ANALYSIS OF CRYPTOGRAPHY ENCRYPTION FOR NETWORK SECURITY AND IMAGE STEGANOGRAPHY TECHNIQUE

SHIKHA CHOUDHARY*
SIET, Shobhit Institute of Engineering and Technology Deemed to be University, Meerut,
U.P., India
shikha@shobhituniversity.ac.in
SHAMSHAD HUSAIN
SBAS, Shobhit Institute of Engineering and Technology Deemed to be University, Meerut,
U.P., India
shamshadhusain0646@gmail.com

Abstract:

Data security involves protecting digital information to prevent unauthorized access to computers, databases, and websites. Cryptography, encryption, and compression are key strategies for data protection. AES is a powerful cryptographic method. Confidentiality, authenticity, integrity, and non-repudiation are crucial for online communication. Steganography enhances message security across networks, using a photo as a cover material. The smart grid offers flexibility, reliability, and efficiency in power production and distribution. To protect privacy and confidentiality, grayscale cover images undergo discrete wavelet transformation (DWT) and a chaotic map is applied to the secret image. This paper also discusses the use of cryptography and network encryption to secure wireless network data transmission. It emphasizes the importance of data protection for wireless network sensors linked to base stations. Network security is crucial as the world transitions into the digital world, addressing issues like administrator-managed data and communication technology. Cryptography aims to protect networks from attacks and intrusions, while intrusion and computer protection technologies are also used.

Keywords: Cryptography Concept, Network Security, Integrity DWT, Security, Information Hiding, Steganography.

1. INTRODUCTION

To help clients and UPs perform near actual-time monitoring of strength use, transmission, and generation, SGs strive to easily integrate various technologies. **Shikha and Chetan (2014)** focuses on key based image Steganography using DWT (discrete wavelet transformation) and chaotic map. In this, the major focus on the secrecy and privacy of information. DWT is used to perform on a grey level cover image for secrecy and on the other hand chaotic map is applied on the secret image for privacy. Different businesses may additionally use this information to target their adverts, but greater significantly, cybercriminals and enemies might also use it in opposition to **Zhu et al. (2017)** evaluations the regulations surrounding the acquisition and management of SM statistics One of the biggest boundaries to the a success implementation of SGs in many nations is SM privateness numerous approaches to improve the capability and value of SMs in SGs are supplied in a wealth of literature. An great assessment of smart metre information analytics from an software standpoint changed into published in a latest famend survey study **Ferrag et al. (2018**). **Abbasinezhad-Mood and Nikooghadam (2018)** The UP can optimize and manipulate the supply and distribution of energy way to an SM. Demand Response (DR) is likewise used to assist stability the weight, and it gives customers additional services. For dynamic pricing, fraud detection, and call for forecasting in SGs, excessive-decision SM information may be employed . If those records are not maintained correctly, it would result in a violation of customer privacy. For example, with the aid of studying SM statistics the usage of Non-Intrusive Load Monitoring (NILM), an outdoor birthday party can pinpoint specific equipment intake.**Husain and Shivani (2018)**found study of properties of soft set and its applications. Key articles that examined critical privacy-maintaining techniques in current years may be located in works by **Hossain et al. (2019)** addressed statistics aggregation processes for SM privateness and included difficulties with signal processing, safe cryptographic algorithms, and hardware constraints. reviews Homographic Encryption (HE)-based techniques, a specialized subset of SM privacy. Without deliberating greater current functions like value-added offerings (VAS), SM statistics altering techniques, and renewable electricity assets (RES), the publications in **Natgunanathan et al. (2019)**focused on the greater mounted factors of SM privacy. A current studies **Wang et al. (2019)** tested the benefits and disadvantages of various data safety and privacy protection systems in SG communications. According to 4 regions (information privateness, non-public privacy, organizational privateness, and highbrow privacy), the look at in **Hossain et al. (2021)** evaluated, debated, and assessed numerous SM privacy protection methodologies earlier than pointing out their faults and deserves. This necessitates the gathering of a sizeable quantity of facts, which offers several facts control problems, the most critical of that is the renovation of purchaser privateness **Dong et al. (2021).** One of the important thing additives of smart grids (SGs), clever metres (SM), is often considered as the first step inside the powerful deployment of SGs. A SM compromise could have big results for the whole SG. Two-way conversation among clients and UPs is made possible with the aid of SMs. In almost real-time, they can screen and offer records on energy use. It is likewise viable to infer touchy and personal statistics, like appliance types and types, client family sizes, age groupings, and day by day workouts. We have visible in current years how quick technologies are being advanced to help the big implementation of clever grids (SGs). **Abdalzaher et al. (2022)** SG is a extra state-of-the-art form of strength grid that permits two-way statistics and electricity alternate among clients and Utility Providers (UPs) with the aid of utilising cutting-edge communique era and facts control. **Husain et al. (2022)** used a family of linked subsets to create a club characteristic for fuzzy soft units. Additionally, **Husain et al. (2022)** produced a hybrid model for a single decision maker to choose a choice value.Compression and encryption are essential security measures for data protection in IT companies. Compression saves disk space and allows for faster data transfer via the internet. Data safety goals include confidentiality, authentication, integrity, and non-repudiation. To address the growing problem of information protection, companies are increasingly adopting cryptography to protect their valuable data. Data compression reduces storage and communication costs by reworking data into smaller formats, while encryption protects information from eavesdropping. Modern cryptography is based on mathematical ideas and computer technology, making it difficult to break. However, its potential for espionage and sedition has led to legal issues and restrictions on its use and export.

This paper is organized as follows: The energy grid of the present day period known as the "smart grid" gives flexibility, dependability, and efficiency within the manufacturing, management, and distribution of electricity. The clever grid allows for two-way communication among outlets and clients, and touchy information is shared via the community. In an effort to undermine the grid and clients for his or her own advantage, the attacker is attempting to attack statistics. The power industry has an unrivaled opportunity to adopt modern, reliable, and green technologies with the intention to gain our economic system and the environment. This possibility is represented via the smart grid. The blessings of a smart grid include faster energy recovery instances, more environmentally pleasant electricity transmission, and decrease operational and management costs for utilities. Additionally, computer statistics travels from one device to any other, protective their bodily surroundings. When information gets out of hand, it is probably modified or falsified for amusement or the benefit of individuals with bad intentions. Our facts may be become and restructured the use of cryptography to increase the security of its switch throughout computers. The basis of era is mystery codes, which are bolstered by modern-day mathematics and provide robust statistics protection.

2. CRYPTOGRAPHY

The artwork of cryptography is taken into consideration to be born alongside the art of writing. As civilizations developed, people got prepared in tribes, groups, and kingdoms. This brought about the emergence of thoughts which include energy, battles, supremacy, and politics. These thoughts further fueled the natural need of human beings to talk secretly with selective recipient which in flip ensured the non-stop evolution of cryptography as properly. The roots of cryptography are determined in Roman and Egyptian civilizations. The significance of facts and verbal exchange systems for society and the global economic system is intensifying with the growing fee and quantity of information this is transmitted and saved on those systems. At the equal time those systems and records are also an increasing number of vulnerable to quite a few threats, which include unauthorized access and use, misappropriation, alteration, and destruction. The hiding of facts is known as encryption, and whilst the records is unhidden, it's miles referred to as decryption. A cipher is used to accomplish the encryption and decryption. Merriam-Webster's Collegiate Dictionary defines cipher as ―a way of remodeling a textual content as a way to conceal its which means. The records this is being hidden is referred to as plaintext; once it has been encrypted, it is known as cipher textual content. To cover any facts two strategies are specially used one is Cryptography different is Steganography. In this paper we use Cryptography. Cryptography is the technological know-how of defensive statistics, which gives techniques of changing statistics into unreadable form, so that Valid User can get right of entry to Information at the Destination. Cryptography is the technological know-how of the use of mathematics to encrypt and decrypt records. Basic Terminology of Cryptography. Computers are utilized by millions of human beings for plenty purposes. Along with banking, buying, military, scholar facts, and so on.. Privacy is a crucial difficulty in many of those programs, how are we want to ensure that an unauthorized parties can't examine or modify messages. Cryptography is the transformation of readable and comprehensible statistics into a shape which cannot be understood so that you can steady information. Cryptography refers exactly to the method of concealing the content material of messages, the phrase cryptography comes from the Greek phrase "Kryptos", that means hidden, and "graphikos" this means that writing. The facts that we want to hide, is known as plaintext, It’s the unique textual content, It might be in a form of characters, numerical information, executable applications, snap shots, or every other form of information, The plaintext as an example is the sending of a message inside the sender before encryption, or it's far the textual content on the receiver after decryption. The information so as to be transmitted is called cipher text , it's a term refers back to the string of "meaningless" statistics, or doubtful text that nobody have to understand, except the recipients. It is the facts that will be transmitted Exactly via network, Many algorithms are used to transform plaintext into cipher textual content. Cipher is the set of rules that is used to transform plaintext to cipher textual content, This technique is called encryption, in different phrases, it's a mechanism of converting readable and understandable facts into "meaningless" data. The Key is an input to the encryption set of rules, and this cost must be impartial of the plaintext, This enter is used to transform the plaintext into cipher textual content, so different keys will yield specific cipher textual content, In the decipher facet, the inverse of the key could be used within the set of rules instead of the important thing. Computer security it is a common time period for a set of tools designed to shield any records from hackers, robbery, corruption, or herbal catastrophe while allowing these facts to be available to the users on the identical time. The instance of those equipment is the antivirus program. Network security refers to any interest designed to protect the usability, integrity, reliability, and safety of information during their transmission on a community, Network safety offers with hardware and software program. The activity can be one of the following anti-virus and anti-spyware, firewall, Intrusion prevention systems, and Virtual Private Networks. Internet Security is measures and procedures used to protect data at some stage in their transmission over collection of interconnected networks, at the same time as statistics security is ready a way to prevent assaults, and to hit upon assaults on information-primarily based structures.

2.1 Cryptography Goals

By the use of cryptography many goals may be performed, these dreams may be both all finished at the same time in one software, or only considered one of them. These goals are:
Confidentiality: it is the most essential intention, that guarantees that no person can recognize the acquired message besides the only who has the decipher key. Authentication: it's far the manner of proving the identification that assures the communicating entity is the one that it claimed to be. This means that the person or the system can prove their very own identities to other events who don’t have private expertise in their identities. Data Integrity: its guarantees that the acquired message has no longer been changed in any way from its unique shape. The data may additionally get modified by using an unauthorized entity deliberately or accidently. Integrity provider confirms that whether records are unbroken or now not because it become closing created, transmitted, or stored with the aid of a licensed user. This can be completed by using the usage of hashing at both facets the sender and the recipient for you to create a unique message digest and compare it with the only that acquired. On-Repudiation: it's miles mechanism used to prove that the sender honestly sent this message, and the message became received by using the desired birthday celebration, so the recipient can't claim that the message turned into now not dispatched. For instance, as soon as an order is placed electronically, a client cannot deny the acquisition order, if non-repudiation carrier was enabled on this transaction. Access Control: it's far the method of stopping an unauthorized use of resources. This aim controls who may have access to the resources, If you may get right of entry to, beneath which regulations and situations the get entry to may be happened, and what is the permission stage of a given access.

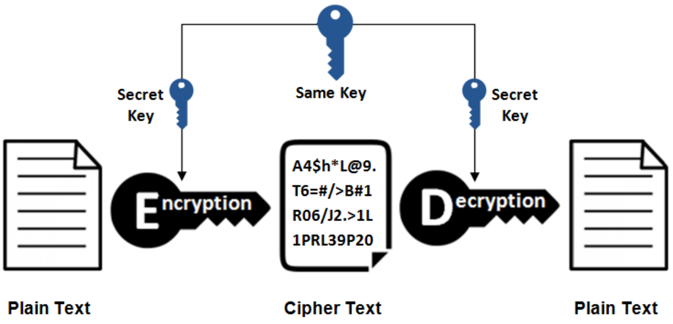
2.2. Data Encryption

A statistics encryption is a random string of bits created explicitly for scrambling and unscrambling information. Data encryption is designed with algorithms meant to ensure that every key is unpredictable and specific. Cryptography uses styles of keys: symmetric and asymmetric. Symmetric keys had been across the longest; they utilize a unmarried key for each the encryption and decryption of the cipher text. This form of key's referred to as a mystery key. Secret-key ciphers usually fall into considered one of two classes: circulation ciphers or block ciphers. A block cipher applies a non-public key and algorithm to a block of information concurrently, whereas a movement cipher applies the key and set of rules one bit at a time .Most cryptographic strategies use symmetric encryption to encrypt information transmissions however use asymmetric encryption to encrypt and change the name of the game key. Symmetric encryption, also called private key encryption, makes use of the identical private key for each encryption and decryption. The danger on this machine is if either party loses the important thing or the key's intercepted, the gadget is broken and messages cannot be exchanged securely. One of the foremost motives for implementing an encryption-decryption device is privacy. As records travels over the World Wide Web, it turns into situation to get entry to from unauthorized people or organizations. Decryption is the manner of taking encoded or encrypted text or different records and converting it lower back into text which you or the pc can examine and understand. This term will be used to explain a method of un-encrypting the statistics manually or with un-encrypting the records using the proper codes or keys. Encryption is the process of translating plain text statistics (plaintext) into something that looks to be random and meaningless (cipher textual content). Decryption is the technique of converting cipher textual content returned to plaintext.

2.3. Symmetric Key Cryptography

In symmetric key cryptography is also called non-public-key cryptography, a mystery key can be held by using one man or woman or exchanged among the sender and the receiver of a message. If private key cryptography is used to send mystery messages among events, each the sender and receiver ought to have a replica of the secret key.

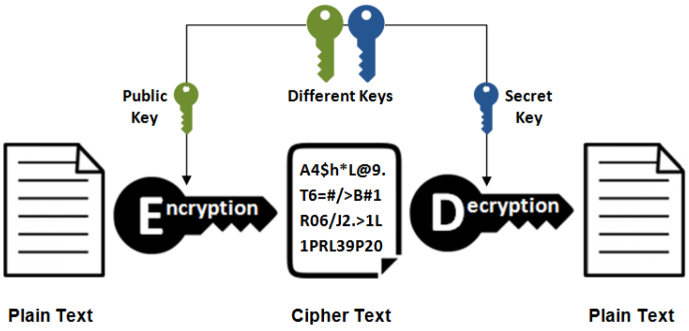
Symmetric Encryption



2.4. Asymmetric Key Cryptography

In the two-key gadget is likewise called the general public key system, one key encrypts the statistics and any other, mathematically related key decrypts it. The pc sending an encrypted message makes use of a designated private key that is by no means shared and so is understood only to the sender. If a sending computer first encrypts the message with the supposed receiver’s public key and once more with the sender’s secret, private key, then the receiving computer may decrypt the message, first using its mystery key after which the sender’s public key. Using this public-key cryptographic approach, the sender and receiver are able to authenticate one another in addition to protect the secrecy of the message.

Asymmetric Encryption



3. NETWORK SECURITY

1. Computer security is the umbrella term for tools that prevent hackers and safeguard data. Data protection measures for networks during transmission network safety
2. Internet Security: Connected data collection methods for data protection Services, Mechanisms, and Security Attacks the security manager in charge of an organization's safety needs a systematic way to determine what security is needed.
3. Security attack - Any actions that affect an entity's information security.
4. Security mechanism: A technique for identifying, stopping, or recovering from a security breach.
5. Security services: These are services that enhance the security of data management infrastructure and the exchange of corporate information. By utilizing one or more security measures, the services are intended to counter security threats.

Defence is a wide variety of subjects and encompasses several sins. The goal is to ensure that nobody can read or, worse, alter messages secretly for others. In its simplest shape. It's a matter of people wanting to use remote resources that they can't use. The majority of threats to security are intentionally created by malicious people who try to gain some benefit, care or damage others. Network securities problems can be divided loosely into Fournier related areas:

a) Secrecy
b) Authentication
c) No repudiation and
d) Integrity control

3.1 Secrecy

Secrecy, also known as secrecy, is related to retaining data from unauthorized users. That's what people generally think about when thinking about network protection. Authentication Is about who you are talking to before you share confidential information or enter a company. Without repudiation, there are some basic safety criteria, including: authentication, in the sense of all application-to - application communications. Privacy: Ensure no one can read the message except the desired recipient. Message Integrity: ensure there sapient has not altered the message received from the initialing any way. Non-repudiation: method to demonstrate that this message was actually sent.

3.2 Authentication

The evidence of the phase of identity. Host-to - host authentication now consists mostly of names and addresses that are notoriously weak. Host-to The receiver and the sender shall confirm their identities in order to confirm that the other person is who they say or say to be. It is necessary for the other party to confirm its identity. This issue is overcome quickly through visual identification and face-to - face contact. Authentication is not so easy when interacting individuals exchange messages through a medium that they cannot "see" the other entity. For eg, why do you think you got an e-mail with a text string stating that the e-mail was actually from a friend of yours? Will you send the information on the phone when someone is calling for your bank and demands your account number, hidden PIN and authentication accounts? I hope that this does not happen

3.3. Privacy/Confidentiality

Ensured the message can only be read by the sender and the intended recipient, the content of the transmitted message should be understood. Since eaves droppers can stop the message, this necessitates somehow encrypting the message (disguising data) so that an interceptor cannot decrypt the intercepted message (understood). Perhaps the most common interpretation of the word protected communications is the element of confidentiality. But this is not only a restricted description of protected communications; it must be remembered, but a more restrained term of confidentiality.

3.4. Message

Integrity providing that the recipient has not changed the message p received. Even if the sender and recipient may authenticate each other, they want to make sure that they do not change the contents of the correspondence maliciously or by mistake. Extensions of check summing methods found in the reliable protocols for transport and data connection.

3.5. No repudiation

Non-repudiation is an evidence that this message was actually sent by the sender. It covers signatures, which have defined our significance in the context of safe communication; then let us consider precisely what a "in certain channel" means. What information an attacker has access to and the behavior that Alice, the sender, may do to deliver the data to Bob, the recipient.

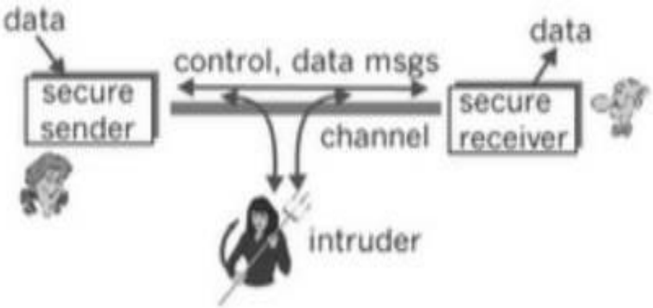


Figure1.Thethreetypesof algorithms

3.6. Cyber security policies

Cyber security policies are a set of rules of how companies should practice responsible security. It begins with general security expectations, roles, and responsibilities inside the company. There are a set of templates that platforms offer to make a well efficient cuber policy.

The larger organizations have more clauses as they have more stakeholders inside and outside. While the smaller ones follow basic precautions to ensure safety at the operational level. They are mainly –

1. Rules for using email encryption
2. Steps for accessing work applications remotely
3. Guidelines for creating and safeguarding passwords
4. Rules on the use of social media

But the size is secondary; the priority should be on sensitive data, risk analysis, and previous breaches. All organizations should primarily focus on these things, no matter what. They should make these policies easy to understand so that more people can follow them.

And all employees should make it a point to follow them for a more secure workspace. There are multiple benefits of having a cyber security policy in place, for organizations as well as for the employees. They are mainly –

3.7. Importance of Cyber Security Policies

1. Efficient

The policies are to ensure safety at all times, resulting in higher consistency. The money and other resources are also managed more effectively due to this. The employees should be well aware of all the policies and should avoid mistakes and work more productively.

2. **Disciplined and Accountable**

These policies make companies accountable to follow certain sets of instructions, which they will not otherwise. And this in turn leads to a more systematic approach because every mistake on the company’s front needs disciplinary action.

3. **Business Contracts**

It has the ability to manage business deals as well. When companies enter a contract, they need to share their security policies beforehand. A similar policy can lead to a longer relationship while some can lead to complications as well.

4. **Security Literacy**

The employees receive exposure to ethical security policies through the organizations. And now this is for all of the employees as such details come in their company contract. This leads to an increase in security literacy and fewer breaches in the company due to human errors.

4. STEGANOGRAPHY

Steganography is the art and technology of writing hidden message in information besides the sender and intended recipient. Security plays a vital function in steganography. Steganography is an encryption method that may be used along with cryptography as an extra steady technique wherein to protect statistics. Steganography techniques may be carried out to snap shots, a video file or an audio document. Typically, steganography is written in individual together with hash marking, but its usage interior photography is moreover commonplace.

Cryptography is approach of securing facts and conversation via use of codes so that simplest those humans for whom the records is supposed can recognize it and procedure it. Thus, preventing unauthorized get right of entry to data. In cryptography the strategies which can be use to shield statistics are acquired from mathematical idea and a hard and fast of guidelines-primarily based calculations called algorithms to convert messages in techniques that make it difficult to decode it. These algorithms are used for cryptographic key generation, virtual signing, verification to shield facts privateness, internet purchasing on net and to defend personal transaction including deposit card and debit card transactions.

4.1. Key primarily based assault: In this grid a mystery key has been used for registration and authentication. The attacker has implemented identified and unknown key assault on the clever grid to take keep of the name of the game key.

4.2. Impersonation primarily based attack: In this grid the detrimental can look at clever meter statistics which coming from smart houses to read how a bargain electric electricity intake is accomplished. The attackers are tries to display and modify these facts.

4.3. Data based assault: In this attack, the weight balancing among demand and era is required. The attackers are trying to regulate these facts. Further, the records-based totally assault is categorized into a number of assault, which consists of modification assault, data integrity assault, selected plaintext cipher text assault and repudiation assault.

4.4. Physical based totally assault: In this assault, the attacker's intention the hardware used in smart grid which encompass battery motors, a neighborhood aggregator and a proxy server. This assault is labeled into 4 sorts such as a differential attack, malware attack, and collusion attack and so on.

5. STEGANOGRAPHY TECHNIQUE

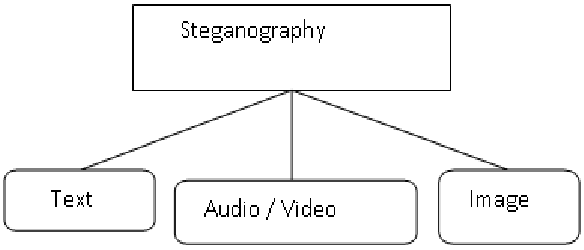


Fig.1 Steganography Techniques

On the basis of different types of cover files Steganographic techniques can be classified as shown in the figure below

5.1. Text hiding methodology

The important motive of statistics hiding is the secrecy of the hidden message, robustness of the approach and fact hidden length. Several audio steganography tactics have been advanced. The manner of selecting the area relies upon on the cause of developing the method. In time domain steganography technique watermark is straight away embedded into audio signal in which no domain remodel is required. The information and textual content that's to be hidden inside the cowl frame. The text has been converted into binary shape and every pixels of the frame had been calculated. Each little bit of the text message is to be changed with the two frames of LSB. Their goal was established an impervious way of retrieve the message. The frame has been examined and each pixels of frame is calculated. The approach is amazing transportable.

5.2. Video Hiding methodology

The primary paintings of video steganography is cover secret message without affecting the great of the video file.In embedding algorithm, they first study the cover video. Now the video has been segments into frames and to compute the histogram of each body. If the 2-histogram fee of body is more or identical to histogram steady cost then determined the parameter used in recovery stage. Now embedded the hidden information into frame and get the stego image.

5.3. Audio Hiding methodology

Audio steganography is one of the well-known records hiding techniques that embedded mystery facts into audio signs. On the opposite hand, the name of the game reality is hidden in a manner that unauthorized character isn't aware in the existence of the embedded statistics and except altering the first-rate of the quilt audio. Data hiding in audio regulate has numerous application consisting of safety of copyright audio sign ,covert communication ,hiding data that also can have an effect on the protection of governments and private .An excessive first-class audio steganography need to have the traits for profitable embedding and extracting records, high records charge and robustness of the embedded facts.

5.4. Related Work in Image Steganography

Till now many photo Steganography schemes have been proposed as the use of LSB. LSB is the least huge bit approach. This method is quite simple for both embedding and de-embedding. In this approach mystery bit is embedded into the least great little bit of the cover photo. Another method is Most Significant bit Technique in this method MSB (Most Significant Bit) in a sequence of numbers in binary. For example in binary wide variety: 11001111, the most tremendous bit is far flung left 1. In the MSB method, the secret data is embedded into maximum large little bit of the pixel inside the picture. **Mouachi et al. (2017)**The manner of hiding the binary same of a hundred as follows :

Pixels:	(00111101	00111100	11000100)
	(10000110	11110100	11101100)
	(11011010	10100101	01110011)

100-Binary Value: 100100 Result:

(00100101 01101101 11001010)
(00100101 01001010 11101011)
(11001100 10100101 01101101)

The following method makes use of pixel fee differencing. The PVD is dependent on the variation in pixel values. The cover image become first divided into non-overlapping pieces with two related pixels. They then convert every block distinction returned to its unique pixel fee. The distinction among neighboring pixels in a easy region is much less than the brink range. Therefore, part location pixels comprise more information than easy region pixels. The PVD is advanced than the LSB.

Another technique DCT is the Discrete Cosine Transform technique. It is just like Discrete Fourier Transform. The DCT rework a sign from an picture illustration right into a frequency representation by means of grouping the pixel into 8*8-pixel blocks into 64 DCT. This is a extra complicated way of hiding facts in to the picture. Various algorithms and transformations strategies are used at the image to hide data in it. Transform domain embedding may be term as a domain of embedding techniques for which a many algorithms were suggested. The procedure of embedding records within the frequency domain of a sign is an awful lot stronger than embedding concepts that operate within the time domain. Most of the sturdy Steganography structures these days work inside the transform strategies have an advantage over spatial techniques as they hide records in areas of the picture that are a smaller quantity exposed to compression, cropping, and image processing. Some remodel techniques do now not seem depending on the image format and they may outrun lossless and lossy format conversions. Transform strategies are extensively classify into: Discrete cosine transformation method (DCT) and Discrete Wavelet transformation approach (DWT).

Another method is Spread spectrum Technique. In this technique the message is spread over a huge frequency bandwidth than the minimal required bandwidth to send the records.

6. COMPARATIVE ANALYSIS FOR VARIOUS METHODS

Data compression gives an attractive approach for lowering verbal exchange charges by using the usage of available bandwidth efficaciously. Compression algorithms lessen the redundancy in data illustration to lower the garage required for that records. Over the last decade there has been an unprecedented explosion in the amount of virtual records transmitted through the Internet, representing text, photographs, video, sound, pc packages etc.

Data compression implies sending or storing a smaller quantity of bits. Compression is the reduction in size of records a good way to shop area or transmission time. Many strategies are used for this purpose, in preferred these techniques may be divided into vast classes: Lossy and Lossless methods. Lossy Compression commonly used for compress images. In these unique records is not same to compressed information which means there may be some loss e.g. Block Truncation Coding, Transform Coding, and so on... Lossless Compression used for compress any textual data.

S.No	Research Name	Domain	Method	Performance Analysis
1	Data Embedding using Image Steganography	Transform	DWT &AES Cryptography	Transform technique on DWT Steganography is performance low PSNR value also low
2	Hybrid Approach to Text & Image Steganography using AES and LSB Techniques	Spatial	LSB &AES cryptography	Spatial Steganography High performance PSNR value is High
3	High PSNR based Image Steganography	Transform	DCT	Transform technique DCT Medium Steganography performance PSNR value is Medium
4	Digital Image Steganography Using Modified LSB and AES Cryptography	Spatial	LSB & AES Cryptography	Spatial Steganography High performance PSNR value High
5	Steganography Using AES and LSB Techniques	Spatial	LSB & AES Cryptography	Spatial Steganography High performance PSNR value High
6	LSB Based Image Steganography for Information Security System	Spatial	LSB Steganography	Spatial Steganography High performance PSNR value High
7	LSB Based Stegnographyto Enhance theSecurity of anImage	Spatial	LSB Steganography	Spatial Steganography High performance PSNR value High

6. CONCLUSIONS & RECOMMENDATIONS

Cryptography is used to ensure that the contents of a message are confidentiality transmitted and would not be altered. Confidentiality means no one can apprehend the acquired message besides the only that has the decipher key, and "records can't be modified" method the authentic records would not be changed or modified. This studies expands at the notion of the a brand new image Steganography scheme is proposed in this paper. In this paper, the principal importance is given at the secrecy as well as the privateers of information. The proposed technique provides better safety and may guard the message from stego image. The embedding technique is hidden underneath the DWT transformation of the quilt photograph. This paper also includes the overview of the way to cover photo and smart grid assault. Further to triumph over the attack cryptography and steganography set of rules and proposed a new algorithm to cover an image and additionally talk the smart grid and clever grid attack.

REFERENCES

[1] Abbasinezhad-Mood, D., & Nikooghadam, M. (2018). Design of an enhanced message authentication scheme for smart grid and its performance analysis on an ARM Cortex-M3 microcontroller. Journal of information security and applications, 40, 9-19.

[2] Abdalzaher, M. S., Fouda, M. M., & Ibrahem, M. I. (2022). Data privacy preservation and security in smart metering systems. Energies, 15(19), 7419.

[3] Asghar, M. R., Dán, G., Miorandi, D., & Chlamtac, I. (2017). Smart meter data privacy: A survey. IEEE Communications Surveys & Tutorials, 19(4), 2820-2835.

[4] Dong, R., Hao, S., Yang, T. H., Tang, Z., Yan, Y., & Chen, J. (2021, November). Recent Advances in Smart Meter: Data Analysis, Privacy Preservation and Applications. In International Conference on Big Data and Security (pp. 105-114). Singapore: Springer Singapore.

[5] Ferrag, M. A., Maglaras, L. A., Janicke, H., Jiang, J., & Shu, L. (2018). A systematic review of data protection and privacy preservation schemes for smart grid communications. Sustainable cities and society, 38, 806-835]

[6] Hossain, M. B., Natgunanathan, I., Xiang, Y., Yang, L. X., & Huang, G. (2019). Enhanced smart meter privacy protection using rechargeable batteries. IEEE Internet of Things Journal, 6(4), 7079-7092.

[7] Hossain, M. B., Natgunanathan, I., Xiang, Y., & Zhang, Y. (2021). Cost-Friendly differential privacy of smart meters using energy storage and harvesting devices. IEEE Transactions on Services Computing, 15(5), 2648-2657.

[8] Husain, S., & Shivani, K. (2018). A study of properties of soft set and its applications. International Research Journal of Engineering and Technology (IRJET), 5(01), 2395-0056.

[9] Husain, S., Kumari, A., & Tyagi, V. K. (2022). An Approach to Group Decision Problems Using Fuzzy-soft-set Theory and Lambda Cuts. International Journal of Early Childhood Special Education (INT-JECSE), Vol 14, Issue 08.

[10] Husain, S., Tyagi, V. K., & Gupta, M. K. (2022). A Fuzzy Soft Set-Theoretic New Methodology to Solve Decision-Making Problems. In Electronic Systems and Intelligent Computing: Proceedings of ESIC 2021 (pp. 671-683). Singapore: Springer Nature Singapore.

[11] Mouachi, R., Ait-Mlouk, A., Gharnati, F., & Raoufi, M. (2017). A Choice of Symmetric Cryptographic Algorithms based on Multi-Criteria Analysis Approach for Securing Smart Grid. Indian Journal of Science and Technology, 10, 39.

[12] Natgunanathan, I., Hossain, M. B., Xiang, Y., Gao, L., Peng, D., & Li, J. (2019). Progressive average-based smart meter privacy enhancement using rechargeable batteries. IEEE Internet of Things Journal, 6(6), 9816-9828.

[13] Choudhary, S., & Panwar, C. (2014). Key based image steganography using Dwt and chaotic map. International Journal of Engineering and Management Research (IJEMR), 4(4), 94-97.

[14] Wang, Y., Chen, Q., Hong, T., & Kang, C. (2018). Review of smart meter data analytics: Applications, methodologies, and challenges. IEEE Transactions on Smart Grid, 10(3), 3125-3148.

[15] Zhu, L., Zhang, Z., Qin, Z., Weng, J., & Ren, K. (2016). Privacy protection using a rechargeable battery for energy consumption in smart grids. IEEE Network, 31(1), 59-63