safe and reliable exchange of data between Users 1 and 2, is a complex process that demands the development of original and non-traditional approaches based on trust. This paper seeks to examine techniques and Cryptography methods that may enable Users 1 & 2 to securely transfer information through Cloud even in the absence of a trusted third party.

A low road of reasoning is to state that the idea of such a thing cannot be imagined. One argues that any such protocol produces message exchanges between the Users 1 and 2 on the secured digital channel. As the messages seem to appear in a certain order, there might be some initial message from which, for example, User 1 will be able to guess what secret User 2 is sharing. If the User 1 receives this message before giving the User 2 the secret, then the User 1 can just not bother to complete his or her part of the procedure. Same could be emulated by User 2, if the other reveals the secret to the user before the user reveals the same to the other. A protocol which prevents an instance of improper behaving is inconceivable since the communications are ordered and the party unveiling the secret cannot compel the other to reciprocate.

The naïve argument has a problem with the claim that User 1 can descriptively identify that some initial message reveals User 2 ‘s secret. As a matter of fact, in a common example of the situation of a public key and private key pair, both the participants have sufficient information to arrive at the secret that is the private key given the information that is in the public domain that is the public key but they cannot perform the computations required to do so. Therefore, the process of transferring information between Users 1 and 2 can be viewed as the scenario where one party shares some information with the other in order to allow the latter to recover the secret information from the information it has available at its discretion. The following step is to design a process by which Users 1 and 2 can exchange information “bit by bit” so that it can be easier for each of them to calculate the second secret of the other side from the revealed information. If at any point one or the other party decides to abandon the protocol both will be given an equal amount of information regarding the other party’s secret for their secrets will remain safe from the other party due to issues of equal degree of difficulty.

The aforementioned procedure remains vulnerable to the specific counterparty risk that User 2 cannot detect a forged document until User 1 and User 2 complete sufficient rounds of the protocol that User 1 and User 2 would both be able to obtain each other’s secrets if both parties were honest. However, under this scenario, while a malicious User 1 would have been reporting fake information, a genuine User 2 on the other hand, would have been revealing their private information only to be eaten by the vicious User 1. Hence, for User 1 and User 2, there should be a technique through which both users are not only able to convey part knowledge about their secrets but also be able to prove the truth regarding the partial information transmitted without reveal any more information about their secret. From the study, it is found that the exchange of such a secret can be done by using isogeny-based strategies.

A. Isogeny-based Cryptography

Modern cryptography uses isogeny-based encryption; it means that the protection of data security takes advantage of some properties of isogenies between elliptic curves. This type of encryption has recently gained more popularity due to the threats that arise from quantum computing and since it provides high level of data protection. Data is encrypted through isogenous transformations in the manner that is extremely difficult to crack for the third party, including even the most advanced quantum computers. In the modern world where there is rising concern in the protection of information, this makes it an attractive option in the protection of such information. Elliptic curve isogeny captures the concept a relation between two elliptic curves that preserves certain algebraic properties, which form the underlying of isogeny based cryptography. However, for the quantum computers, this encryption method relies on the level of difficulty of Random Ella Isogeny Search among the random elliptic curves. In the addition, by the employment of isogenies, the security and the confidentiality of the information that is encoded is ensured.

This basic mathematical concept forms the foundation to make operations of key creation and decryption and encryption. In particular, it is crucial to note that isogeny-based encryption is rather resistant to quantum attacks. Classical ciphertext algorithms such as RSA and ECC are susceptible to quantum solutions which are capable of factoring large numbers using algorithms such as Shor’s algorithm. However, isogeny-based encryption may be one of the potential solutions to the long-term protection of information since its challenges are expected to be quantum-resistant. This kind of encryption also results in efficient and compact cryptographic procedure, suitable to environments with substantial computing constraints such as cloud computing and IoT.

Suppose that H is the sum of D points which are elements of the subgroup of D provided some operations addition. We denote the set D as an elliptic curve. Then, if D and D/H given in Weierstrass formulas in the coordinates (u,v) and (u ’,v ’) respectively, then the map ϕ transform into the form of Equation (1). This allows for the construction of a different elliptic curve, which the research labels D/H, and a surjective map ϕ:That is, D→D/H which is a group homomorphism or a mathematics map.

$$(u', v') = \phi(u, v) = \left(\frac{\psi_{u'}(u,v)}{\eta_{u'}(u,v)}, \frac{\psi_{v'}(u,v)}{\eta_{v'}(u,v)}\right) \quad (1)$$

For polynomials in u and v, ψ_(u^’), η_(u^’),ψ_(v^’), and η_(v^’). The degree of the mapϕ, which is the same for the

functions of rationality that define it, is given by the dimensions |H| of the corresponding sub-group H The kernel of the function map ϕ is in fact the group H The key focus of isogeny based cryptography is however the map often referred to as an isogeny.

Knowing the subgroup H it is possible to define how the elliptic curve D/H and mapϕ has to be calculated. In fact, there are equations which do this for the primary case and the case of interest is when H is cyclic. Thus the assertion that the pair (D/H,ϕ) satisfies a so called "first isomorphism" property follows. If (D^',ϕ^') is an additional pair such that ϕ^':If ϕ:D→D^' is an isogeny with kernel G, there exists an isomorphism α:D^' → D/H such that ϕ=α ∘ ϕ^' is valid. As it has often been the case that the various isogeny-based protocols require the isomorphic curves to be agreed upon by constructing two separate isogenies using the same kernels, this trait is rather important.

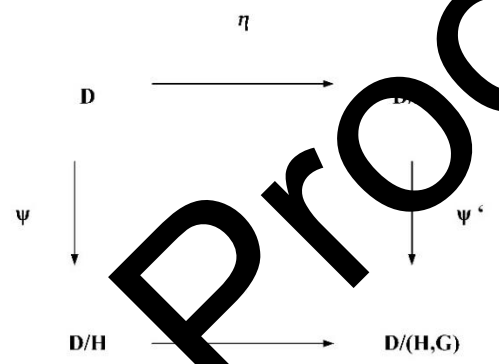
It generally is exceedingly challenging to create an isogeny: Where D is an elliptic curve and D' is another elliptic curve then the notation used is D→D^'. Moreover, if some other details, and the degrees of the isogeny φ, are given, one may often ensure that there is only one possible isogeny. In the context of this, isogenies instinctively fit the function of private and public key pairs in cryptography: the public key is the very pair(D,D^'), it may contain several different data based on the procedures of interest, and the private key is the isogeny φ. However, computing the map: ϕ:D→D/H for the subgroup H i not always simple. The issue is that the degree has to be exponentially large for there to be an exponential searching space to allow for identifying challenging for the attacker. But if the degree of ϕ is exponentially important, then the rational functions that define it are also exponentially large, which complicates working with it and evaluating.

The following approach would probably be applied to rectify this problem. Choose a prime q = m ± 1 of the forms^e where s is a negligible prime and e is an exponential getting an exponential value of se. n is a positive composite number with a lot of small divisors. It is convenient to attach to it a code number of the form F_(q^2). It is the elliptic curve of elliptic curves for each isomorphism class of curve the presence of F_(q^2) points satisfies the given relationship D (F_(q^2)) ≅ (K/nK). This specifically means that there is exponential number of distinct subgroups of order s^e which is generated over the F_(q^2). Should H be such cyclic subgroup produced by Q, then it will follow that H has chain of subgroups.

$$(O_D) \subset (|s^{e-1}|Q) \subset (|s^{e-2}|Q) \subset \cdots \subset \langle |s|Q \rangle \subset \langle Q \rangle = H \quad (2)$$

For instance, let where, O_D is a position on D that is infinitely distant from it. With the curves D_0=D and D_e=D/H and the kernel of ϕ_i:To be specific, D_(i-1)→D_i set to be the representation of the group (|s^(e-i) |Q) under the map ϕ_(i-1)…∘ϕ_1, the study can then arrive at the map, ϕ:D→D/H of degree 'e' as a sequence of isogenies. The whole isogeny ϕ may be described in such a manner since every map ϕ is of a low degree.

Using the protocols, an isogeny ϕ:D→D/H may protect anything, including the symmetrical cipher's private keys, encrypted data, or anything that is protected by signatures. To implement the trading mechanism, hence, it is sufficient to demonstrate how to expose ϕ:D→D/H "one phase at a duration" in a way that each phase can be corroborated by a static exposition. The method that comes out most clearly is to unveil the maps ϕ_1,ϕ_2, etc as they are in turn.



Where, G is a subdivision of order (being a small prime relative to the high exponent), and & are isogenies of degree &. Where each is an isogeny connected to G of a degree relatively co. The prover then proves knowledge of the curves D/G and D/(H, depending on the bit delivered by the challenger, either or the maps has to be provided by the prover. An interactive proof may be converted to a non-interactive one with the help of a technique named as Fiat-Shamir transform. Specifically, if the study chooses η =, it will be possible to provide the existence of the isogeny satisfying for the purpose of confirming the truthfulness of the revealed map.

1) Steps involved in Isogeny-based Cryptography: The Working of the Isogeny-based Cryptography is depicted in the following manner:

a) Step 1: Generate Isogeny Keys: The first step in the procedure which follows is the generation of elliptic curves and isogenies for user 1 and user 2. Thus, the need to use these elliptic curves and isogenies in performing the cryptographic operations. Using the feature called "Generate Elliptic Curves and Isogenies", User1 and User2 generate User1 Elliptic Curve, User2 Elliptic Curve, User1 Isogeny and User2 Isogeny.

b) Step 2: Share Isogeny Information: Then User1 and User2 exchange information about their respective isogenies after the elliptic curve and isogenies have been generated. The info relating to isogeny of User1 provides User2 with specific information about User1 Isogeny. As with the case of User1, User2 lets User1 know of the isogeny that exists between them, User2Isogeny. Many of the interactions described in the present research are the first steps towards safe communication through the exchange of information about isogeny.

c) Step 3: Establish Secure Communication: Establish Secure Communication: Another reason is that isogeny information is exchanged, and User1 and User2 are able to build secure communication channels. The formation of the secure channel is begun by User1 by way of User2 isogeny

(User2 Isogeny). Contrary to it User2 comes up with a secure channel employing the isogeny of User1 which is referred to as User1 Isogeny. These secure channels help in the transfer of information from the sources such as User1 to the target destination such as User2.

B. Spread Spectrum Steganography

Spread-spectrum communication is the method of slicing a narrowband signal's bandwidth over a large range of frequencies. For that to happen, the narrowband waveform could be modulated with a wide band waveform example being white noise. Spreading weakens the actual power in the narrowband signal in the scenario making it difficult to single out in any particular frequency bands. In particular, this method is used by SSIS to hide something, most often a binary signal, behind very sparse white Gaussian noise. It is also quite impossible to make the user to come to identify the difference between the first image and the Stegimage as a result Steganogram Generator outlined in the diagram below in Fig. 2.

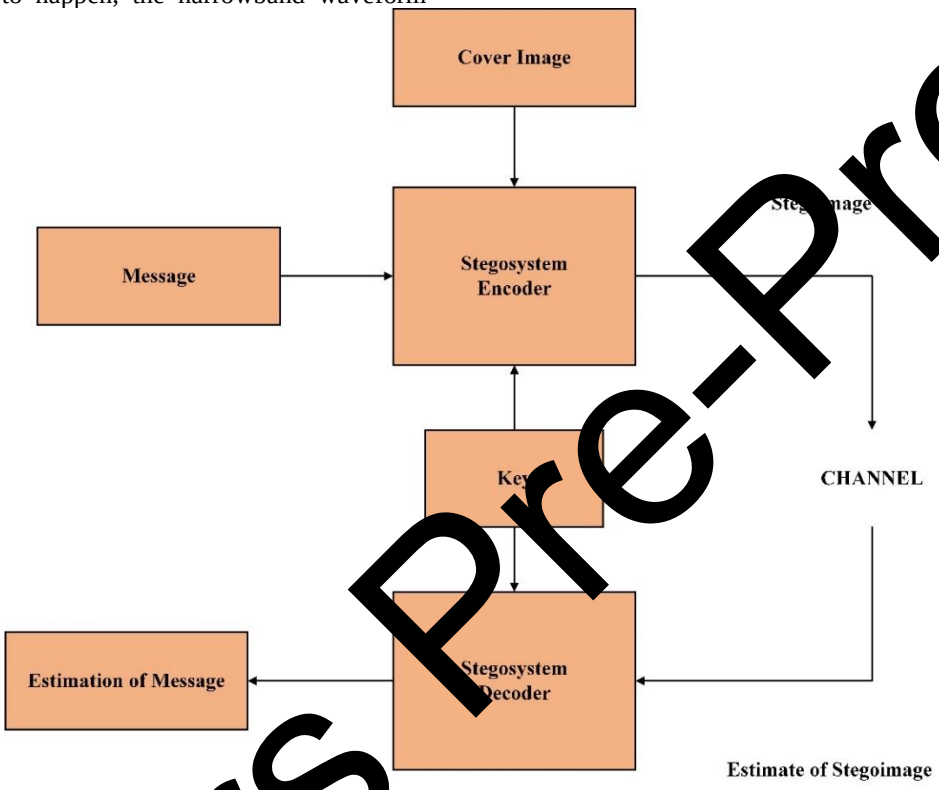


Fig. 2. Steganogram Generator

It may not be possible to provide all information since concealing the information is done by placing messages in other, seemingly meaningless documents is known as steganography. Privacy techniques are usually implemented in cooperation with encryption methods yet steganography is used more often. What's more, even if the encrypted document has been opened and somehow accessed, the concealed message will not be seen and steganography is still practical to be employed to embed information into a file that is encrypted. Steganography techniques could be used to bring attacks into the network, to enable data theft or for provision of secure and concealed data exchange between two parties. These methods are intended to cover the passage of sensitive information (Steganogram) such as those belonging to the user communications that seem normal. In the very best of the world, third parties should not be in a position to decipher secret passing of information. In fact most of the electronic document formats can be used for steganography but the ones containing much redundancy are optimal. When one or more portions of an element are duplicated, then these portions serve precision beyond the needed for the use and display of the element. Two similar elements refer to the fact that alteration of some element is possible and the change will be immediately noticeable. Research also shows other file formats that may be used to conceal the data; these are imagine and particularly audio recordings meet this condition.

Spread Spectrum image Steganogy embeds a message in an image in a way that appears to be as random as noise, for instance random Gaussian noise. The image quality degrades to a level undetectable to the human eyes especially at low noise power however it becomes noticeable at higher noise power or in form of "snow" or speckles. The procedure has been classified into the following steps as explained below.

- By including redundancy through error-correcting coding, encode messages.
- To assure that the encoded message's size match that of the image, include padding.
- The message must be interspersed.
- Make a pseudo-random noise sequence of length.

- Modulate the sequence by using the encoded message to produce noise.
- Add the noise to the original image.

It should be pointed here that it is not required to recover the initial image in the process. A low-quality image of the original image is generated when filter functionality eliminates noise from the stegoimage. The number of mistakes arising from the retrieved message depends with how well this filter works.

1) Steps involved in Spread Spectrum Steganography: The procedure involved in the Spread Spectrum Steganography is described in the following manner:

a) Step 1: Encode a Message into an Image: The first step in the procedure is to encode a message in an image. What can be regarded as input offering is the following message. To enhance reliability of the message, it is initially encoded with error – correcting codes. This means that the encoded message is padded so that they both are of the same size as the cover image. In order to eliminate the pattern that the concealed message was made from, the data in the padded message is interlaced. The created pseudorandom noise sequence will be used to embed the message within the image. The intersecting message, the initial cover image and the noise sequence are encoded to create the stego image which encases the message in the cover picture. The last step results in the extraction of the stegoimage or the original image totally different from the host image.

b) Step 2: Decode a Message from a Stegoimage: Decode a Message from a Stegoimage: Stegoimage is the data that is used as the input in the decoding procedure. When retrieving the encoded information, the stegoimage noise should be reduced as shown in the next section. Extracting the original message from the filtered image is done by applying some function deinterleave and decode. Thus the previously decoded message is given out as the result or consequence of the procedure.

c) Step 3: Main Execution: The subsequent steps perform in the primary execution section They are fundamental Cover Image: the loaded cover image serves as a foundation in which the secret message is concealed into. In this case "Secret message" is the message to be hidden. The messages are written on the cover image through the Encode Message function which results into stego image. After blurring, the stegoimage is used on the Decode Message function in order to extract the secret message. The intended recipient can then look at the message which has been retrieved and then wade through the coded message.

Algorithm 1: Pseudocode for Combined Isogeny-based Cryptography and Spread Spectrum Steganography

The methodology's main phases are outlined in the pseudocode given below, starting with the creation of isogeny-based encryption keys and continuing with secure communication and the Spread Spectrum Steganography technique for encoding and decoding hidden messages within digital images.

```
// Isogeny-based Cryptography
Function Generate Isogeny Keys ():
        // Generate elliptic curves and isogenies
        User1EllipticCurve, User2EllipticCurve,
User1Isogeny, User2Isogeny = Generate Elliptic Curves And
Isogenies ()
        // Share information about isogenies
        User1 Shares Isogeny Information (User1Isogeny)
        User2 Shares Isogeny Information (User2Isogeny)
Function Secure Communication ():
        // Establish secure communication channels
        User1 Establishes Channel (User2Isogeny)
        User2 Establishes Channel (User1Isogeny)
// Spread Spectrum Steganography
Function Encode Message (message, coverImage):
        // Encode the message with error-correcting codes
        encoded message = Encode with Error Correction
(message)
        // Add padding to match image size
        padded message = Add Padding (encoded message,
coverImage)
        // Interleave the data
        interleaved message = Interleave Data (padded
message)
        // Generate pseudorandom noise sequence
        Noise sequence = Generate Pseudo Random Noise ()
        // Modulate the noise with the encoded message
        stegoimage = Modulate Noise(coverImage, interleaved
Message, noise Sequence)
        return stegoimage
Function Decode Message (stegoimage):
        // Remove noise from the stegoimage
        filtered Image = Remove Noise (stegoimage)
        // Deinterleave and decode the message
        decoded Message = Deinterleave and Decode (filtered
Image)
        Return decoded message
// Main Execution
Generate Isogeny Keys ()
Secure Communication ()
Message to Hide = "Secret message"
coverImage = Load CoverImage ()
        // Embed the message into the cover image
        stegoimage = Encode Message (Message to Hide,
coverImage)
        // Extract the hidden message from the stegoimage
        extracted Message = Decode Message (stegoimage)
Print ("Extracted message: " + extracted Message)
```

V. Result and Discussion

In this approach, Users 1 and 2 aimed at sharing of private information stored in cloud without third party intervention. They accomplish this using two main techniques: First, they generate a pair of public and private keys by using the isogeny-based cryptography. They can therefore securely encrypt and or process their data through these keys. The existence of mathematics in the encryption design with the isogeny, ensures the security, not even in the case of quantum attacks. Second, to encode their secrets and then embed these secrets in digital images, they employ Spread Spectrum Steganography (SSIS). The SSIS works on the data that is to be embedded in images for purposes of encoding including redundancy and interleaving. Since the secrets are incorporated into a noise sequence into the message, the steganalysis image produced looks indistinguishable from the original. For User 1 and User

2, this combination of isogeny-based cryptography and SSIS provides a strong base of a secure communication in untrusted environment.

A. Peak Signal to Noise Ratio (PSNR)

PSNR assesses the steganographic image's quality value, which is expressed in decibels (dB).It is expressed in Equation (3).

$$\text{PSNR} = 10log_{10}(\frac{255^2}{MSE}) \quad (3)$$

Where, MSE stands for mean square error. The image quality is improved by a higher PSNR value.

TABLE I. PSNR COMPARISON OF PROPOSED METHOD WITH OTHER EXISTING APPROACHES

Algorithm	PSNR
RSA	40
AES	74
ECC	63
Proposed Method	92

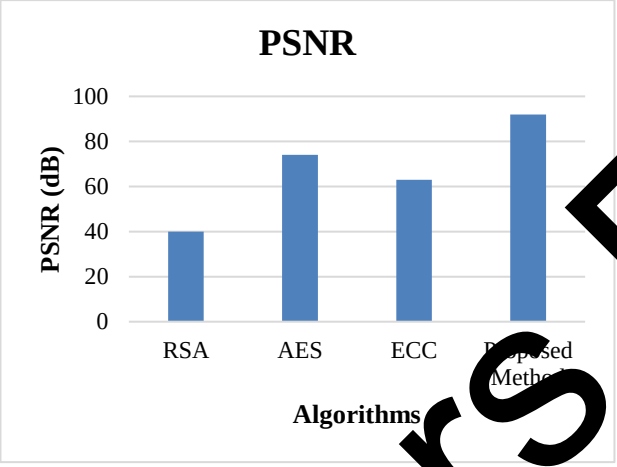


Fig. 3. PSNR Comparison of Proposed Method with Other Existing Approaches

The PSNR values of the proposed approach have been compared with the three other encryption methods RSA, AES and Elliptical curve cryptography (ECC) and the results are summarized in Table 1 and depicted in Figure 3. Larger values of PSNR which is used while measuring efficiency of image encryption signify better image quality. The proposed method provides a very high PSNR value of 92 which proves that image is well retained during the encryption phase as depicted in table. The percentage signal to noise ratio for other algorithms likes RSA is 40, AES is 74 while ECC is 63 a significantly lower value. This demonstrates that the suggested approach is far more effective in maintaining the image's quality and ensuring sufficient encryption compared to traditional methods localized in traditional linear combinations or weighted mean calculations methods while ensuring information safety and image quality, showing applicability for the secure image transfer or storage in cloud applications.

B. Structural Similarity Index (SSI)

The initial image and the Steg image are compared using the structural similarity index parameter. It is given in Equation (4).

$$SSI\ (u, v) = \frac{(2\mu_u\mu_v+d_1)(2\sigma_{uv}+d_2)}{(\mu_u^2+\mu_v^2+d_1)(\sigma_u^2+\sigma_v^2+d_2)} \quad (4)$$

TABLE II. SSI COMPARISON OF PROPOSED APPROACH WITH OTHER EXISTING APPROACHES

Algorithm	SSI
RSA	0.6
AES	0.8
ECC	0.4
Proposed Method	1

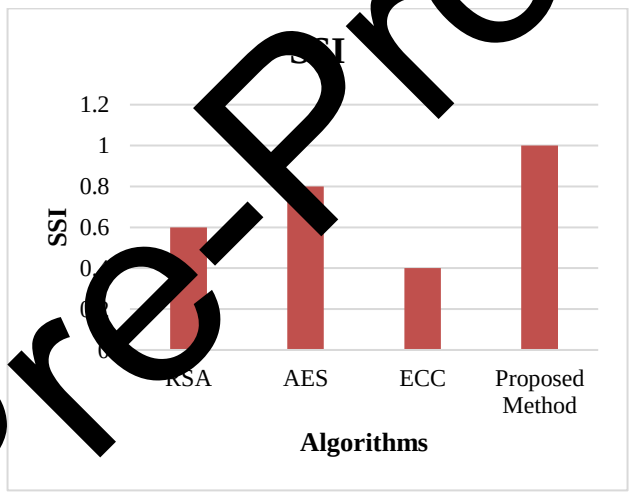


Fig. 4. SSI Comparison of Proposed Method with Other Existing Approaches

The proposed work SSI values of suggested encryption method represent by table 2 and figure 4; RSA, AES and ECC encryption. Values of SSI measure closer to 1 testifies to the higher performance of the steganographic approach of hiding the hidden information in the digital images. From the table derived from the result, the suggested technique has a large SSI of 1 indicating that the information hiding inside image is excellent. By using some of these other methods such as the RSA which has an SSI of 0, the SSI levels of the other methods are presented below. 6, AES with 0. 8 and ECC with 0. 4, are significantly lower. That is why the suggested approach is very good at hiding data into images and can be considered as the reliable tool for applications which require covert communication and data concealment including secret transmission of messages and steganographic applications in insecure environments.

C. Encryption and Decryption Time

The encryption and decryption timings of the proposed algorithm and three other encryption algorithms RSA, DES, AES are compared in Table III and figure 5. The time required to encrypt a specific set of data is described as encryption time in terms of time in seconds while the time taken to decrypt the same set of data is described as decryption time [24]. From the table it is seen that the suggested technique outperforms the

current algorithms by a far better encryption time. The RSA algorithm takes the longest time to encrypt data in comparison to the other algorithms with a procedure duration of 2. 133ms while the DES and AES algorithms also have small variation in their procedure duration of 0. Thus, the proposed approach looks fabulous and powerfully effective, devoting, moreover, exclusively 0. 516 seconds for encryption. This has demonstrated that the suggested method is indeed very efficient at protecting data through encryption and as such suitable for situations where instant encryption is vital ideal for instance real data protection, secure communication. The suggested approach also provides tremendous time effectiveness in decryption phase, which takes only 0. 513 seconds. However, the decryption times of the RSA and DES algorithms are comparatively much more and which is 2. 098 and 1. 123 seconds, respectively, while the decryption time for AES is similarly longer that is 1. 110 seconds.

TABLE III. COMPARISON OF ENCRYPTION AND DECRYPTION TIME OF THE SUGGESTED ALGORITHM WITH EXISTING ALGORITHMS

Algorithm	Encryption Time (sec)	Decryption Time (sec)
RSA	2.133	2.098
DES	1.706	1.123
AES	1.140	1.110
Proposed Method	0.516	0.513

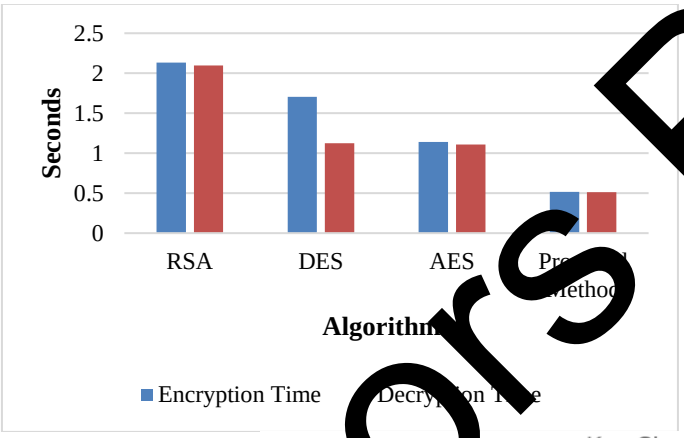


Fig. 5. Comparison of Encryption and Decryption time of the Suggested Algorithm with Existing Algorithms

D. *Key Size vs Security Level*

A performance comparison of core sizes of RSA, ECC and Isogeny-based cryptography at various levels of security reveals fundamental differences in efficacy and scalability. From the data derived from the research, RSA is seen to need significantly bigger key size to offer comparable securityComparing the three mentioned technologies; ECC, Isogeny-based, and RSA, the latter is revealed to perform significantly poor in terms of security level key size. For example, at the security level of 80 bits the RSA algorithm operates with a 1024 bit key, the ECC with only 160 bit key and the Isogeny-based cryptography with 268 bits. Continuing this trend, as the security level increases for 256-bit of security level, RSA needs 15360 bit key, whereas ECC need only 521bits and Isogeny-based cryptography just 832 bits. It has been proved that ECC is more efficient than RSA, however Isogeny-based cryptography is the post-quantum cryptographic solution with the smallest key sizes and also being quantum resistant. With growing threats from quantum computers, classical cryptography such as RSA and ECC face vulnerabilities, Isogeny-based cryptography proves that it is secure with small key sizes while planning for the future of cloud computing. Isogeny-based methods are more bandwidth-efficient since the key size is significantly smaller in cloud environment, where storage, processing speed, and efficient bandwidth is a major concern, without any compromise in the security. These results highlight the need to both address classical S-KA and explore use of post-quantum-safe algorithms hence Isogeny-based cryptography as a potentially reliable solution for ensuring effective and secure communication and data protection in the future. It is depicted in Fig 6.

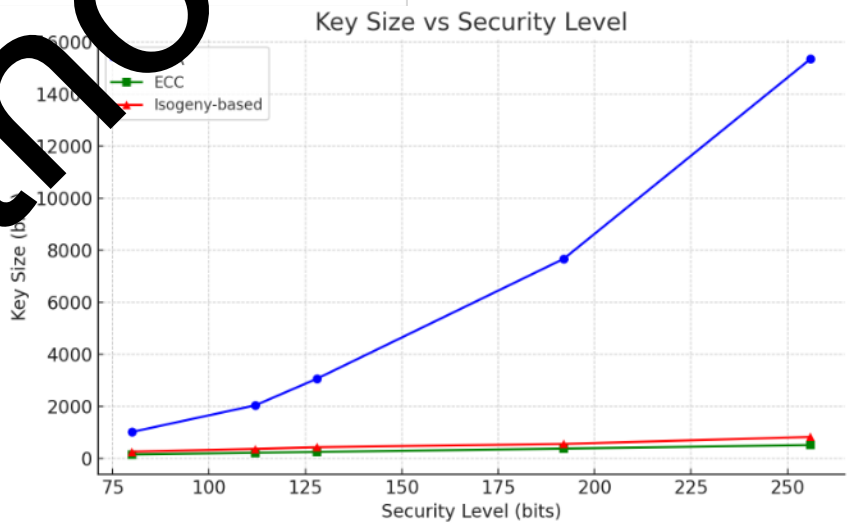


Fig. 6. Key Size vs Security Level

E. Latency in Data Transmission

Transmission delay is therefore the amount of time it takes for data to be transmitted across a network from one point to the second. This delay is normally in milliseconds and is depended on distance from source to the destination, speed of the network, type of communication protocol used and the time taken by the network to encrypt or compress the data. Latency is a very important indicator in evaluating and quantifying the efficiency and response time of different networks in an application where the processed data need to be delivered in real-time for instance in video streaming, online gaming solutions, cloud solutions, and IoT systems. For instance, cloud applications require a low latency because end-users and servers are in different geographical locations and data transmission needs to occur at a high speed. Latency depends on the extra mechanisms that are put in place in a network to ensure security; example, encryption or other defenses mechanisms may take time to work. Latency should therefore be kept to a minimum because delays, delay variation, or interruptions of service can be detrimental to appropriate communication. Consequently, the reduction of data transmission latency is a significant factor that should be considered in the cases where real-time data transfer is needed, and the high-speed and highly reliable networks are essential in modern and constantly developing cloud technologies and cybersecurity systems. It is depicted in Fig 7.

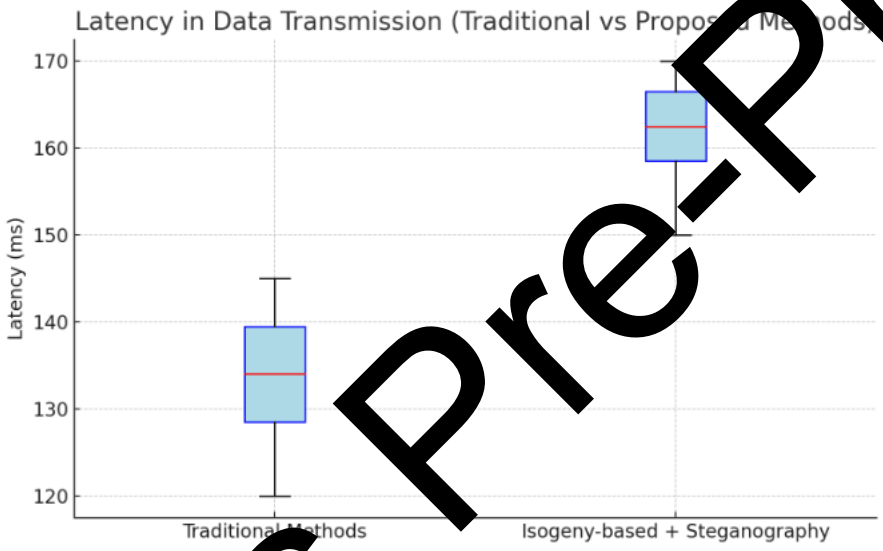


Fig. 7. Latency in Data Transmission

F. Cloud Security Efficiency

Cloud security efficiency means how effective the cloud infrastructure is safeguarding data, preserving confidentiality, enforcing the integrity of data, not allowing unauthorized access, and preventing Cyber-attacks alongside with its capability to perform and consume the resources optimally. Optimum cloud security entails the use of longer and harder keys for encryption, strong passwords for authentication and integrated monitoring solutions for control of any breach or unauthorized access and usage of cloud data. Data security involves data privacy; data integrity and cloud system's ability to resist data attacks including DDoS attacks and hacking. Another important parameter is clandestine communication effectiveness where steganographic means can be incorporated to effect hidden messages transfers without arising and getting caught again making security stronger. However, where security is an issue, the cost of the overhead in terms of implementation viz the protective measures that have to be put in place, viz; encryption and user authorization controls is that it has to translate into a higher transmission overhead which is the amount of processing that has to go on before the data is transmitted from one point to another. The optimum cloud security efficiency, therefore, needs to address the strength of security measures against the impact on the system's speed, scalability, and usability, where stronger mechanisms compromise the protection of data or the volume and processing flexibility in the cloud environment that work with large data traffic and complex workloads. Effective cloud security hence aims at delivering high data protection without much bogging the network performance and or adding considerable processing burden. It is depicted in Fig 8.

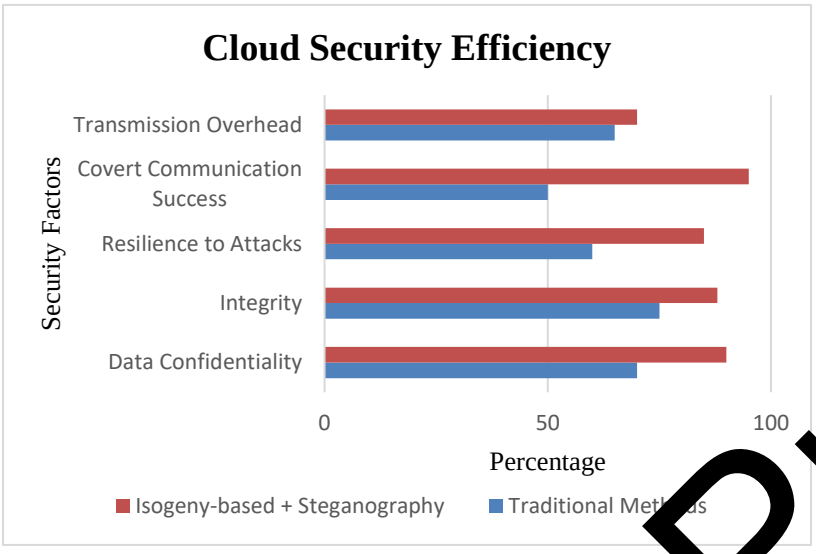


Fig. 7. Cloud Security Efficiency

VI. CONCLUSION

Consequently, this research has offered a novel and efficient approach toward enhancing the data privacy and achieving the covert communication in cloud environments. The suggested approach gives the correct handle towards the insecure data shield and secrecy along with sharing of secure information in the cloud through integration of isogeny-based cryptography and spread spectrum steganography for instant issues prevailing in present days. The technology improves security of the data with resilience against quantum attacks through development of secure connection between users using isogeny cryptography. Spread spectrum steganography also helps in the keeping of information hidden within digital images, making the process even more secure. The results have demonstrated that the proposed method has high efficiency in terms of low encryption and decryption time, high PSNR and SSI values that refer to outstanding image preserving and excellent information hiding. Besides, showing the concept of the Rosetta Stone with respect to safe data transmission, this work also reveals how it can be applied to cloud computing, which elucidates that, apart from data security, the task demands effective data transfer. The proposed technique enhances security and feasibly provides a hidden channel to share information and so, the proposed technique can revolutionize the current Cloud environment in handling and transferring sensitive information. The outlined strategy can be considered as an optimistic start towards enacting on the shift in concerns of security and privacy of data and information in a more connected world and with increased reliance on data in the cloud. Subsequent research may examine at how it can be implemented and generalized to address numerous cloud-based apps and safe data-sharing scenarios.

REFERENCES

[1] G. Chisoni and G. Selvam, "The Design and Implementation of a Secure File Storage on the Cloud using Hybrid Cryptography".

[2] M. S. Maulana, S. R. Widianto, and A. Sasongko, "Steganography based on the B217AN Algorithm for secret messages on flip horizontal and resize image," 2023.

[3] A. Dave and S. S. Rajpe[illegible], "Evaluating the Efficacy and Security of Steganography Techniques in Cloud Computing," *Scand. J. Inf. Syst.*, vol. 35, no. 3, pp. 38[illegible]89, 2023.

[4] A. Prake[illegible] and [illegible] Chauhan, "Exploring Innovative Methods for Enhancing Data Security in Computing," in *2023 3rd International Conference on Smart Data Intelligence (ICSMDI)*, IEEE, 2023, pp. 63–68.

[5] S. Ku[illegible] P. S[illegible]daresan, R. Logith, and N. Mathivanan, "A Data Security-based Efficient Compression and Encryption for Cloud Computing," in *2023 7th International Conference on Trends in Electronics and Informatics (ICOEI)*, IEEE, 2023, pp. 647–653.

[6] V. K[illegible]shnamaneni and S. Premkumar, "Enhancing security in public cloud using novel cryptography and enhanced steganography with E-Lsb encoding comparing with traditional steganography," in *AIP Conference Proceedings*, AIP Publishing, 2023.

[7] M. K. Abdul-Hussein and H. T. ALRikabi, "Secured Transfer and Storage Image Data for Cloud Communications.," *Int. J. Online Biomed. Eng.*, vol. 19, no. 6, 2023.

[8] A. D. Prathyusha, D. Lavanya, V. S. Sreeram, S. V. Narayana, and V. N. Singh, "Image Data Security in Cloud by using Steganography," in *2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN)*, IEEE, 2023, pp. 344–347.

[9] P. Chatterjee, R. Bose, S. Banerjee, and S. Roy, "Enhancing Data Security of Cloud Based LMS," *Wirel. Pers. Commun.*, vol. 130, no. 2, pp. 1123–1139, 2023.

[10] M. F. Roshan, J. Jenish, and P. MercyAssociate, "SECURE FILE STORAGE ON CLOUD USING HYBRID CRYPTOGRAPHY".

[11] M. C. Ghanem, M. D. Uribarri, I. I. Araujo, and R. Djemai, "The Automation of the Extraction of Evidence masked by Steganographic Techniques in WAV and MP3 Audio Files," *ArXiv Prepr. ArXiv230707293*, 2023.

[12] A. Salim, K. A. Mohammed, F. M. Jasem, and A. M. Sagheer, "Image Steganography Technique based on Lorenz Chaotic System and Bloom Filter," *Int. J. Comput. Digit. Syst.*, vol. 14, no. 1, pp. 1–xx, 2023.

[13] P. Arockia Mary, A. Albert Raja, S. Anbarasan, and R. Arivazhagan, "MULTI SECRET SHARING: AN EFFICIENT DATA HIDING WITH ENCRYPTED SECRET SHARING FOR SECURE COMMUNICATION".

[14] A. Gera and V. Vyas, "Securing Data using Audio Steganography for the Internet of Things," *EAI Endorsed Trans. Smart Cities*, vol. 6, no. 4, 2023.

[15] V. A., M. Naved, A. Fakih, Dr. A. N. Venkatesh, P. Vijayakumar, and P. Kshirsagar, *Supervise the data security and performance in cloud using artificial intelligence*, vol. 2393. 2022. doi: 10.1063/5.0074225.

[16] Z. Chen, A. Wu, Y. Li, Q. Xing, and S. Geng, "Blockchain-Enabled Public Key Encryption with Multi-Keyword Search in Cloud

Computing," *Secur. Commun. Netw.*, vol. 2021, pp. 1–11, Jan. 2021, doi: 10.1155/2021/6619689.

[17] I. Haverkamp and D. K. Sarmah, "Evaluating the Merits and Constraints of Cryptography-Steganography Fusion: A Systematic Analysis," 2023.

[18] A. M. Soomro, A. B. Naeem, S. K. Debnath, S. Bagchi, S. Gupta, and K. Saluja, "Private Cloud Hybrid Architecture for Protected Data Communication," in *2023 International Conference on Advancement in Computation & Computer Technologies (InCACCT)*, IEEE, 2023, pp. 450–455.

[19] R. Adee and H. Mouratidis, "A dynamic four-step data security model for data in cloud computing based on cryptography and steganography," *Sensors*, vol. 22, no. 3, p. 1109, 2022.

[20] C. Ponnusamy, S. Padmavathi, and R. Swathy, "Efficient Data Security Using Hybrid Cryptography on Cloud Computing," 2020, pp. 537–547. doi: 10.1007/978-981-15-7345-3_46.

[21] P. R. Kumar, "Cloud Data Security Improvement Using Steganography by Pseudo Random Number Generation (PRNG)".

[22] F. Thabit, A. P. S. Alhomdy, A. H. A. Al-Ahdal, and P. D. S. Jagtap, "A new lightweight cryptographic algorithm for enhancing data security in cloud computing," *Glob. Transit. Proc.*, vol. 2, no. 1, pp. 91–99, Jun. 2021, doi: 10.1016/j.gltp.2021.01.013.

[23] D. Bi, S. Kadry, and P. M. Kumar, "Internet of things assisted public security management platform for urban transportation using hybridised cryptographic-integrated steganography," *IET Intell. Transp. Syst.*, vol. 14, no. 11, pp. 1497–1506, 2020.

[24] S. Mandal and S. Bhattacharyya, "Secret data sharing in cloud environment using steganography and encryption using RSA," in 2015 *International Conference on Green Computing and Internet of Things (ICGCIoT)*, Greater Noida, Delhi, India: IEEE, Oct. 2015, pp. 1469–1474. doi: 10.1109/ICGCIoT.2015.7380699.