International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v10i5.5548
***Article Received**: 14 March 2022 **Revised**: 24 March 2022 **Accepted**: 25 April 2022 **Publication**: 31 May 2022*

A Study of Data Security on E-Governance using Steganographic Optimization Algorithms

Sk Anamul Hoda
Research scholar, The Department of Computer Science
The University of Burdwan, West Bengal, India
skanamulhoda@gmail.com.

Dr. Abhoy Chand Mondal
Professor, The Department of Computer Science
The University of Burdwan, West Bengal, India
abhoy_mondal@yahoo.co.in

Abstract— Steganography has been used massively in numerous fields to maintain the privacy and integrity of messages transferred via the internet. The need to secure the information has augmented with the increase in e-governance usage. The wide adoption of e-governance services also opens the doors to cybercriminals for fraudulent activities in cyberspace. To deal with these cybercrimes we need optimized and advanced steganographic techniques. Various advanced optimization techniques can be applied to steganography to obtain better results for the security of information. Various optimization techniques like particle swarm optimization and genetic algorithms with cryptography can be used to protect information for e-governance services. In this study, a comprehensive review of steganographic algorithms using optimization techniques is presented. A new perspective on using this technique to protect the information for e-governance is also presented. Deep Learning might be the area that can be used to automate the steganography process in combination with other methods.

Keywords- Cryptography; steganography; e-governance; Internet of Things.

I. INTRODUCTION

Information privacy [1] has always been a concern that affects everyone. Throughout the human history, there are plenty of examples in which methods are developed in order to keep the secrecy of sensitive information and to obstruct unauthorized people of revealing this information. In the context of this protection, steganography is becoming more and more popular among individual, researchers and governments also. Digitally transferred data can be copied without any loss of content and quality, which may lead to serious data security, authenticity, and copyright problems. Data security is crucial while governments also encouraging various e-governance [2] application through which citizens of any country can avail different services by sharing their information and it may confidential.

Nowadays, there is a plethora of applications using steganography [3] to insulate confidential information such as application on copywrite protection, authentication, etc. Steganography is the technique of concealing particulars in data of any digital format in such a way that these hidden parts are known only by sender and receiver of the data. The opposite procedure, steganalysis, can detect the existence of steganographic methods on a digital object. Nowadays, the variety of steganographic algorithms, combine with the explosive growth of tools made for steganography reasons, have initiated a hunting game of stego objects that can be found in almost everywhere. However, according to that growth, steganalysis is still in its infancies, and always one step behind steganography but it is expected to be developed equally in the nearest future. In the real-world steganography, someone can just connect to a website and download files that only appeared to be legitimate HTML or JPEG files. However, it is not always genuine as it has become effortless to copy and distribute illegal digital information which is easily created by changing file's elements in a visually imperceptible way.

Due to the variety of steganographic methods, it becomes effortless to hide a piece of information on a media without being caught. A steganalysis expert often has to have some information about the steganographic algorithm in order to detect whether there is additional information on the

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v10i5.5548
***Article Received**: 14 March 2022 **Revised**: 24 March 2022 **Accepted**: 25 April 2022 **Publication**: 31 May 2022*

examined piece of media. As a consequence, developing steganalysis, which are updated and independent of any steganographic method, has become essential. These factors allow the Steg analytic tool to resolve if a media (i.e., an image) is a stego, without any previous clue about the hidden content or the embedding method. Moreover, steganalysis should be trustworthy for a variety of steganographic techniques in order to take suitable countermeasures.

The word Steganography originates from Greek and literally means "Covered writing" because it is the art of camouflaging information without arising suspicion. It consists of a broad array of secret communication techniques that disguises the message's very existence. Drawings were also used to hide information by varying the length of a line, the colours, or other features of the picture.

A. Applications of Steganography

Steganography ranges over a broad area of applications such as advanced data structures , medical imagery where patient's record is embedded into the image providing protection of information and reducing transmission time, strong watermarks, military agencies , document tracking tools, document authentication, intelligence agencies as organizations for safe circulation of secret data , general communication, online elections and electronic money, in smart identity cards where personal details are embedded in the photograph itself for copyright control of materials, radar systems, modern printers and remote sensing.

This diverse of applications typify steganography as digital vigilance and a hot topic of study, thus its continuing evolution is guaranteed.

As it was mentioned before, armies had used steganographic techniques to communicate confidential sensitive information to their allies and troops. Also, they used steganography to store this secret data. Nowadays, it is very crucial to be protected from any data alteration and to have an access control system for digital content distribution. Nonetheless, the information about all the modern steganographic techniques and uses is kept as a valuable secret among people, due to security reasons issues. The second case is well known and mostly used in countries for their e-governance services for their citizens.

B. Optimization Techniques and Steganography

When Steganography is used with optimization techniques it is referred as adaptive domain [31] or sometimes also called as statistics aware domain. In this hybrid combination optimization techniques use statistics and meta heuristics to embed the data into the digital medium. The embedding of data is performed through changing statistical features of the cover. This process based on splitting the cover into blocks which are called best regions and sometimes referred as regions of interest (ROI). To find the best regions optimization techniques such as particle swarm optimization (PSO), ant colony optimization (ACO), and genetic algorithms are used. These methods help in enhancing the embedding process. Some researchers also use advanced methods like fuzzy logic and neural networks. While protecting the image or video data the optimization techniques increase the steganographic capacity of the method and also improves the quality of stego images.

C. Deep Learning and Steganography

Deep Learning is the subfield of machine learning. Recently deep learning [32] also considered to be a significant method applied in steganalysis. Artificial neural network (ANN) and it different variants are capable to extract the features and detect the stego images. This area is still unexplored since only few techniques like convolution neural network (CNN) is used in this domain. Deep learning can provide fast advancement of data protection, while communicating data in various e-governance applications. Since internet is helpless against various attacks and the application need to give more consideration to the security issue for availing any services. The traditional mechanism for securing the information like only encryption is not adequate, since it is very easy to break the cipher text and see the mystery correspondence exist in it by the assailant. Hence the strong combination of various methods is desired to achieve the information security.

II. METHODOLOGY

The review on the research topic is aimed to explore the related methods and techniques used to protect the information using steganographic algorithms as well as with the combination of it with other techniques. The review process involved pinpointing and exploring the research papers based on existing steganographic methods used for data security in e-governance applications. The whole process of review can be divided into various steps which are shown below in the figure 1 which illustrate all phases of our review.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v10i5.5548
***Article Received**: 14 March 2022 **Revised**: 24 March 2022 **Accepted**: 25 April 2022 **Publication**: 31 May 2022*

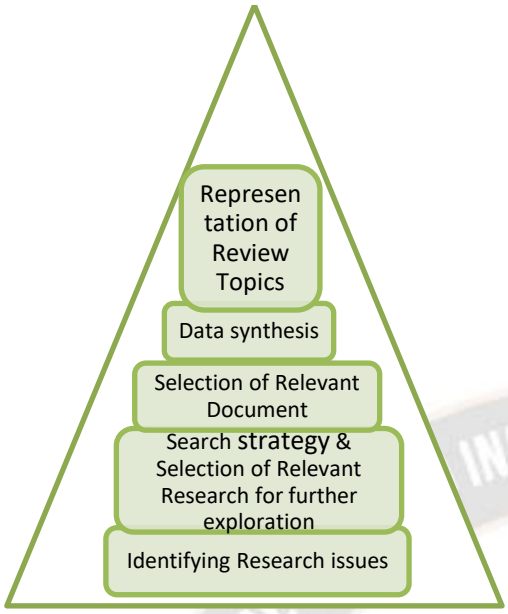

Figure 1: Review Process Hierarchy

III. LITERATURE REVIEW

With the advancement of Information and Communication Technology E-governance and M-governance has been evolved. Main concern while adoption of these services is security of information, since hackers always prone to intercept and alter the information of importance. In [2] the research study various risk factors pertaining to information security is discussed along with probable remedies. Various mechanism including cryptographic algorithms, digital watermarking and steganography can be used to hide important information in such a way that hackers may not identify the presence of hidden information.

In [4] the ancient and digital steganography meant for information hiding is depicted. various existing methods of steganography is discussed in the study. it is also mentioned that emerging techniques of steganography such as DCT, DWT and other adaptive methods are less prone to attacks. But these methods have lower payload in comparison to spatial domain techniques. a fine difference between steganography and watermarking is also described and that is to detect watermark is not required for steganography techniques.

In [5] the limitation of existing steganography methods are discussed. The study emphasizes on fusion of steganography with some advanced methods such as least significant bit (LSB) and DCT based steganography to improve the imperceptibility for the hidden information.

In [6] the study a steganography scheme has been proposed which claims efficient and effective information hiding specially in video steganography. To achieve optimal imperceptibility of hidden information genetic algorithms can be used which also helps in enhancing the base techniques. Information hiding in video can be performed efficiently through steganography. Since video is an effective tool for communication it might be used for embedding secret data. To implement effective steganographic scheme imperceptibility and video quality are two key parameters. Optimal imperceptibility of hidden data can be achieved through optimization techniques. The proposed method applied in uncompressed domain and it could be extended to compressed domain as a future direction.

According to [7] steganography has been used since long period and travelled its journey from very basic technique like LSB matching process to adopting complex artificial intelligence methods also. In e-governance using non secure channel for transferring data is risky and may cause of damage to governmental security and privacy. So important documents can be protected by applying steganography. Various steganography techniques along with their positive and negative aspects are discussed which may help to secure transaction of e-governance data.

In the research [8] authors proposed a new data hiding method using pixel value difference (PVD) steganography for digital images. This claims to be efficient than older versions of the method and it is because of using non-overlapping blocks and optimal adjustment process. The proposed method can be used to secure data transfer for e-governance.

In [9] authors discussed the importance of genetic algorithms for steganography. They also advocate for combining cryptography and steganography for highly secured data communication. The data to be transfer is first compressed and transformed into cipher text by using cryptographic algorithm. If the data is in image format, genetic algorithm can be used for pixel assortment to conceal the data.

Steganography hides [10] the secret information in the image and the purpose of it is not only hide the information but even anyone can hard to think that information is exist. In the study delivery technique using steganography is discussed and the impact various attacks is also studies.

Particle swarm optimization technique [11] in which each particles position is altered according to its neighbours' position. each iteration of the process produces velocity to direct the movement of the particle, hence can better conceal the information. it can improve the steganography system. this method may give significant coefficient to embed secret data.

In e-governance applications [12] most of the data transmitted may be in the form of images which may be confidential data. These applications may be related to healthcare, forensics, fingerprints etc. Hackers can copy, delete or alter this data for their malicious purposes. Different watermarking techniques (presented tabular summary in the

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v10i5.5548
***Article Received**: 14 March 2022 **Revised**: 24 March 2022 **Accepted**: 25 April 2022 **Publication**: 31 May 2022*

study) can be implemented to secure e-governance applications.

In [13] the authors mention that security is the main concern for the government agencies while providing e-governance services. A text steganography method is proposed with the use of cryptography. In the proposed method non- printed letters embedded as a secret text bit with the text message. The method is claimed to be efficient and improved results in implementation.

In [14] a new technique for image steganography is proposed which is also based on particle swarm optimization used to embed a secret image in spatial domain. This technique is claimed to possess a strong resistance against the steg analytic attack. While implementing the technique it shows better performance over existing techniques with little improvement requirement for PSNR and MSE value to maintain the highest level of embedding capacity.

Digital documents transferred through e-governance applications [15] more prone to vulnerability and need a strong protection. In the proposed method a block wise embedding process is introduced in which blocks of different size embedded to hide the secret digital content. Proposed method claimed to show better PSNR ratio over the existing methods.

In digital steganography the major challenges [16] are to improve hiding capacity, achieve better imperceptibility and to improve security. In the research a comprehensive study of various image steganography techniques is presented scratch from its classical to recent development. Various open challenges and future directions also discussed. One of the future directions mentioned that if steganography is combined with other techniques such as encryption, watermarking etc, it gives better results.

Medical data is very important [17] and may be confidential for individual and health industry. to protect it from fraudulent cases occurring in health sector, hybrid techniques such as encryption and steganography and genetic methods such as swarm optimization can be used. a hybrid method is proposed in the study to protect medical data and evaluated and compared with existing state of art techniques. In [18] a technique for steganography is proposed within RGB shading to achieve enhanced security. The proposed technique claimed to show improved performance with limitations such as decoration, scaling and clamor assaults.

Recently with the advancement of ICT, internet of things is emerged as providing various e-governance applications. In [19] the proposed scheme cryptography and steganography techniques are used to protect IoT information. A proposed protocol is claimed to provide better security for IoT data.

By combining Huffman encoding and particle swarm optimization [20] the performance for data hiding scheme is improved. The experimental analysis proves better performance and also make it robust against various statistical attacks.

Authors in [21] also advocate for hybrid techniques to protect data. Proposed work based on combining of steganography with various encryption techniques and optimization techniques to increase the payload capacity. It is also better to use hybrid fuzzy neural network to enhance quality of stag images. In [22] video steganography technique is proposed which is based on encryption and mapping method. Video frames are encrypted using logistic and henon mapping to improve efficiency of the security model. The method to be claimed to provide better security for video data.

In [23] a method for tuneable visual image quality in spatial domain is proposed. the proposed method is based on genetic algorithm. the concept is to model the steganography problem as a search and optimization problem. It is claimed that proposed method shown improved results for achieving high embedding capacity and also enhances the PSNR of the stego image. it is also suggested to further improve the method in terms of efficiency by utilizing metaheuristic optimization algorithm.

Data communication [24] should be secure and confidential. According to the key challenge to design steganographic system is to maintain robustness, imperceptibility and higher bit embedding rate. To achieve better security non-traditional methods like swarm intelligence algorithms.

Medical data may be transmitted [25] over the internet and the protection of patient data is proposed in by embedding ECG steganography. Proposed approach uses optimization technique i.e., Continuous ant colony optimization using discrete wavelet transform and singular value decomposition. One of the limitations of the proposed method the size of watermarked signal during the real transmission. The future research should be focused on combining steganography and data compression.

In [26] hybrid method consist of adaptive neural network and modified genetic algorithm used to conceal large amount of information into colour images. In the proposed method the number of secret bits to be replaced is non uniform and differ from one byte to another byte. The proposed intelligent method neural network and modified genetic algorithm provides strong security and improves the quality of the stego-image.

In [27] genetic algorithm (GA) and particle swarm optimization (PSO) improves the performance of steganography. The QR code used for secret message considered a new innovation in the proposed methodology. It is claimed that the proposed method maintains the quality of stego image with high embedding capacity. The performance

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v10i5.5548
***Article Received**: 14 March 2022 **Revised**: 24 March 2022 **Accepted**: 25 April 2022 **Publication**: 31 May 2022*

of proposed method can be improved by introducing few modifications in optimization process.

Smart city surveillance cameras [28] are essential for recording events for safety and security. But these collected records must also be secured. Steganography and optimization techniques can be utilized to improve the security of collected records in various smart city applications to protect them from the hackers.

To improve the security performance of steganography the pixel level's adaption may also considered instead of image level's adaption. In the proposed method [29] optimization strategy based on texture is adopted and smallest change of the image with respect to features in steganalysis is adopted. However, it considering to treat the individual image with the individual strategy to enhance the security of steganography. It might quite cumbersome technique for huge data.

Electronic voting (e-voting) can play significant role for the large countries. But the security issue is the barrier in widespread adoption of e-voting. Existing methods for managing e-voting are vulnerable to attacks and prone to manipulation by eavesdropper. In [30] the proposed method claimed for enhanced stego-cryptographic model to protect electronic voting system in poll website and apps aiming to provide better citizens participation in democratic election. However, some grey area still requires attention like security against dos (Denial of Service) attacks, multifactor authentication and validation of voters, exploring of audio steganography for wide coverage of implementing the system.

A. Sub Application areas

Internet of Things (IoT) is a domain where the transfer of huge amount of the data is taking place every moment through various applications. It is very difficult and a challenging task to secure the whole data which in transit. However, there are several methods exists which can mitigate these challenges, such as cryptography and steganography techniques and optimization techniques. IoT is in use to provide various services to citizens though e-governance applications. The information transfer through this application can be secured with the use of integrated data security techniques.

Medical image protection is very important and it requires advanced techniques which may be another application area of steganography and image watermarking.

From the literature review it is clear that hybrid solution for protecting information may give better results like Steganography and cryptography

IV. ANALYSIS OF SELECTED PAPERS

The study analyses important existing research work done during the last ten years, which are published between 2010 and 2021. The exploration aims to find research done with identifying the further research scope. Table 1 depicts the publication sources with their key synthesis.

Table 1: Salient features and Future direction from existing work

Referred Paper	Year of Publication	Salient feature	Techniques used	Application area/Domain	Future Research Direction
A. K. Singh [1]	2020	Provided a comprehensive survey on data hiding techniques including their application areas such as telemedicine, mobile devices and cyber physical systems etc., their new trends as well as their implementation challenges.	Watermarking and Encryption	Telemedicine applications	Schemes, unable to solve some issues need to be covered in future studies
Abhishek Roy et al. [2]	2011	Provides an overview of risk and remedies of the information security in various E-governance services.	Cryptographic algorithm	E-governance security	To encounter future threats advanced cryptographic techniques must be studied.
T. Patel et al., [3]	2017	Introduced Steganography with integrating cryptography for hiding file in imaage in block wise method.	Cryptography, Steganography	Information (image/text/audio/video) Security	Scalability issues are not discussed
Cheddad et al., [4]	2010	Vaious methods of steganography such as DCT, DWT is discussed a fine difference between steganography and watermarking is also described.	Watermarking, Steganography	Image security	The missuse of steganography need to be assesed.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v10i5.5548
***Article Received**: 14 March 2022 **Revised**: 24 March 2022 **Accepted**: 25 April 2022 **Publication**: 31 May 2022*

J. Mohd et al., [5]	2012	Emphasizes on fusion of steganography with some advanced methods such as Least significant bit (LSB) and DCT based steganography to improve the imperceptibility	Steganography, DCT	Image security	Issue of optimum quantization with the capaccity issue.
K. Dasgupta et al., [6]	2013	Steganography scheme is proposed for information hiding specially in video steganography to achieve optimal imperceptibility of hidden information genetic algorithms	Genetic Algorithm (GA), Steganography	Video security	Techniques are useful in uncompressed domain and it can be further extended to compressed domain also
T. Halder et al., [7]	2014	Transferring data in e-governance applications is risky and may cause of damage to govenmental security and privacy and it can be protected by applying steganography.	Steganography, Adaptive LSB	E-governance security	Usage of Steganography against threats need to be established.
T. Halder et al., [8]	2015	Data hiding method is proposed using pixel value difference (PVD) steganography for digital images	Pixel value difference, steganography	E-governance security	Idea could be used to defend E-governance documents against vulnerable attack
P. Sethi et al., [9]	2016	Importance of genetic algorithms for steganography is highlighted	Genetic algorithm, cryptography	Image security	Need to be assessed for huge data.
A. Jeyasekar et al., [10]	2016	Coding and delivery process through steganography is discussed	Steganography	Information Security	Detection technique for identifying attacks over behavioural analysis of attack at target node can be explored.
D. Hemnath et al., [11]	2016	Particle swarm optimization technique can better conceal the information and causes improvement in Steganography system.	Steganography, Particle Swam Optimization	Image security	Coputational complexity can be reduced.
C. Kumar et al., [12]	2017	Provides overview of nature of information in e-governance application	Watermarking techniques	Image security	More suitable techniques need to be identified
W. A. Alhamami et al., [13]	2018	Highligts text steganography method with the use of cryptography.	Cryptography, steganography	E-governance security	Need evaluation on different evaluation metrics
Mohsin et al., [14]	2019	Method of steganogarpahy with particle swarm optimization is proposed which used to embed a secret image in spatial domain.	Particle swarm optimization, Steganography	Image security	Improvement in PSNR and MSE value whereas maintaining the highest level of embedding capacity
T. Halder et al., [15]	2019	Blockwise embedding process is introduced for blocks of different size embedded to hide the secret digital content.	Steganography	E-governance security	Test on securing e-Governance related attachments against unauthorized attack
A. K. Sahu et al., [16]	2020	Focused on improving hiding capacity, achieve better imperceptibility and to improve security.	Steganography	Image security	Advocates for Hybrid method for information security
K. Tamilarasi et al., [17]	2020	Encryption and steganography and genetic methods such as swarm	Encryption, Particle swarm optimization	Medical Application	Encryption time needs to be reduced

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v10i5.5548
***Article Received**: 14 March 2022 **Revised**: 24 March 2022 **Accepted**: 25 April 2022 **Publication**: 31 May 2022*

		optimizatio are better to protect medical data			
S. Rehman et al., [18]	2020	Technique for steganogaphy is proposed within RGB shading to achieve enhanced security	Steganography	Image security	Have limitations such as decoration, scaling and clamor assault.
M. Khari et al., [19]	2020	Cryptography and steganography techniques are used to protect IoT information.	Cryptography, steganography	Information Security	Embedding efficiency need to be improved.
N. Sharma et al., [20]	2021	A combination of Huffman encoding and particle swarm optimization is used for improved performancee of hiding scheme	Huffman Encoding and Particle Swarm Optimization	Image security	The study does not address the exchange of a secret key between sender and receiver
S. Dhavan et al., [21]	2021	Hybrid techniques proposed with combining of steganography with various encryption techniques and optimization techniqes to increase the payload capacity.	Encryption, Particle swarm optimization	IoT Security	Need to assess under diffeent IoT protocols
J. Vivel et al., [22]	2021	Video steganography technique is proposed based on encryption and mapping method. video frames are encrypted using logistic and henon mapping to improve efficiency of the security model.	Encryption, Steganography	Video Security	Video compression need to be improved by developing further enhanced technique

Table 2: Summary of different Application areas in the review

Reference Number	**Application Area**	**Count**
1, 17, 25	Medical/Telemedicine applications	3
4, 5, 9, 11, 12, 14, 16, 18, 20, 23, 29	Image security	11
2, 7, 8, 13, 15	E-governance security	5
3, 10, 19	Information (image/text/audio) Security	3
6, 22	Video Security	2
21	IoT Security	1

From the above table, based on different combination used in proposed methods for information security, a Pi-chart has been drawn. It shows that the combination of Steganography and optimization techniques for information security in various e-governance application is popular. Similarly, the combination of Cryptography and Steganography is also extensively used. It provides the future direction and motivates to work on research gaps in hybrid methods established for information security in various e-governance application such as, healthcare, social security, banking etc.

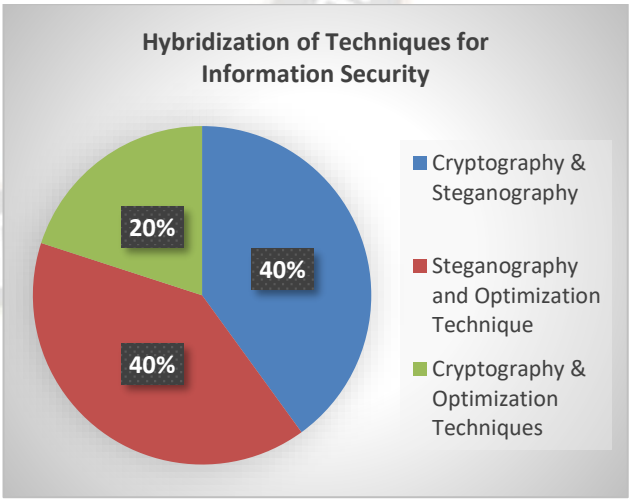

Figure 2: Combination of Techniques used for Information Security

V. Conclusion and Future Work

Steg analytics methods are used with several other methods. Variety of steganography methods are existing and can be

used to protect for different nature of information. Some steganographic methods perform well with the combination of cryptography and some with the optimization techniques. In this study an extensive survey of steganography methods and their collaboration with the other methods to improve their performance, is conducted. Steganography would be a game changer for e-governance applications where the information security is very important. With the use of steganography with some advanced techniques like optimization techniques and deep learning, the crucial information of citizens, such as healthcare data, social security data and even governments financial and defense data may be protected. A robust method need to proposed and implemented in perspective of securing the huge information transit through the e-governance applications.

ACKNOWLEDGEMENTS

This review work was supported and got technical help from the department of computer science, The University of Burdwan, West Bengal, India. We are especially thanks to Dr. Sunil Karforma the department of computer science, The University of Burdwan for his guide.

REFERENCES

[1] A. K. Singh, "Data Hiding : Current Trends , Innovation," ACM journals,vol. 16, no. 3, pp 1-16,2020.

[2] A. Roy and S. Karforma, "Risk and Remedies of E-Governance Systems," *Orient. J. Comput. Sci. Technol.*, vol. 4, no. 2, pp. 329–339, 2011.

[3] M. June, I. No, and T. J. Patel, "Available Online at www.ijarcs.info Improved Data Security using Steganography," vol. 8, no. 5, pp. 2782–2785, 2017.

[4] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," *Signal Processing*, vol. 90, no. 3, pp. 727–752, 2010, doi: 10.1016/j.sigpro.2009.08.010.

[5] B. J. Mohd, S. Abed, B. Al-Naami, and S. Alouneh, "Image steganography optimization technique," *Lect. Notes Inst. Comput. Sci. Soc. Telecommun. Eng.*, vol. 62 LNICST, pp. 205–209, 2012, doi: 10.1007/978-3-642-32573-1_35.

[6] K. Dasgupta, J. K. Mondal, and P. Dutta, "Optimized Video Steganography Using Genetic Algorithm (GA)," *Procedia Technol.*, vol. 10, pp. 131–137, 2013, doi: 10.1016/j.protcy.2013.12.345.

[7] T. Halder, S. Karforma, and R. Mandal, "E-govornence Data Security using Steganography, Concepts, Algorithms and Analysis," *Int. J. Appl. Sci. Eng.*, vol. 2, no. 1, p. 41, 2014, doi: 10.5958/2322-0465.2014.01116.2.

[8] T. Halder, S. Karforma, and R. Mandal, "A novel data hiding approach by Pixel-Value-Difference steganography and optimal adjustment to secure E-Governance documents," *Indian J. Sci. Technol.*, vol. 8, no. 16, 2015, doi: 10.17485/ijst/2015/v8i16/51269.

[9] P. Sethi and V. Kapoor, "A Proposed Novel Architecture for Information Hiding in Image Steganography by Using Genetic Algorithm and Cryptography," *Procedia Comput. Sci.*, vol. 87, pp. 61–66, 2016, doi: 10.1016/j.procs.2016.05.127.

[10] A. Jeyasekar, D. Bisht, and A. Dua, "Analysis of exploit delivery technique using steganography," *Indian J. Sci. Technol.*, vol. 9, no. 39, 2016, doi: 10.17485/ijst/2016/v9i39/102075.

[11] D. J. Hemanth, S. Umamaheswari, D. E. Popescu, and A. Naaji, "Application of Genetic Algorithm and Particle Swarm Optimization techniques for improved image steganography systems," *Open Phys.*, vol. 14, no. 1, pp. 452–462, 2016, doi: 10.1515/phys-2016-0052.

[12] C. Kumar, A. K. Singh, and P. Kumar, "A recent survey on image watermarking techniques and its application in e-governance," *Multimed. Tools Appl.*, vol. 77, no. 3, pp. 3597–3622, 2018, doi: 10.1007/s11042-017-5222-8.

[13] W. A. Alhamami, "A PROPOSED TEXT STEGANOGRAPHY METHOD TO ENHANCE E-GOVERNMENT SECURITY SYSTEMS," vol. 9, no. 05, pp. 59–64, 2018.

[14] A. H. Mohsin *et al.*, "New Method of Image Steganography Based on Particle Swarm Optimization Algorithm in Spatial Domain for High Embedding Capacity," *IEEE Access*, vol. 7, pp. 168994–169010, 2019, doi: 10.1109/ACCESS.2019.2949622.

[15] T. Halder, S. Karforma, and R. Mandal, "A block-based adaptive data hiding approach using pixel value difference and LSB substitution to secure e-Governance documents," *J. Inf. Process. Syst.*, vol. 15, no. 2, pp. 261–270, 2019, doi: 10.3745/JIPS.03.0111.

[16] A. K. Sahu and M. Sahu, "Digital image steganography and steganalysis: A journey of the past three decades," *Open Comput. Sci.*, vol. 10, no. 1, pp. 296–342, 2020, doi: 10.1515/comp-2020-0136.

[17] K. Tamilarasi and A. Jawahar, "Medical Data Security for Healthcare Applications Using Hybrid Lightweight Encryption and Swarm Optimization Algorithm," *Wirel. Pers. Commun.*, vol. 114, no. 3, pp. 1865–1886, 2020, doi: 10.1007/s11277-020-07229-x.

[18] S. Rahman *et al.*, "A novel approach of image steganography for secure communication based on LSB substitution technique," *Comput. Mater. Contin.*, vol. 64, no. 1, pp. 31–61, 2020, doi: 10.32604/CMC.2020.09186.

[19] M. Khari, A. K. Garg, A. H. Gandomi, R. Gupta, R. Patan, and B. Balusamy, "Securing Data in Internet of Things (IoT) Using Cryptography and Steganography Techniques," *IEEE Trans. Syst. Man, Cybern. Syst.*, vol. 50, no. 1, pp. 73–80, 2020, doi: 10.1109/TSMC.2019.2903785.

[20] N. Sharma and U. Batra, "An enhanced Huffman-PSO based image optimization algorithm for image steganography," *Genet. Program. Evolvable Mach.*, vol. 22, no. 2, pp. 189–205, 2021, doi: 10.1007/s10710-020-

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v10i5.5548
***Article Received**: 14 March 2022 **Revised**: 24 March 2022 **Accepted**: 25 April 2022 **Publication**: 31 May 2022*

09396-z.

[21] S. Dhawan, C. Chakraborty, J. Frnda, R. Gupta, A. K. Rana, and S. K. Pani, "SSII: Secured and high-quality steganography using intelligent hybrid optimization algorithms for IoT," *IEEE Access*, vol. 9, pp. 87563–87578, 2021, doi: 10.1109/ACCESS.2021.3089357.

[22] J. Vivek and B. Gadgay, "Video Steganography Using Chaos Encryption Algorithm with High Efficiency Video Coding for Data Hiding," *Int. J. Intell. Eng. Syst.*, vol. 14, no. 5, pp. 15–24, 2021, doi: 10.22266/ijies2021.1031.02.

[23] H. R. Kanan and B. Nazeri, "A Novel Image Steganography Scheme with High Embedding Capacity and Tunable Visual Image Quality Based on a Genetic Algorithm Steganography is knowledge and art of hiding secret data into information which is," *Expert Syst. Appl.*, 2014, doi: 10.1016/j.eswa.2014.04.022.

[24] J. N. Saeed, D. Q. Zeebaree, D. A. Zebari, D. Q. Zeebaree, J. N. Saeed, and N. A. Zebari, "Image Steganography Based on Swarm Intelligence Algorithms : A Survey Image Steganography Based on Swarm Intelligence Algorithms : A Survey."

[25] "Imperceptibility-Robustness tradeoff studies for ECG steganography using Continuous Ant Colony Optimization _ Elsevier Enhanced Reader.pdf." .

[26] N. N. El-Emam and R. A. S. Al-Zubidy, "New steganography algorithm to conceal a large amount of secret message using hybrid adaptive neural networks with modified adaptive genetic algorithm," *J. Syst. Softw.*, vol. 86, no. 6, pp. 1465–1481, 2013, doi: 10.1016/j.jss.2012.12.006.

[27] S. Uma Maheswari and D. Jude Hemanth, "Performance enhanced image steganography systems using transforms and optimization techniques," *Multimed. Tools Appl.*, vol. 76, no. 1, pp. 415–436, 2017, doi: 10.1007/s11042-015-3035-1.

[28] Y. S. Jeong and J. J. Park, "IoT and smart city technology: Challenges, opportunities, and solutions," *J. Inf. Process. Syst.*, vol. 15, no. 2, pp. 233–238, 2019, doi: 10.3745/JIPS.04.0113.

[29] X. Wu and S. Tan, "An optimization strategy for improving security in steganography," *Proc. - 2018 IEEE SmartWorld, Ubiquitous Intell. Comput. Adv. Trust. Comput. Scalable Comput. Commun. Cloud Big Data Comput. Internet People Smart City Innov. SmartWorld/UIC/ATC/ScalCom/CBDCom/IoP/SCI 2018*, pp. 1461–1466, 2018, doi: 10.1109/SmartWorld.2018.00253.

[30] O. M. Olaniyi, A. O. T. Omidiora, and E. O. Okediran, "Enhanced Stegano-Cryptographic Model for Secure Electronic Voting," *J. Inf. Eng. Appl.*, vol. 5, no. 4, pp. 1–16, 2015, [Online]. Available: www.iiste.org.

[31] D. A. Shehab and M. J. Alhaddad, "SS symmetry Comprehensive Survey of Multimedia Steganalysis :," *Symmetry 2022, MDPI*, vol. 14, no. 117, pp. 1–26, 2022.

[32] Das, Abhishek, Japsimar Singh Wahi, Mansi Anand, and Yugant Rana, "Multi-image steganography using deep neural networks." *arXiv preprint arXiv:2101.00350*, 2021.