Original Article
ISSN (Online): 2456-8651

International Journal of Engineering Science Technologies
September-October 2023 7(5), 80–87

IMAGE STEGANOGRAPHY USING TWO LAYER SECURITY ALGORITHMS

Shikha Choudhary [1], Shamshad Husain [2]

[1] SIET, Shobhit Institute of Engineering and Technology Deemed to be University, Meerut, U.P., India
[2] SBAS, Shobhit Institute of Engineering and Technology Deemed to be University, Meerut, U.P., India

Received 19 August 2023
Accepted 20 September 2023
Published 04 November 2023

Corresponding Author
Shikha Choudhary,
shikha@shobhituniversity.ac.in

DOI 10.29121/IJOEST.v7.i5.2023.549

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ABSTRACT

Steganography is a method used to enhance the security of messages across networks, derived from the Greek words steganos (secret) and graphic (writing). Researchers have explored image steganography, a method that uses a photo as a cover material. The modern energy grid, known as the smart grid, offers flexibility, dependability, and efficiency in power production and distribution. To protect privacy and confidentiality, a greyscale cover picture is subjected to discrete wavelet transformation (DWT), while a chaotic map is applied to the secret image. This method offers more security and can shield communication from stegoimage attacks. Additionally, a novel approach to disguise an image is presented to combat cryptography and steganography algorithms attacks.

Keywords: DWT, Security, Information Hiding, Steganography, Lightweight Algorithm, Stego Image

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. (2016) 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 & 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 & 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. (2018) 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.

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.

2. MATERIALS AND METHODS

Some of the most popular smart grid attacks are:

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.
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.
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) **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.

3. STEGANOGRAPHY

Steganography is the art and technology of writing hidden message in information besides the sender and intended recipient. Security play 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.

3.1. STEGANOGRAPHY TECHNIQUE

Figure 1

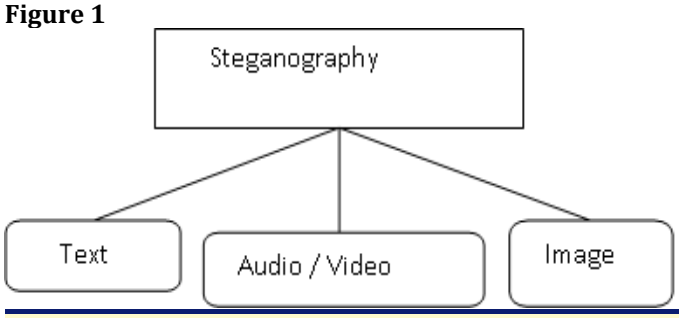

Figure 1 Steganography Techniques

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

3.2. 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.

3.3. 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.

3.4. 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 applications 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.

3.5. 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.

4. PROPOSED TECHNIQUE

Step 1-Select the quilt photo.

Step 2-Check the dimension of the cover image whether it's miles energy of 2 or no longer. If it no longer makes it electricity of 2.

Step 3-Apply Haar rework on the cover image.

Step 4-Select the secret records and divided into constant chunks of 64 bit.

Step 5-128-bit key is XOR with the chosen mystery facts.

Step 6-These two parameters are input to a light-weight encryption set of rules (PICO).

Step 7-The cowl photo.

Apply DWT to get the stego image.

Figure 2

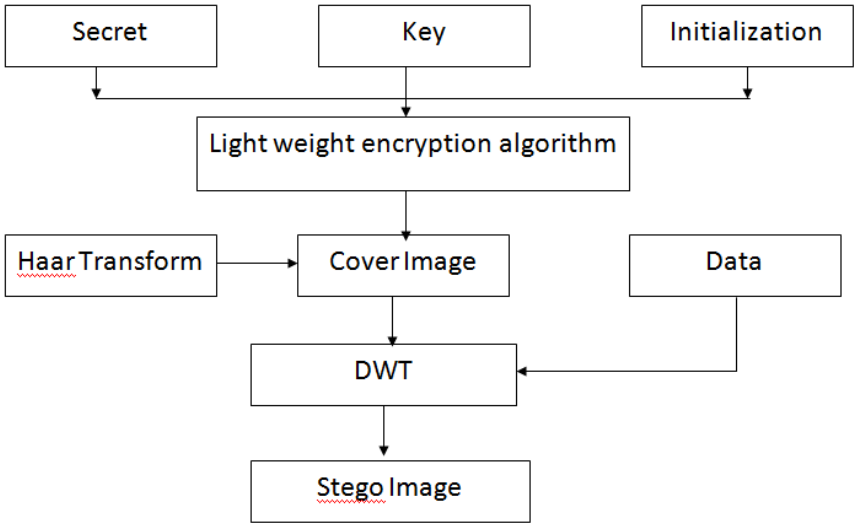

Figure 2 Block Diagram for the Proposed Technique

5. COMPARATIVE ANALYSIS FOR VARIOUS METHODS

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	Spatial	LSB & AES Cryptography	Spatial Steganography High performance PSNR value High

	Modified LSB and AES Cryptography			
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 the Security of anImage	Spatial	LSB Steganography	Spatial Steganography High performance PSNR value High

6. CONCLUSIONS AND RECOMMENDATIONS

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 privateness 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.

CONFLICT OF INTERESTS

None.

ACKNOWLEDGMENTS

None.

REFERENCES

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. https://doi.org/10.1016/j.jisa.2018.02.007.

Abdalzaher, M. S., Fouda, M. M., & Ibrahem, M. I. (2022). Data Privacy Preservation and Security in Smart Metering Systems. Energies, 15(19). https://doi.org/10.3390/en15197419.

Asghar, M. R., Dán, G., Miorandi, D., & Chlamtac, I. (2017). Smart Meter Data Privacy: A Survey. IEEE Communications Surveys & Tutorials, 19(4), 2820-2835. https://doi.org/10.1109/COMST.2017.2720195.

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.

Dong, R., Hao, S., Yang, T. H., Tang, Z., Yan, Y., & Chen, J. (2021). Recent Advances in Smart Meter : Data Analysis, Privacy Preservation and Applications. In International Conference on Big Data and Security. Singapore : Springer Singapore, 105-114. https://doi.org/10.1007/978-981-19-0852-1_8.

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. https://doi.org/10.1016/j.scs.2017.12.041.

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. https://doi.org/10.1109/TSC.2021.3081170.

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. https://doi.org/10.1109/JIOT.2019.2914135.

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.

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), 14(08). https://doi.org/10.48047/INTJECSE/V14I8.

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. Singapore : Springer Nature Singapore, 671-683.

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. https://dx.doi.org/10.17485/ijst/2017/v10i39/119856.

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. https://dx.doi.org/10.1109/JIOT.2019.2932085.

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. https://dx.doi.org/10.1109/TSG.2018.2818167.

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. https://dx.doi.org/10.1109/MNET.2016.1500292NM.