Journal of Theoretical and Applied Information Technology
31st March 2023. Vol.101. No 6

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A HYBRID RANDOM IMAGE GENERATION STRATEGY (HR-IGS) FOR SECURING PLAIN TEXT DATA IN NETWORKS

SUSHREE BIBHUPRADA B. PRIYADARSHINI [1, *] ,SMITA RATH[1,*], SUSHREE M. PATEL[2], AMLAN UDGATA [3] ,APARNA MOHANTA[4], S. RIZWAN ALI[5] ,SANGRAM PANIGRAHI[6] ,PRABHAT SAHU[7]

[1, 1, *, 6, 7,]Assistant Professor, Siksha 'O' Anusandhan Deemed to be University, Computer Science & Information Technology, India

[2,3,4,5]Student, Siksha 'O' Anusandhan Deemed to be University, Computer Science & Information Technology, India

E-mail: [1,*]bimalabibhuprada@gmail.com, [1,*]smitarath@soa.ac.in, [2]manasipatel1121@gmail.com, [3]amlanudgata.official@gmail.com,[4]mohantaaps@gmail.com, [5]aliriz1999@gmail.com

[6]sangrampanigrahi@soa.ac.in, [7]prabhatsahu@soa.ac.in

Corresponding Authors: Sushree Bibhuprada B. Priyadarshini, bimalabibhuprada@gmail.com

,Smita Rath, smitarath@soa.ac.in,

ABSTRACT

The rapid proliferation of information highways has resulted in an explosion of issues on the internet. The greater the amount of data transfers, higher is the number of cyber-attacks like man-in-the-middle, hacking, and so on. In such context, cryptography is the study of secure communication mechanisms that encrypt and decode messages using two separate keys, public and private. Our paper focuses on encrypting and decrypting text using a revolutionary hybrid technique that uses Rivest-Shamir- Adleman (RSA) and DH to ensure security in data transmission. Our suggested method uses a random picture generation process to generate largest prime numbers, which improves the security and dependability of data sent from the concerned sender to the receiver. We have used the RSA Algorithm to extract the prime numbers using XOR function from the corresponding two vectors in each row and column of the scanned picture. Moreover, with the help of DH algorithm we are generating secret keys. Then the encryption and decryption phenomenon is carried on. The main goal here is to enhance the execution time, minimize the image generation time, improving key generation time, while conjointly hiking the avalanche effect, that assert the lower the risk of being hacked in case of proposed scheme. The outcomes of the investigation support the efficacy of our proffered approach over other existing approaches.

Keywords: *Cryptography, Encryption, Decryption, RSA, Random Image generation, Public Key, Private Key, XOR-Operation, Asymmetric method.*

1. INTRODUCTION

In current digital world, data security is posing as a crucial challenge to the researchers and scientists as a result of intensified penetration assaults spawned due to the unauthorized users at the time of data communication [1,2]. In this connection, the major motto is that data should not be disclosed to or exposed to any unauthorized parties and must be protected from unauthorized alteration, while making it available to only the authorized individuals. Further, there has been rapid advancements in the use of the internet, as well as a significant increase in cyber-attacks in the past, posing several issues in the huge web globe [3]. Hence, while talking about security of data, it takes into account the data's integrity, confidentiality, and accessibility for protecting the data from unauthorized access. Cryptography, commonly known as "secret writing," indicates the method of

turning messages into secret texts which are impervious to attacks from a suspicious person. Hence, prior to commencement of any kind of communication, cryptography is typically employed that entails encrypting the data prior to transmitting it and decoding it once it has been received. Moreover, data is scrambled using an encryption key, and it is subsequently decoded using either the same key or different key, that achieves the same result as reversing the encryption's impact and recovering the original data. For the message to be encrypted, both parties must exchange a secret key based on the challenge of discrete logarithm computation [4,5].

At the time when anyone attempts to gain unauthorized access to an open wireless network, there is a chance of being caught on the spot. When anyone tries to obtain unauthorized access to any data or resources, it results in unauthorized access to the system. In this context, three common ways to gain unauthorized access are codesharing, guessing, and capturing. Similarly, data integrity is violated when records are changed without any kind of authorization. Any change to the information or even the software could lead to serious issues, possibly deteriorating databases, spreadsheets, or other crucial features. Any miner not authorized to changes in software application may ruin the entire operating system or even all concerned documents associated with the software program and possibly need to reinstall the software along with all related requests. Any alteration in the information or even in treatment can redirect the info to a few distinct places. These detaa Such details could be employed by any outsider or other cyberpunk which can conveniently do some adjustments and subsequently transmit data to the destined region [6,7].

Various types of attacks are encountered in case of data transmission. While discussing a threat, it basically indicates any individual or behavior that has the potential to harm data or a system. Additionally, hazards may be natural or they may even be inadvertent, such as when a file is accidentally deleted. While talking about data security, the term susceptibility of data comes first which is defined as any network's flaws that a threat could arise out of it. Network technology have only recently been used practically everywhere, including in banking, tax, shopping malls, and so on. These programs are made up of numerous computers and network tools. Additionally, it is crucial to protect both these applications and devices. Out of various kinds of attacks encountered in networks, man in the middle attack represents a popular type of cyber-security hazard that enables attackers to listen to the ongoing transmissions between the exporter and the importer. Similarly, phishing, password assaults, and virus attacks are some of the most elementary computerized attacks. The attack usually occurs between two users, allowing the attacker to "listen" to a conversation without the victims' permission, thus the name "Man-in-the-Middle attack". As a result, we utilize cryptography in our discussion which represents the art of encoding sensitive instructions in a way that only the intended recipient can comprehend and process them [7].

The origins of the word cryptography are 'crypto' and 'graphy', which essentially translates to "hidden writing". Data security can be achieved through the use of cryptography. Using mathematical concepts and a sequence of algorithmic calculations, cryptography changes messages in a way that makes them difficult to read. The two primary processes of cryptography are encrypting and decrypting data. The phenomenon of changing plaintext into cypher text is known as encryption. The opposite of encryption, or the conversion of cypher text to plain text, is decryption. There are various ways to protect information that are now fundamental to contemporary cryptography like non-repudiation, data integrity, authentication, etc.

In terms of their keys, cryptography is segregated into two major categories (symmetric and asymmetric). Symmetric cryptosystems call for the use of the same key by all users in order to encrypt and decrypt material. On the contrary, asymmetric cryptosystems demand that users have two unique keys—one for decryption and another for decryption. To make the symmetric key with higher security and impregnable and to stop remaining users from discovering the plain text, it should be frequently changed. Therefore, the key exchange protocol employed by the framework determines how secure any symmetric cryptography system is. Because the user does not have to share their private keys with the recipient or anybody else, an asymmetric algorithm is far more rational than a symmetric method in terms of safe encryption. This reduces the risks of a cybercrime during transmission. Key creation is the process of producing keys in cryptography.

Key exchange protocol is a mechanism for securely sharing keys among users [1-4]. There are numerous ways for Alice and Bob to exchange the

keys. Diffie-Hellman(DH) and Rivest-Shamir-Adleman (RSA) are the two main asymmetric algorithms for encrypting and decrypting messages, respectively. DH key exchange protocol, which is widely employed for secured key exchange today. According to this protocol, Alice and Bob must agree on two apparently prime values, p and g, and subsequently, each one of those utilizes the knowledge they have learned to determine the other's public keys. Thereafter, they exchange their public keys with one another and combine them with respective private keys, p and g, to produce the exchanged key. Consequently, Alice and Bob were both able to access the shared key without having to transfer concerned private keys across the communication medium. DH is basically an encryption method rather than a mechanism for exchanging secret keys between two parties. It's a key-exchange protocol in which each participant produces and shares a public/private key pair. It also allows the two parties to communicate and share the public key through an insecure way without jeopardizing the security of the public key [3, 13]. Symmetric key exchange is the foundation of DH for both encryption and decryption. Since there is no stringent authentication provided by DH, The user's choice of a random prime number totally determines the security of the DH cryptography system. It is a logarithmic problem to find private keys followed by accessing the public key and prime number.

On the other hand, a message can be encrypted using both public and private keys with the help of the public-key encryption algorithm RSA, and it may be decrypted using a different algorithm. It's extensively used to protect sensitive data sent across an unsecured network like the Internet. It has not been demonstrated that defeating the RSA method is analogous to dividing huge numbers, but it has also not been proved that factorization is not equivalent. The various RSA attacks include low exponent, message space searches, cycle assaults, lastly factoring variable N, and common modular, that factors the public key and stands as the most effective method of breaking RSA.

In current paper, we have proffered a cipher hybrid approach to simulate unrevealed instructions, which is a concept that converts simple information to cipher content. Basically, hybrid approach refers to a grouping of two or more schemes. The advantages of both symmetric and asymmetric methods are combined in a hybrid algorithm. There have been a huge number of hybrid algorithms advocated. Various authors employ merely symmetric methods some others employ merely asymmetric algorithms and few researchers employ a merge of these two. So as to ensure the security of data transfer, our research focuses on encrypting and decrypting text using a cutting-edge hybrid technique namely "Hybrid Random Image Generation Strategy (HR-IGS)" that combines both Rivest-Shamir-Adleman (RSA) and DH.

Our proffered method enhances the security and dependability of data transported from the source to the desired destination by using a random picture generation strategy to generate biggest prime numbers. We have applied the RSA Algorithm to extract the prime numbers using XOR function from the corresponding two vectors in each row and column of the scanned picture. We are also creating secret keys with the DH method. Then the encryption and decryption processes are carried on. The main goal here is to minimize the image generation time while also improving key generation time, that can ensure security in data transmittal. Our proposed hybrid strategy mainly offers authentication while conjointly making the secret message exchange possible during data transmittal.

The remaining portions of this research is arranged as follows: the subsequent section incorporates the related literature works done in this domain. Section 3 discusses the proffered strategy. Section 4 elaborates the experimental results attained out of the experimentation. At Last, section 5 summarizes the paper.

2. LITERATURE REVIEW

Cryptography [14], is used to protect information by changing it into an unexpected format. After that, an unauthorized third party will be unable to disrupt the data. In general, this is a way for encapsulating data across an insecure communication channel. When a cryptographic technique is used to change the information sent by the sender and a specific key into a different appearance, the result is known as cipher text, which is then sent to the receiver. The asymmetric algorithms addressed in this study cover RSA, DH, DSA, ECC, hybrid, and DNA cryptography. In the manner of a table, these algorithms are contrasted based on the size of their keys, their capabilities, limitations, attacks, and possible defenses. Due to the sensitivity and urgency of data deposited on cloud base, Hossain et al. [15] studied assessment of several cryptographic techniques, where

defending is analyzed as one of the very demanding features. Encryption/decryption is a common method for protecting hypersensitive information. It is a combination of two different sorts of algorithms as shown in Fig. 1.They are as follows: -

- Symmetric-key algorithms, where data gets encrypted and decrypted employing the same key.
- Asymmetric-key algorithms, where the receiver decodes data using a private key and the sender encrypts it using a public key.

Table 1 represents a scenario of altering the plain text into cipher text and vice versa.

Table 1: Converting Plain Text To Encryption And Vice Versa As An Example

Examples	
Encrypt:- **Plaintext:** This is not me. **Cipher:** Uijtjtopunf	**Decrypt:-** **Cipher:** Mjgfjtbnbajoh **Plaintext:** Life is amazing

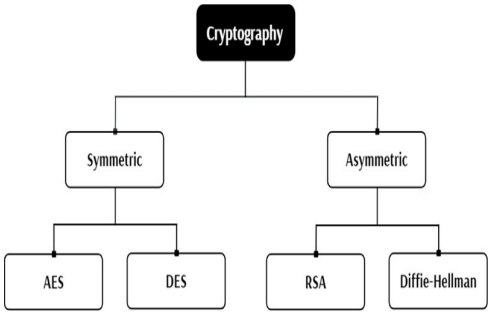

Fig. 1. Classification of Cryptography

2.1 Symmetric Algorithm Overview

Symmetric cryptography, also known as shared key cryptography, is one of the earliest known ways to man, in which a system employs one key for encoding and decoding. Because of its symmetry, the key must be kept hidden at all times. Symmetric encryption is acceptable if you can guarantee that the key will be kept secret. This becomes an issue if you need to maintain the key in many locations or speak with people you don't know. Prior to data swapping between two parties, the key must be agreed upon. As a result, it's known as secret key cryptography. Symmetric encryption is quick to implement. Its encryption is used to send large amounts of data. The likeness is that of an involuntary lock. With the aid of a servant, we enclose a section of a secret message in a box and deliver it to our target recipient. Because he may unlock the lock and reveal the secret message, the real key is never shared directly with the assistant. Our companion, on the other hand, will be carrying a backup duplicate of the same key as us, which he will be able to unwrap. In this case, we're contrasting a public key strategy in which the locking and unlocking keys are non-identical and appear to be separate.

The benefit of symmetric key is that it is solely available to the sender and recipient, and outsiders have no knowledge of it. Symmetric cryptography systems employ techniques such as AES and DES. DES is the first symmetric encryption technique that uses just one key for both ciphering and decoding. The first supremacy is to use 56-bit keys, which makes it difficult to decrypt a message using a brute force technique. Second, supremacy demands that we know the identity of that algorithm; cryptanalysts can do cryptanalysis by employing properties of particular algorithms that are free of critical flaws.

AES is a popular option for the general public due to its faster encryption speed and superior security text.

2.2 Asymmetric Algorithm Overview

Asymmetric cryptography is based on the usage of two(2) keys: public and private keys. Furthermore, the public key gets exchanged via a public network, however the private key is held as private, as the titles suggest. If Bob wants to send an encrypted message to Alice, he can do so now. He needs Alice's public key to encrypt the communication, and after collecting the encoded message, Alice can decode it using her private key. Using Bob's public key, Alice may send encrypted communications to Bob at the same time. Signing the message with asymmetric cryptography is also an option. For example, Bob can encrypt a signed message for Alice with his own private key, and any third party, including Alice, who has Bob's public key, can guess that the identical message came from Bob [15, 16].

Assume the keys are distributed among 2000 people.As a result, each will receive a set of public keys as well as a private key.
As a result, the total number of keys required is: 2 x 2000=4000
In general, 2n keys are required for a network of n end users.

When it comes to key management, asymmetric systems go beyond structured. This is due to the fact that the public key may be broadly disseminated whereas the private key can be held completely secret. However, when it comes to encrypting or signing communications, asymmetric cryptography is currently not very systematic. It necessitated a lot of space, had higher performance (CPU time), and was far more vulnerable to assaults. It employs the RSA and DH protocols.of it.

2.3 Management And Classification Of Key Personnel

Key management is a systematic procedure of producing and administering keys to the various sensor nodes, according to Senthil Kumar et al. [17]. If the nodes are hacked, we'll have to re-

administer the keys. There are two main methods of key management. To begin with, Symmetric Key Management just requires one type of key for node authentication. The use of relatively basic mathematical operations in key pre-distribution is frequently favored in WSN since it reduces computing power requirements and, as a result, battery power consumption. Because it utilizes simpler keys, it will have less memory overhead. It is also often used in WSN because of its lower resource use. Second, Asymmetric Key Management employs a public key and a private key for encrypting and decrypting data separately.

It has a lot of overhead in terms of memory, compute power, and battery life, hence it's not recommended for WSN. It was initially proposed as the primary goal of a public key cryptography system by W. Diffie and M. Hellman. The public key can be shared with all nodes, but the secret key ha to be remained as private. Despite the fact that each node received the public key, hackers will be unable to reconstruct the secret key just by utilizing the public key. Each node in the network can communicate its public key to its neighbors if message encryption is necessary.

The criteria for good key management are covered in the sections below :

- Secure key stores: If malicious people get hold of the keys, they can decode the encrypted data in search of the corresponding keys. The key stores must thus be secured throughout storage, transmittal, and conjointly on backup media.
- Access to key stores: Users who have the right to use the key store's data should be given a certain amount of access. Role separation may be useful here. The entity that keeps a key and the entity that utilises it shouldn't be the same.
- Backup and recovery of keys: Secure key backup and recovery solutions are necessary. Although losing keys might be effective in limiting data access, it can be extremely expensive for a firm. Keys cannot be lost, and cloud service providers must ensure this via backup and recovery procedures.

2.4 Symmetric And Asymmetric Processes Converge

In this issue, Maqsood et al. [13] examined symmetric and asymmetric cryptography techniques. Cryptography's basic functions are to encrypt and decode any message. Symmetric key cryptography employs a single secret key to maintain a secure link between sender and receiver, whereas asymmetric key cryptography applies a public key and a private key. Further, the public key is accessible to all because to its public nature, however the verified user is the only one who can manage the private key.

To identify which encryption system offers the highest level of security. Various characteristics are taken into account to decide which encryption system provides superior security and takes the shortest time to generate keys, encrypts and decrypts sensitive data. Because the key size is less than in asymmetric cryptography, symmetric cryptography gives less data protection. The key generation time is determined by the key length size. Because symmetric cryptography takes less time to compute than asymmetric cryptography, encryption and decryption of large volumes of data becomes more difficult. Plaintext/message is transformed to encoded text (cypher text) and vice versa to calculate the encryption/decryption time.

The file size is also taken into account while evaluating the performance of both systems.

Public key cryptography is used just once for the key exchange, and symmetric cryptography is used for the remainder of the encryption and decryption since asymmetric cryptography has a larger key size and requires more computation time.

2.5 Key Generation Using RSA

Hossain et al. [15] provide an overview of the asymmetric cryptography approach, which employs two distinct encryption and decryption methods. The asymmetric approach is the most often utilized. The RSA (Rivest-Shamir-Adleman) method is a popularly used asymmetric encryption/decryption method that requires both a public and private key. Only the private key can decode messages encrypted with the public key. For the implementation of RSA methods, a 4096-bit key size is employed. Rivest, Shamir, and Adleman are the names of its creators. The P and Q prime numbers are used in this procedure. The strength of this technique stems from the difficulty in locating these two huge prime integers, which are required to position the secret key, whilst the public key may be freely released.

The demands for operational needs are significant in terms of resources since we employ huge prime numbers and factorization as a process. This covers memory, computing power, and operating duration, as well as power supply. To use this approach in wireless sensor network security, you'll need all three resources. The RSA scheme of asymmetric cryptography approaches was evaluated by Mohamad et al. [16], who classed the asymmetric cryptography employs two separate keys to encrypt and decode the message. According to him, the process of transforming plaintext into cypher text, which cannot be read, is known as encryption, while the process of decryption is the opposite. Cryptography's goal is to assure that data is transferred over a secure network by encrypting it into an encrypted format; only the authorized person who has access to the key can encode and decode the message. According to Gowda et al. [19], RSA is an algorithm that current computers employ to encrypt and decode communications. Because one of them may be shared to anybody, this is also known as public key cryptography.

2.5.1. Phase 1: Key Generation

For its procedure, RSA needs two keys. Encryption gets performed using the public key of the recipient, while decryption gets performed using the recipient's private key.

It utilizes the steps below to produce a key:

a) Pick two big and different prime numbers, such as P and Q.
b) Determine N is set to P*Q.
c) Determine z is set to (P-1) * (Q-1).
d) Select a public key exponent E, where 1< E < z and E and z have no other Divisors than 1.
e) Find the congruence relation that D fulfils. 1 = E*D (mod z).
f) E can be segregated by the lowest number in the series: z+1, 2z+1, 3z+1, 4z+1, and so on.

Public Key: (E, N) and Private Key: (E, N) are now becoming present (D, N).

2.5.2. Phase 2: Encryption

Here is a description of how to change plain text into cypher text. It is necessary to utilize a key and an encryption method for this process. The expression C = M ^ E mod (N), in which C represents cypher text and M represents plain text or the message, is used to encrypt a message at the sender's end.

2.5.3. Phase 3: Decryption

This procedure explains how to translate cypher text into plain text. A decryption algorithm and a key are required for this process. The following equation is used to perform decryption at the receiver's send: M = C ^ D mod (N).

The stages of the RSA method are shown in Fig. 2.

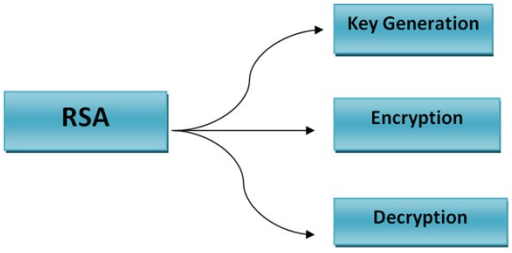

Fig. 2. Classification of Steps in RSA

Journal of Theoretical and Applied Information Technology
31st March 2023. Vol.101. No 6

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

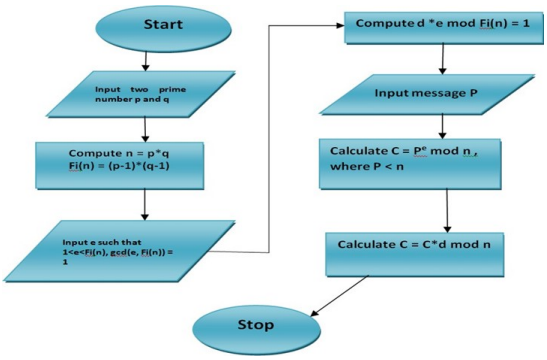

Fig. 3. RSA Scheme Flowchart

The RSA scheme flowchart and Algorithms are portrayed in the Fig. 3 and Fig. 4. Respectively.

Step – 1.
Choose two l arg *est prime numbers* (*p and q*)
Step – 2.
Calculate $n = p * q$
Step – 3.
Calculate $\phi(n) = (p-1)*(q-1)$
Step – 4.
Choose 'e' such that: $1 < e < \phi(n)$
'e' is co – *prime to* $\phi(n)$, $\gcd(e, \phi(n)) = 1$
Step – 5.
Calculate 'd' such that $d_e = 1 \bmod \phi(n)$

$$d = \frac{1 + k * \phi(n)}{e}; \quad k = 0, 1, 2, \ldots\ldots$$

$$d_e \bmod \phi(n) = 1$$

Step – 6.
Find out cipher text (*encryption*)
$C = P^e \bmod n$; *Where* $P < n$

Step – 7.
Decryption
$P = C^d \bmod n$

Fig. 4. Algorithm of RSA

2.5.3.1 RSA Benefits

- It employs Public Key Encryption, which encrypts the message by someone's public key (which is known to the public), but only the intended receiver can decode it with their private key (which only the recipient knows about it).
- RSA establishes irreversible digital signatures by using a public key.
- The algorithms for ciphering and decoding are identical.

2.5.3.2 RSA Drawbacks

- If you know one of the values p, q, e, or d, you can figure out the others. As a result, secrecy is essential.
- It's crucial to keep the message length within the bit length; otherwise, the algorithm would fail.
- RSA is slower than that of other symmetric cryptographic algorithms because it uses public keys.
- n = p * q determines the length of original message that may be encrypted.
- Each time you use the RSA initialization technique, you must choose two very big prime integers at random (p and q).

2.6 Key Generation Using Diffie Hellman

The DH Key Exchange Applications considers the followings aspects [10-12]:

- Programming Language
- LSB Method (Least Significant Bit)
- Key exchange process

The LSB method used substitutes of the two significant bits of the pixel's values coding an image. A Bitmap image is an array which comprises of a set of pixels. For each pixel, the color is coded with three bytes: one for red, one for green and one for blue. The intensity of the corresponding color is indicated by a single byte whose value ranges from 0 to 255. The color does not change much if we change the last bit. In our example (01101011), 1 on the extreme right corresponds to the least significant bit. Table 2 represents a scenario of Diffie Hellman and the steps involved in it are portrayed in Fig. 5.

Table 2. A Scenario of Diffie Hellman

Alice and Bob admit on two numbers lets say 'p' & 'g'	'p' = largest prime number 'g' = base or generator
Alice select a secret number 'a'	Alice's secret number = a
Bob choose a secret number 'b'	Bob's secret number = b
Alice calculated her public number $x = g^a \bmod p$	Alice's public number = x
Bob's calculated his public number $y = g^b \bmod p$	Bob's public number = y
Alice and Bob interchange their public numbers which they have calculated	Alice have p, g, a, x, y Bob have p, g, b, x, y
Alice evaluated $k_a = y^a \bmod p$	$k_a = (g^b \bmod p)^b \bmod p$ $k_a = (g^b)^a \bmod p$ $k_a = g^{ba} \bmod p$
Bob evaluated $k_b = x^b \bmod p$	$K_b = (g^a \bmod p)^b \bmod p$ $K_b = (g^a)^b \bmod p$ $K_b = g^{ab} \bmod p$
By using law of algebra fortunately Alice's 'k_a' is same as Bob's 'k_b' i.e. $k_a = k_b = k$	Now, Alice and Bob both have that secret value i.e. 'k'.

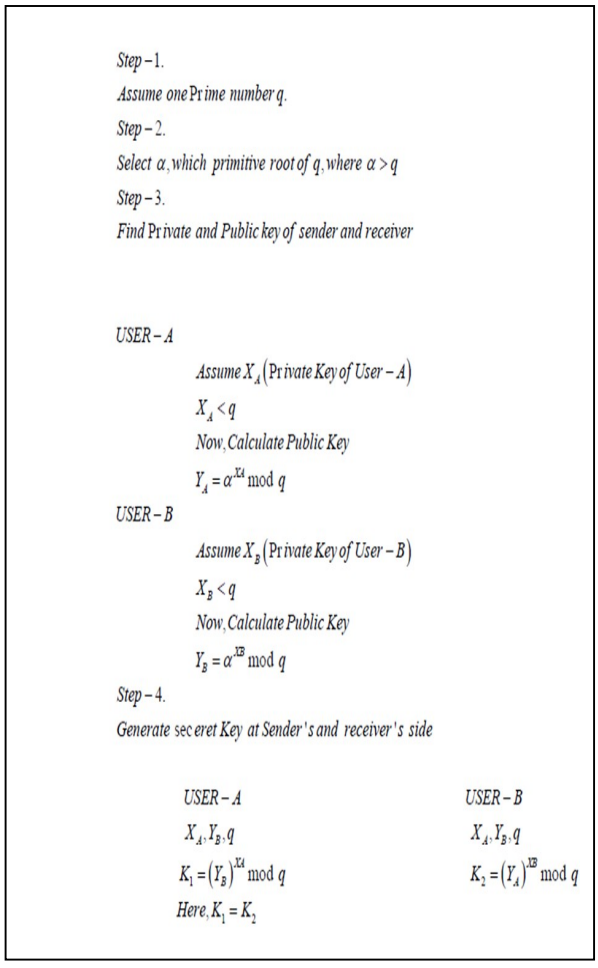

Fig. 5. Diffie Hellman Algorithm

A) Advantages of DH

- It is secure since there have been no effective attack tactics discovered yet. (Year - 2012).
- The DH protocol creates a "shared-secret," a cryptographic key that is shared by both parties to the conversation.

B) Disadvantages of DH

- It is highly prone to man-in-the-middle attacks
- The algorithm cannot be used in encrypting the messages.
- There is also an absence of authenticity.
- Because of the algorithm's computational nature, it may readily be employed in a denial-of-service attack.

2.7 Comparison of RSA and DH

Roy et al. [20] here in this journal compared the RSA and DH (public key) algorithms and explained that an attacker's primary goal is to collect sensitive data that is being transmitted via a public network. Therefore, a cryptographer's responsibility is to defend the data from such attacks by generating a cipher text from plain text. Asymmetric key encryption algorithm and symmetric key algorithm are the two key generating processes. RSA and DH, two asymmetric key methods, are highlighted.

The cryptographic methods regarded as symmetric-key methods apply the similar cryptographic keys for both encoding as well as decoding of plaintext. Public-key also known as asymmetric key algorithms use "public keys" to decode messages instead of "private keys." The sender's private key is applied for encryption, while the recipient's public key is employed for decryption. Because the similar key is applied to encryption and decryption, symmetric keys lose their confidentiality and integrity. The sender's private key is required for asymmetric key encryption. It is an asymmetric key that the two parties share. It is susceptible to man-in-the-middle attacks. With key lengths of 1,024 bits, RSA and DH provide equal levels of security. Both algorithms are based on apparently insurmountable issues, namely the difficulty of factoring huge numbers and the complexity of exponentiation and modular arithmetic, respectively.

2.8 Different Strategies in Literature to Secure Networks

The work done in [1] examines cutting-edge routing strategies and reviews existing solutions for

security. The authors divided these strategies into individual and group Black Hole Attacks, and have evaluated the various divisions of these solutions. They aim to afford complete work to further investigators in the ensuing future. Due to such intrinsic design problems, many academics have proposed a variety of approaches to prevent the black hole problem. The black hole attack, that delays the regular network operation by taking advantage of the routing protocol, is one of the principal attacks.

Our investigation leads us to the conclusion that both proactive and reactive routing require specialist knowledge. The strategy that uses proactive detection has the maximum success rate for properly delivering packets and the maximum likelihood of correct detection. The problem of the black hole is still being researched. Future works will focus on developing a workable strategy to defend data in VANETs and MANETs from such attacks. Likewise, the model used in [2] intends to increase the security of DH key sharing. The outcomes of this study demonstrate the efficacy of the suggested model in comparison to the S-SEJAD approach, which in turn represents a significant advancement over earlier approaches like S-WANE, New-Two-Pass, etc.

The work suggested in [3] employs a hybrid method that combines the (RSA and Modified Diffie Hellman (MDH) algorithms that exchanges keys using two prime factors (P and Q) while conjointly curtailing the likelihood of a man-in-the-middle assault. The MDH also contains a system for authentication. The communication will continue if the two shared keys are equal. Apart from that, it will cease since it gets settled. Furthermore, the RSA method also applies the two prime components produced through MDH (P and Q) while also performing the encryption and decryption of concerned message.

Likewise, a technique as suggested by Khader, et al. In [4] discusses the ways for securing DH aiding systems' defense against MITM assaults. The Geffe generation of binary sequences is used in this method. High levels of unpredictability are offered through the usage of the Geffe generator. Further, data hashed and encoded employing this proffered strategy will be very hectic to cut off and decrypt omitting the required keys. It affords top-levels of security and assists in preventing MITM intrusion. So as to counter the MITM attack, the study in [5] suggests a paradigm for combining the DH key exchange with the RSA cryptography scheme. The effectiveness of the suggested model has been determined by comparing its performance to that of the DH Key Exchange method and the RSA.

Similarly, a broad framework[6] has been suggested by Zhang et al. for intrusion detection. To handle the high dimensional, repeated, but categorically varied and scarce labelled data, a network enclosing property representation is specifically developed in this paper. A network function with clarifying regularization is created to alter the network structure so as to reduce the impact produced by the erroneous network structure. The suggested framework in [6] executes better than various state-of-the-art algorithms in many evaluation metrics. Likewise, a review on cyber security hazards in IoT-enabled industry gets elaborated in [7]. Similarly, the work done in [8-11] discuss various cryptographic strategies.

Gupta et al. [12] proposed a hybrid technique that combines the DH and RSA algorithms, which are both prominent asymmetric algorithms. This strategy was chosen to give the secret key system the advantage in terms of speed while the public key system took the lead in terms of security. The work done in [13] compares the effectiveness of different symmetric and asymmetric methods by taking into account a number of factors, considering file size, key generation time, and encryption/decryption time. The authors compared several cryptographic techniques for evaluation purposes. Similarly, the work in [14-17] discusses various relevant works done in the context of cryptography. The work in [18] details DH key exchange through steganography images.

The study in [19] uses a straightforward DH key exchange scenario. Next, it uses straightforward mathematics to assure that the encryption of data and how it is substantially more secure. Here the DH is used to create a private shared key, which is then subjected to a mod of 26 to produce a value less than or equal to 26, the recent symbol is then chosen, and the key gets added to this to create a novel character. To obtain the encrypted symbol for any symbol at the "x" location, the key gets multiplied by "x" before being "mod"ed.

The work in [20] compares both RSA and DH approaches in the context of secured message transfer. Similarly, Bhardwaj et al. discussed security strategy for cloud computing in [21]. Moreover, a review of prior work is conducted in [22] that applies several algorithms for picture encryption and afford a general introduction to cryptography. With the growing popularity of multimedia software and the relevance of security in data transmission and cache.

Patel et al. [22] advocated a strategy of converting the original image to a complicated image in order to keep the image classified among users and ensure that no one could decrypt the message without the key. As a result, effective storage security is ensured. An enhanced colour picture security technique as suggested by Bhatia, et al. in [23] divides and combines the colour image into shares using visual cryptography, and then encrypts and decrypts it applying the breakdown of the RGB contents (sieving), pixel shuffles, and the RC4 cypher strategy. The resulting encrypted shares are then distributed across the network. Bhaita et al. [23] investigated all available visual cryptography encryption techniques utilizing the RC4 algorithm and pixel shuffling of a picture in their study. When communicating over an unprotected network or channel, the solution he described increases the security and secrecy of colored pictures.

According to color disintegration theories, every pixel in a colored image may be divided into three color values RGB, or Red, Green, and Blue. When applying the pixel shuffling approach, the pixel value remains unchanged, and the RC4 algorithm ensures a high level of anonymity. It was discovered that there was no association between the histograms and security quality factor of the original and encrypted photos, and that pixel intensity was distributed equally.

They devised and put to the test a method for generating two encrypted sections of the secret picture. The results showed that the techniques utilized here made it easier to encrypt and decode pictures while also providing increased security. There was a substantial difference between the encrypted and secret pictures in the system that was tested. As a consequence, the proposed method is very good in securing color pictures and may be expanded to hide data. Shukar et al. [24] updated strategies for deriving a private key from a digital-colored image's unique characteristic, such as (Red, Green, Blue).

The technique for creating a private key from a digital-colored image begins with determining the color frequencies for a blue image, then calculating the greatest frequency of blue, multiplying it by its number, and adding the results to produce a produced key. The private key is then produced, which must be translated to binary form. The resulting key is extracted from the blue keyed picture. Then, when examining a proposed approach for creating the private key, we picked a cover that was a digital-colored image for concealing a text message in the chosen mask. The LSB is used to conceal an algorithm (least significant bit). Finally, the produced key is examined by concealing it and exchanging the additional image; nevertheless, the generated key is not exchanged.

Naeem et al. [25] proposed encrypting the communications using a pseudorandom key stream of bits and later on embedding the ciphered data into a picture using the Bit-shifting technique. The major goal of this research was to improve the data's security by combining steganography with encryption. Moshin et al. [26] explored how technological advancements have resulted in the rise of novel challenges, like intrusion, hacking, and other predicaments, as well as the use of these algorithms to provide data security. The DH method has been one of the most widely used key exchange mechanisms for information security. However, as security has advanced, vulnerabilities like the Man-in-the-Middle attack and the Discrete logarithm attack have arisen. To address such predicaments while also increasing security, each encryption required the development of a randomized color image (N x N), which was then used to generate keys using the XOR function.

3. PROPOSED HYBRID RANDOM IMAGE GENERATION STRATEGY (HR-IGS)

In both the physical and logical levels, the heart of connection/communication is known as the network. It is also widely recognized for packet transfer between our virtual machines and other communication aspects. The Open System Interconnection would adequately explain why network layer protection is so crucial.

Our research focuses on encrypting and decrypting text using a revolutionary hybrid strategy that uses Rivest-Shamir- Adleman (RSA) and DH to ensure security in data transmission. Our suggested method known as "Hybrid Random Image Generation Strategy (HR-IGS) for Securing Plain Text Data" uses a random picture generation process to generate largest prime numbers, which enhances the security and dependability of data sent from the source to the destination. We have employed the RSA Algorithm to extract the prime numbers using XOR function from the corresponding two vectors in each row and column of the scanned picture. Moreover, with the help of DH algorithm we are generating secret keys. Subsequently, the encryption and decryption process carried on. The main goal here is to minimize the image generation time while also improving key generation time, which may lower the risk of being hacked.

According to Patel et al. [22] in this research, with the ever-rising proliferation of multimedia applications, security indicates a critical challenge in picture transmittal and storage. Image encryption methods strive to convert the original image into a difficult-to-understand image in order to keep the picture private between users. No one should be able to access the material without a decryption key, as this ensures storage security. Data security is crucial when a sender intenda to convey a message to a specific individual, which is why we used a random colored picture generating process. Rather than using a black-and-white image like in the instance of Mohsin et al.[26], we used a colorful image in our research.

```
inarray=numpy.random.rand(200,200,3)*255
im=Image.fromarray(imarray.astype('uint8')).conv
ert('RGB') //converting image to "RGB" Format
imgsave=im.save('result_image.png')
imgrad=Image.open('('result_image.png')
frame=numpy.asarray(im)
a=frame.shape[0]
data=imgrad.getdata()

red=[(d[0]) for d in data]
V1=red[0:a]
green=[(d[1]) for d in data]
V2=green[0:a]
```

Fig. 6. Random picture creation with red, green, and blue pixel separation.

```
XOR=list(a^b for a, b in zip(V1,V2))
X1 = random.sample(XOR,4)
V3=sum(X1)
```

Fig. 7(a).

```
Primes=[]
For num in range(100,V3):
if num > 1:
    For I in range(2,num):
        If(num%i)==0:
            Break
else:
    primes.append(num)
```

Fig. 7(b)

Fig. 7: (7(a). Determining a prime number at random, 7(b) Component of the critical generation)

We are using random colored pictures and the original image was then divided into red, blue, and green pictures, from which two vectors were taken to generate private and public keys for encryption and decryption, respectively, in order to secure message transformation as shown in Fig. 6. Fig. 7. shows the XOR operation of two vectors as well as the splitting of a picture into three independent pictures. To increase the unpredictability of prime numbers; the process of manufacturing prime numbers is done.

.

```
pq= random.sample(primes,2)
P = pq[0]
Q= pq[1]
End_1=time.time() * 1000

Message=input("enter message")

N=P*Q
Totient=(P-1)*(Q-1)

def gcd (e, totient):
    while totient !=0:
        c= e% totient
        e=totient
        totient=c
return e

for e in range(2 ,totient):
```

```
    if gcd(e,totient)==1:
     break
d=0
for I in range (1,10):
    x=1+ 1*totient
    if x% e==0
       d=int(x/e)
       break
```

Fig. 8. Component of the critical generation

```
Ascii_values = [ord(character) for character in message]
Ascii_decrypt =[]
Ascii_encrypt=[]
```

Fig. 9. Conversion of character into ASCII value

```
A=e
B=d
G=random.randint(100,1000)
Ridx=random.randint(0, len(primes)-1)
r = primes[ridx]
X=(G**A) % r
Y =(G** B)% r
K1 = pow(Y, A,r)
K2 = pow(X, B,r)
If K1==K2:
   For plain in ascii_values:
      Cipher_text = xor(plain,K1)
      Decrypted_text=xor(Cipher_text)
      Ascii_encrypt.append(Cipher_text)
      Ascii_decrypt.append(decrypted_text)
 else :
  Print("error")
```

Fig. 10. Diffie Hellman Execution

The key generation procedure is depicted in Fig. 8. After tokenizing each alphabet, each character in the message must be translated to its ASCII value, as portrayed in Fig. 9. Fig. 10 represents the execution of Diffie Hellman algorithm where we are taking e as A and d as B whose values are obtained from RSA algorithm.

In this code, r indicates any random prime number selected from the array of prime numbers and g represents a random integer for finding out X and Y which we can utilize in finding K1 and K2. It also illustrates the encryption and decryption of plain text data. The working steps involved in the proposed *HR-IGS* algorithm is as shown in Fig. 11.

4. PERFORMANCE ASSESSMENT

.

We have used Python to implement our proposed approach and other existing approaches. Firstly, we have compared our proposed HR-IGS with both RSA and Diffie-Hellman.

4.1 Performance Parameters

The effectiveness of our proposed approach has been assessed based on the following performance parameters:

- **Execution time:** The execution time associated with any cryptographic method determines the performance of any specific encryption and decryption strategy. The execution time basically indicates how fast or slow the method performs.
- **Avalanche Impact (AI):** The avalanche impact is the degree of variability in ciphertext caused by a little modification or variance in plaintext. For a minor variation in the input, a successful cypher or encryption method must produce entirely different results. The number of variations in the ciphertext are related to an application's level of security, i.e., the greater the method's avalanche effect, the higher its level of security. As a result, it will be challenging for an attacker to conduct statistical analysis.

The goal of flipping just one bit in avalanche effect (%) as given in Eq. (1) is to check the sensitivity of the proffered method by analyzing whether even the smallest change in the plaintexts would absolutely generate a progressive alteration in the cipher text.

$$\%AI = \left({}^{nbct}/_{tnbct}\right) \times 100 \quad (1)$$

Where,

nbct: number of bits present in cipher text

tnbct: total number of bits present in cipher text

4.2 Results and Discussion

We have varied the message size (in bytes) and observed its impact on both encryption and decryption time (in ms) in case of proposed HR-IGS and Classical RSA and Diffie-Hellman as shown in Fig. 12 and Fig. 13 successively. From observing the outcomes in Fig. 12 and Fig. 13, it is evident that the computational complexities of both encryption and decryption strategies of HR-IGS are greater than that of existing RSA and Diffie-Hellman, that justifies that the algorithm will be much more complex and requires higher time for the attackers to breach the security easily than that of the existing methods.

Fig. 14 reports a graphical representation of the avalanche effect estimated in percentage. The result of flipping one bit in 1 K.B. plaintext of RBMRSA produced a 47.52% alteration in the cipher text and that of RSA was calculated as 0.2%, where the value in % indicates the avalanche effect.

In both the proposed and existing approach [26], we have varied the dimensions of colored image as illustrated in Table 3 and Table 4 for both proposed and existing approach to obtain the image generation time as well as prime numbers generation time. It is marked from both the tables that with rise in dimension of image, the image generation time hikes for both the approaches. However, it is found to be lesser in our proposed HR-IGA approach as compared to the existing approach [26].

Likewise, with increase in image dimension, the prime number (P, Q) generation time rises in both the approaches and it is found to be higher in the proposed approach which ensures better security in case of proposed approach. This is because it takes longer time for the attacker to decrypt the keys. Fig. 15 illustrates a sample output of randomly generated image in case of our proposed approach for image size (200x200).

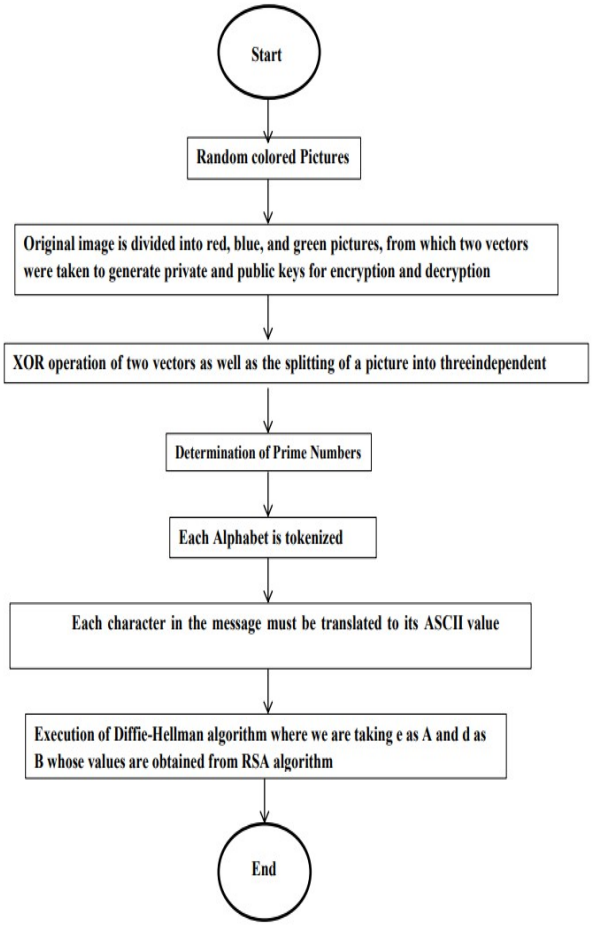

Fig. 11. Working Steps involved in the Proposed HR-IGS

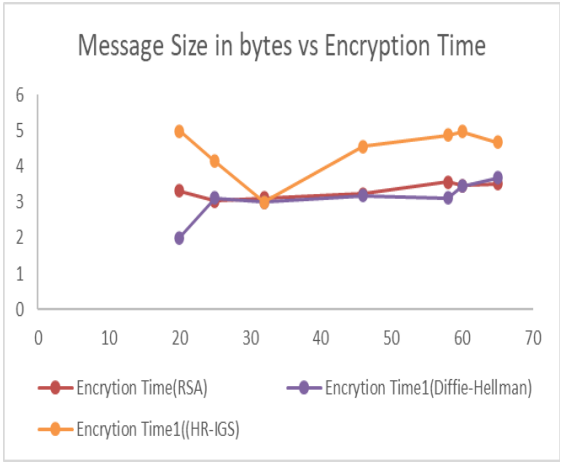

Fig. 12. Result of changing Message Size on Encryption Time

Journal of Theoretical and Applied Information Technology
31st March 2023. Vol.101. No 6

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

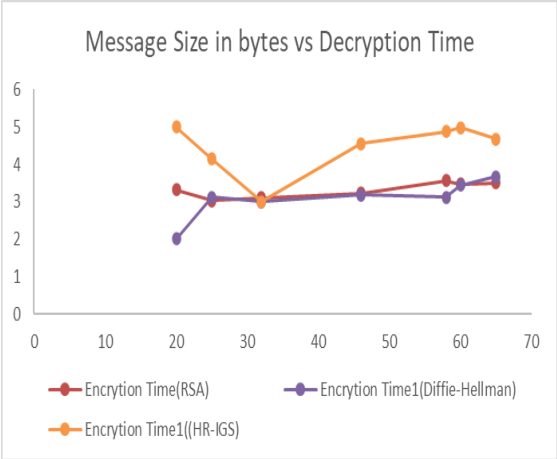

Fig. 13. Result of changing Message Size on Decryption Time

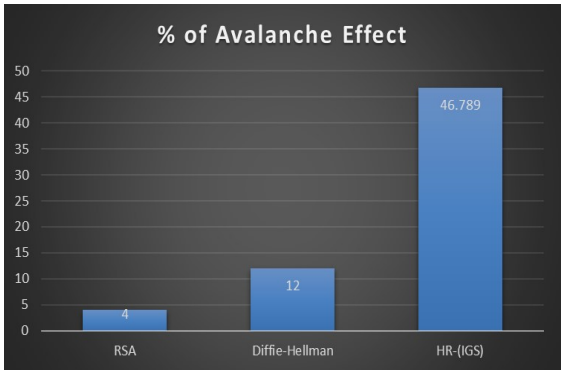

Fig. 14. Percentage (%) of Avalanche Effect in Various Approaches

Table 3. Output of Existing Approach

Dimensions	Image generation Time (ms)	P, Q generation Time (ms)
25x25	**0.002**	0.049
50x50	0.003	0.055
75x75	0.004	1.24
100x100	0.005	3.78
125x125	0.006	5.90
150x150	0.008	9.21
200x200	0.009	**16.1**

Table 4. Output of Proposed approach

Dimensions	Image generation Time (ms)	P,Q generation Time (ms)
25x25	**0.001**	14.8157
50x50	0.002	15.7780
75x75	0.003	21.0312
100x100	0.004	23.55
125x125	0.005	22.7186
150x150	0.007	29.53926
200x200	0.008	**32.84974**

Fig. 15. Random Generated Image

5. CONCLUSION AND FUTURE SCOPE

Security is one among the most important issue in today's digital world. In this paper, we have used a hybrid approach that uses RSA and DH to ensure security in data transmission. Our suggested HR-IGS strategy employs a random picture generation process to generate largest prime numbers, that improves the security and dependability of data sent from the source to the destination.

We have compared our proffered approach with other existing strategy and the outputs received from the experimentation with regard to image generation time and prime number generation time are found to be better as compared to [24]. The image generation time was attained to be minimal at 0.001ms in case of proposed approach for image size of (25 x 25) pixel and the prime number generation time is found to be maximum at 32.84974ms for proposed approach for image size of (200 x 200) pixel. Furthermore, HR-IGS maximizes the avalanche effect while

increasing the execution time, that ensures greater security in data transmission. The outcomes attained from the experimental study support the efficacy of our proffered approach over other existing approaches. Moreover, as a direction towards future work we aim to develop more better algorithm that can afford greater security than that of the proposed algorithm while ensuring the integrity of data transmitted.

ACKNOWLEDGEMENT

The authors are highly grateful to the Computer Science and Information Technology department, Siksha 'O' Anusandhan University for creating this exploration outstanding.

REFERENCES:

[1] A. Lachheb, E.M.Souidi,"The Blackhole Attack on Vehicular Network", International Conference on Wireless Networks and Mobile Communications (WINCOM), IEEE, 2022 Oct 26,pp. 1-5.

[2] A.Ahmed, M.F.Nanne,& B. Gueye,(2022, January), "The effectiveness of a hybrid DH-RSA-AES model", International Conference on Computer Communication and Informatics ,IEEE,2022 pp. 1-5.

[3] J.E. Avestro, A. Sison, R.P.Medina, "Hybrid Algorithm Combining Modified Diffie Hellman and RSA", IEEE 4th International Conference on Technology, Informatics, Management, Engineering & Environment, Bali, Indonesia, 13-15 November, 2019, pp. 100-104.

[4] A.S.Khader, D.Lai, "Preventing Man-in-the-middle attack in Diffie Hellman Key Exchange Protocol", 22nd International Conference on Telecommunications,2015,pp. 204-208.

[5] C.Gupta, N.S. Reddy, "Enhancement of Security of DH Key Exchange Protocol using RSA Cryptography", Journal of Physics: Conference Series, vol. 2161, 2022,pp. 1-10 .

[6] Y.Zhang, C.Yang, K.Huang, Y. Li, "Intrusion detection of industrial internet-of-things based on reconstructed graph neural networks", IEEE Transactions on Network Science and Engineering. 2022 Jun 21.

[7] I.Ashraf, Y.Park, S.Hur, S.W.Kim, R. Alroobaea, Y.B. Zikria, S. Nosheen, " A survey on cyber security threats in IoT-enabled maritime industry",IEEE Transactions on Intelligent Transportation Systems,2022,pp. 280-288.

[8] J.Alshehri, and A. Alhamed, "A Review Paper for the Role of Cryptography in Network Security", In 2022 4th International Conference on Electrical, Control and Instrumentation Engineering, IEEE, 2022,pp.1-5.

[9] C.Singh, L. Kaur, "The A review of different approaches for improving network security in cryptography", Turkish Journal Of Computer And Mathematics Education, 12(1),2021,pp. 819-823.

[10] Rawat, E., Singh, A., Mahar, A., Agarwal, A.: A Review Paper on Cryptography and Network security, 2022.

[11] A. Abusukhon, & S. AlZu'bi, "New direction of cryptography: A review on text-to-image encryption algorithms based on RGB color value", Seventh International Conference on Software Defined Systems (SDS) ,IEEE,2020,pp. 235-239.

[12] Gupta, S., & Sharma, J. (2012, December). A hybrid encryption algorithm based on RSA and DH. In 2012 IEEE International Conference on Computational Intelligence and Computing Research (pp. 1-4). IEEE.

[13] F.Maqsood, M. Ahmed, M.Mumtaz, & M.Ali, "Cryptography: a comparative analysis for modern techniques", International Journal of Advanced Computer Science and Applications, 8(6),2017,pp. 442-448.

[14] P.Singh, & R.K.Chauhan, " A Survey on Comparisons of Cryptographic Algorithms Using Certain Parameters in WSN",International Journal of Electrical & Computer Engineering (2088-8708), 7(4),2017.

[15] M.A.Hossain, M.B. Hossain, M. B., M.S.Uddin, & S.M.Imtiaz, " Performance analysis of different cryptography algorithms", International Journal of Advanced Research in Computer Science and Software Engineering, 6(3),2016.

[16] M.S.A Mohamad, R. Din, & J.I.Ahmad, " Research trends review on RSA scheme of asymmetric cryptography techniques", Bulletin of Electrical Engineering and Informatics, 10(1),2021,pp. 487-492.

[17] U.S.M.N. SenthilKumar,& U.Senthilkumaran, "Review of asymmetric key cryptography in wireless sensor networks", International Journal of Engineering and Technology, 8(2),2016,pp. 859-862.

[18] K.H.A.L.D.I. Amine, K. H. A. L. D. I, "DH key exchange through Steganographied images", Brasilia, 10(1),2018,pp. 147-160.

[19] S.N.Gowda, "Innovative enhancement of the Caesar cipher algorithm for cryptography" In 2016 2nd International Conference on Advances in Computing, Communication, & Automation (ICACCA)(Fall),IEEE,2016,pp. 1-4.

[20] A.Roy, "Brief comparison of RSA and DH (public key) algorithm", ACCENTS Transactions On Information Security, 1(1),2016.

[21] A.Bhardwaj, G.V.B. Subrahmanyam, V. Avasthi, & H. Sastry, " Security algorithms for cloud computing", Procedia Computer Science, 85,2016,pp. 535-542.

[21] K.D.Patel, & S.Belani, "Image encryption using different techniques: A review",International Journal of Emerging Technology and Advanced Engineering, 1(1),2011,pp. 30-34.

[22] S. Bhatia, S.K.Khatri, & A.V.Singh, Digital image security using hybrid visual cryptography. In 2018 7th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions), IEEE,2018, August ,pp. 570-576.

[23] W.A. Shukur, " A proposed method for generating a private key using digital color image",International Journal of Applied Engineering Research, 12(16),2017,pp. 6235-6240.

[24] J.S.Hamad Naeem, W.A. Abro, A. Khalid, M.R. Naeem,A.A. Memon, & S.Tanvir, " Message Encryption by Processing Image Using Pseudo Random Key Streams Generation"

[25] R.M.Mohsin, R.I.Ahmed, R. I., R.Yaqub,& S.Ethar, "A new technique for Diffie-hillman key exchange protocol security using random image generation", In 2019 First International Conference of Computer and Applied Sciences (CAS),IEEE,2019,pp. 262-267.