International Journal of Informatics and Information Systems ISSN 2579-7069
Vol. 5, No. 3, September 2022, pp. 131-141

A Systematic Review on Image Data Protection Methods

Faraj Ali Faraj Alyaqobi [1,]*, Nor Adnan Bin Yahaya [2]

[1,2] School of Science and Engineering, Malaysia University of Science and Technology, Malaysia
[1,]* faraj.alyaqobi@phd.must.edu.my; [2] noradnan@must.edu.my
* corresponding author

(Received: April 12, 2022; Revised: May 12, 2022; Accepted: August 18, 2022; Available online: September 30, 2022)

Abstract

Securing data is the main goal of any data security system (DSS). Valuable data must be protected all the time and stored in a very and highly secure data storage device. This need has become more critical due to the continuous growth of data size. Furthermore, non-text data in the form of images, audios, and videos can now be transferred and processed easily and thus become part of sensitive data that need to be protected. Since there is a need to secure and protect data in any form in order to keep them private and valid, it is expected that there would be many attempts already that have been proposed in literature for this purpose. This paper reviews a group of these proposed strategies and methods that have been applied to different kinds of DSSs. Challenges and future trends of DSSs are also discussed. A number of main findings are grouped and organized as follows: (1) there are many different kinds of security techniques, each of which offers varying degrees of performance in terms of the amount of data and information that can be managed securely, (2) depending on the architecture of the proposed method, the tactics or strategies of the security system, the kinds of DSSs, as well as a few other factors, some methods are more appropriate for the storage of certain categories of data than others.

Keywords: Data Security; Information Security; Data Protection

1. Introduction

Recently, numerous data security systems (DSSs) and applications [1, 2] have been widely used to perform several tasks in regard to security, privacy, and protection [3, 4]. Smart applications are a crucial Internet of Things (IoT) applications that let consumers operate smart services online and they require security schemes. When users may remotely access a smart home system, privacy and confidentiality issues arise. Despite research on authentication techniques to increase smart home security, difficulties remain. Most present solutions concentrate on safe authentication and third-party communication without considering privacy leaks. Many protocols allow users to verify access to a wide variety of smart home gadgets, which is wasteful and unpleasant. In [3], the proposed technique uses XOR and cryptographically functions to accomplish mutual authentication with anonymity and complete forward security.

Usually, these applications send data and other digital contents. Data could be in the form of text, image, video, or audio form. Amongst these forms of data, text and image are more preferable to be shared. Recently, a lot of data/ information are shared and transferred using the Internet due to that data transfer has become faster than ever.

A huge portion of data are transferred per second, producing a huge amount of information. This also would produce a huge amount of bytes size. This phenomenon has encouraged researchers to work and focus on enhancing the way these “things” are sharing data.

As expected, many proposed systems reviewed in the literature have considered this issue. Hence, the aim of this study is to review a number of these proposed systems as well as their techniques and strategies.

This paper is organized as follows. Section 2 provides the design of the review process and explains the review method being used. Section 3 presents the key findings from the selected reviewed papers in the literature. Section 4 discusses the implications of these findings and proposes an architecture of the multi-layer DSS. Finally, Section 5 provides the conclusions and description of future work.

2. Study design

This section presents the context and research questions that are used to guide the review process.

One of the goals of data protection is to gain privacy of the data being protected. Generally, data security depends on techniques or methods that are applied to perform procedures for maintaining data to be safe from being accidentally altered, or modified in an unauthorized manner. For example, cryptographic techniques are normally used for achieving confidentiality and integrity of the CIA triad. Other techniques include using a data mask which is suitable for hiding personal information. In addition, data removal or erasure is another technique applied to protect data that had not been used for a long time. A number of these techniques are described in detail in [5-12]. Furthermore, in some cases, a combination of two methods is applied to the data system in order to strengthen the data protection procedure.

This review paper seeks to gain some insights on the status of research in image data protection methods by analysing a selected set of papers in the literature. In addition, the study also focuses on identifying the challenges and future trends in this area of research.

The following research question(s) guide the review process:

1) What are the different types of methods that have been used in the image data protection procedures in DSS?
2) What are the challenges and future trends in image data protection research?

The method used in this review process is characterized by these three important aspects: (1) keywords for selection, (2) the types of publication and indexing services from which the papers were to be extracted, (3) the period range of the selected publications.

The keywords used in the search engine to extract papers for this review are ones typically found in cybersecurity papers. These include “data systems”, “security”, “information security”, “data security systems”, “data protection”, “data encryption”, and “cryptographic strategies”.

This review paper has collected a group of papers published as journals and conference proceedings that are from SCOPUS and ISI-indexed only.

Another criterion used for selecting the papers is the publication period range, which is between 2001 and 2020. This is considered to be a good coverage period in term of publication date when most of information technologies and data systems are believed to be growing during the last two decades. The procedure applied for papers’ extraction is in detail mentioned in Table 1.

Table 1. Phases performed for extracting papers from digital libraries

Phase	Procedure performed	Result and output of phase
Initial phase	Initially there were a total of 269 papers collected from various different sources.	A screening procedure was applied two times in order to refine them.
First phase	The first screening procedure excluded those papers that are irrelevant to the keywords, have no full texts, or have duplicated document’s title.	This resulted in 118 papers being excluded.
Second phase	the second procedure has been applied on the remaining number of articles which are equal to 151. The second procedure has excluded those surveys, tutorials, and news.	The remaining of included articles have been equal to 69 where the excluded number of articles in the second phase was 82.

3. Results

This section reports the findings from the analyzed papers, organized according to how they are related to the research questions.

3.1. Disciplines and research areas where security methods have been implemented

In the literature, there have been various studies proposed to apply security methods. Those security methods are applied for a variety of purposes in many fields. As for example, a security scheme has been applied in the field of medical images with the purpose to to resist potential attacks [13]. Another study from the field of medical images proposed by [13] has used the reversible watermarking technique where the relevant information has been embedded with the image. Medical images sometimes are stored in health information systems or other storages that need to be always secure and protected. Finally, in [14], medical images as plain images have been protected by implementing a security image processing technique. This technique aims to increase privacy of the selected information system and authentication of images specifically during the decryption process.

Security of information has been considered by many research studies from the field of cloud computing such as in [15, 16]. Cloud computing resources are key assets in which a huge number of users are always sharing and transferring data thoroughly [18]. This reason and other related issues have made cloud computing a vulnerable to so many attacks and threats from unauthorized parties and sources. Therefore, it is very important to overcome related challenges faced by security schemes and algorithms which are proposed to deal with the integration, confidentiality, availability of data and information to countermeasure such attempts of threats and actions e.g., denial of service. In [15], the security scheme aims to secure shared and transferred data as well as to services being requested by users. The security scheme aims by then to increase protection of data by taking the consideration of data integrity.

Besides, Internet of Things (IoT) is another essential field that has been paid much attention by researchers [17-19] in order to maintain its resources, systems, information, and other assets confidential and protected. The authentication procedure has been considered widely for many IoT related systems such as those systems which require authentication via a remote environment for internet banking systems [20]. There is a need to authenticate users using a strong security mechanism. Such an authentication is an essential security procedure for user's data protection from being cloned while IoT-based services are performed.

Security of information systems has been studied very extensively by many researches from the field of nano-communication [21], where it is a very important to consider nano-communication security by protecting those systems from being manipulated, modified, altered by harmful threats. Related security systems have considered both nano-networking and sensor networks to be protected.

In addition, there are several studies concerning the security of mobile communication systems to increase the safety of users, data, shared information [22]. There are further security procedures that trace mobile users and terminals in order to close such open ports and untrusted environments. Related security methods for the field of mobile computing to initialize a reliable security infrastructure in order to keep respective users, resources, terminals, and important resources in a private environment and to allow them interact in-between each other and operate securely [23]. Also, mobile computing related security methods focus on making middleware safe and unthreatened so that information systems and users can be protected.

The reviewed literature has shown that there are a number of methods and techniques applied for DSS-related protection purposes. In the next sections, we shall provide numerous examples of these strategies that are found in the literature.

3.2. DSS-applied watermarking techniques

In the medical images field, many researchers have designed and proposed a number of security methods. For example, in [24], authors have applied a watermarking scheme applied on medical images and health information systems where such a method is proposed to increase security of medical images as well as authentication. Besides, a transformation process has been applied to images for achieving stronger security [25, 26]. It is mentioned that authentication and security scheme applied to such types of images can secure images against many types of attacks. Furthermore, , the use of transformation-based watermarking to secure medical images and patients' records and information is analyzed in [27] with examples of embedding image hiding technique into an image scheme can be

found in [28-32]. This is also called steganography [33-39] by which a certain amount of information can be hidden [40, 41]. For the purpose of hiding a medical image, one of the techniques is to embed an image to another. Precisely, the secret image can be inserted to the normal or cover image.

Usually, this procedure can be followed by a transformation procedure in order to scramble the image, i.e., secret image or information aimed to be protected. The paper [42] mentions that safeguarding the originality and authenticity of medical images is crucial. Two approaches, reversible watermarking and region-of-interest (ROI) lossless watermarking, are primarily devoted to solving these problems. However, the former raises security issues by segmenting images geographically for watermark embedding. The latter falls short in safeguarding images against manipulation by not providing a reliable recovery option for the altered regions. In response to these problems, this work proposes a revolutionary resilient reversible watermarking approach. To eliminate potential for error in diagnosis, we propose a methodology that employs a reversible watermarking technique. To further safeguard picture originality, the procedure is integrated with singular value decomposition. In addition, for watermark creation, regions being processed are separated so that an efficient recovery mechanism may be designed even with limited embedding capacity. Finally, watermarks are included into whole medical pictures to eliminate the dangers associated with spatial image segmentation. Experiments show that with this proposed lossless plan outperforms prior art methods for protecting medical images in a variety of respects, including in terms of its remarkable indiscernibility and sufficient robustness, as well as its provision of reliable verification and recovery functions.

In [43], two security methods have been used which are watermarking and encryption in order to increase security and protection of medical images. natural images have been considered to be original images and medical images taken as watermark images. Then, medical images will be embedded with the natural images. Then, an encryption scheme has been applied to this mixture using different encryption algorithms. In [14], encryption and watermarking have been the security technique used to be reversibly carried out so that the original image can be readable in the decryption party.

The applied security scheme in [15] has used a public key based authenticator with randomly performed masks. In [17], the security method has focused on detecting vulnerabilities at devices in order to increase security of embedded security devices.

3.3. DSS-applied cryptographic techniques

Cryptographic methods are proposed to be effective and applicable with nano-communication and its related sensor networks as proposed by [36]. Additionally, in the field of mobile communication [37], it is proposed that the use of cryptographic technique with a digital proxy signature security scheme might be able to produce more computation power than other competitive security schemes. Also, cryptographic methods have been used in medical images and information systems to ensure reliability and authentication of systems. In [58], a cryptographic algorithm to perform authentication procedure is implemented and applied to health information system. The proposed algorithm aims to secure data and records of patients and protect the system in term of integrity.

Securing images using cryptographic techniques can be an alternative solution to securing by identifying features and other related properties such as biometrics [44]. Even then securing the associated images are also of concern to researchers. In [45], a visual cryptographic technique is proposed to secure images and its integrated information. The proposed visual cryptographic scheme is aimed to enhance security of information where additional parameters are used to increase security with more reliability.

Another visual cryptography scheme has been applied to color images. In this proposed scheme [46], details of images are expanded. The security scheme aims to make colors have similar contrasts. That means, regions and details inside the image are similar and therefore details and edges will not be obvious easily. Thus, this leads to increase security of images.

Cryptographic algorithms are also used to support image protection mechanism that hide their information by embedding more than an image [47]. For example, in [48], encryption is applied on images to produce distorted forms which subsequently can only be decrypted through certain known cryptographic secret. The proposed security

method uses a double random phase cryptography procedure. In addition, an asymmetric encryption procedure has also been used after that in order to allocate initial values and system parameters.

For an effective security method related to the field of mobile computing, it is proposed by [23] to use an agent technology middleware. This security technology can be supported if a reliably prepared security infrastructure is used when such a standard cryptographic mechanism can be exploited to increase the security level of mobile computing related components [49] such as users, database, terminals, and communication medium.

An effective way to protect digital images and keep them secure is to use sometimes images' encryption. A 2D chaotic system has been designed in [50] in order to produce several 2D chaotic maps. This way can produce complex chaotic forms. An image encryption algorithm has been designed and the original image will be scrambled by using the chaotic sequences. This procedure is followed by a transformation. The scrambled image is confused and diffused by the chaotic sequences. It is mentioned by [50], the performance of the proposed encryption algorithm can be reliable.

Nowadays, encryption of image based on chaos is considered a secure choice in communications. The proposed security scheme in [51] depends mainly on the use of a logic based operation, that is, a bit-pair of XOR operation. It also aims to increase the form of the diffusion with pixel level XOR operator from the bottom to the top and from the right corner to the left corner. Authors in [51] have mentioned that the pair level encryption utilizing logic operation can significantly increase the security and encryption effectiveness. A chaotic random series for the encryption has been obtained using chaotic maps. It is reported that this scheme is robust and can resist a set of attacks.

One of the other security methods in addition to the image encryption procedure is to use an image compression process following the security scheme so that size of images will be significantly reduced [52]. This security procedure maintains the assurance of contents. To use the symmetric encryption scheme, keys are generated for both encryption and decryption terminals [53].

Security images related methods are aimed to safe contents and information with the confidentiality of digital images. Additionally, these security methods are attempting to protect images from being unavailable either temporarily or permanently such as denial of service or service interrupt. In [54], a security scheme is proposed to enable a safe sharing of their contents. The proposed method has utilized the asymmetric encryption algorithms. This scheme shall increase the complexity in term of computation for security purposes so that it can securely reconstruct pieces of data in different sources and data storages. The security of this scheme confirms its confidentiality for securely shared images. The proposed method has also utilized the steganography method to add a cover for a more security purpose. The proposed method in total has also confirmed it is suitable to resist against cryptanalysis related methods.

3.4 DSS-applied integrity techniques

Integrity of data and digital contents is very essential specifically for images that contain sensitive details such as medical images. For data integrity, in [55], a steganography technique is proposed to consider the issue of data integrity. For the integrity security objective, and in order to be securely achieved, the hashing algorithm has been used so that variables will be integrated once the integrity procedure has been performed.

Images being transferred through cloud platforms have been paid a lot of attention in order to ensure they are stored, transferred, and managed in a secure manner. Such security schemes considering cloud images need to take into account a set of characteristics of cloud images. Thus, a real-time integrity verification scheme has been proposed and designed in [56]. For example, the authentication and integrity of data during generating, storing, and transferring processes should be carefully considered. Besides, providers of services are another security issue, in this setting, due to that such mis-behaviorally performed actions and threats might happen thorough. The proposed security scheme has utilized an adaptive reversible watermarking algorithm. So, the hiding information and images can be embedded and therefore data used for authentication procedure will also be hidden using the watermarking technique. The proposed method has established a protocol so that potential performance can do resist against attacks and privacy of digital contents of images could be achieved.

3.5 Challenges faced by DSSs

This subsection discusses a number of challenges DSS might face towards achievement of highly secure performance.

There are a number of reported challenges faced by DSS in order to achieve a very highly advanced level of security for a wide range of applications. One of these challenges, the exponential increase in terms of amount of information. This increase has made the security task more difficult due to the huge number of sizes of processed information and stored data.

Besides, a huge amount of data required a huge space assigned for storage. This requires a computation-efficient strategy that can be powerful to address such a very huge number of bytes.

In addition, availability of huge amount of data will be certainly vulnerable to many attacks and potential threats.

Researches in the reviewed papers that have been conducted within the realm of cloud computing, such as [15, 16], have also considered the issue of information security. Hence, cloud computing is very susceptible to a wide variety of assaults and dangers posed by untrusted third parties and sources as a result of this reason and other related problems. For this reason, it is of the utmost importance to overcome the related challenges faced by security schemes and algorithms that have been proposed to deal with the integration, confidentiality, and availability of data and information in order to countermeasure such attempts of threats and actions such as denial of service. According to [15], the purpose of the security system is to protect not only the data that is being shared and moved but also the services that users are requesting but also to improve the level of protection afforded to data by taking into account the data's integrity [57].

3.6 Future of DSSs

The application of security strategies and techniques to DSS will continue to grow in term of the management of the information size. In addition, there will be a number of data-related systems specifically those which include sensitive data and information such as smart IoT and cloud computing dependent applications. Finally, data systems that rely on open source and online platforms such as Software-as-a-service (SaaS) and Platform-as-a-Service (PaaS) are expected to be a major focus of DSS in the future where many security strategies and several security measures will be implemented to safeguard data associated with these types of systems.

4. Discussion

This paper has reviewed a number of methods collected from literature to provide some insights on the application of security and protection strategies to data and information related to DSSs, in particular, image data. Different types of security methods have varied levels of performance in terms of security strength and data management. Some methods are more suitable to certain types of data depending on the design of the proposed method, techniques or strategies of the security scheme, types of DSSs, and a few others. Preferably, there should be security strategies applicable to varied types of DSSs in order to achieve overall high level of security. The insights that we have uncovered in the course of this review serve as the basis for deriving a conceptual model for guiding the development of multi-layer DSSs

Security of information concerns two related issues which are the protection of information and reducing potential risks by preventing such a potential action which attempts to cause hazards to information [58, 59]. Sometimes, information security aims to reduce unauthorized access to information resources. Security of information is the process that guarantees a safe arrival of information to the destination with no disclosure of any part belongs to information being protected [60]. This procedure aims to achieve a high level of the confidentiality, the integrity, as well as the availability [61]. This idea leads to the conceptualization of the security mechanism that is represented in Figure 1 below.

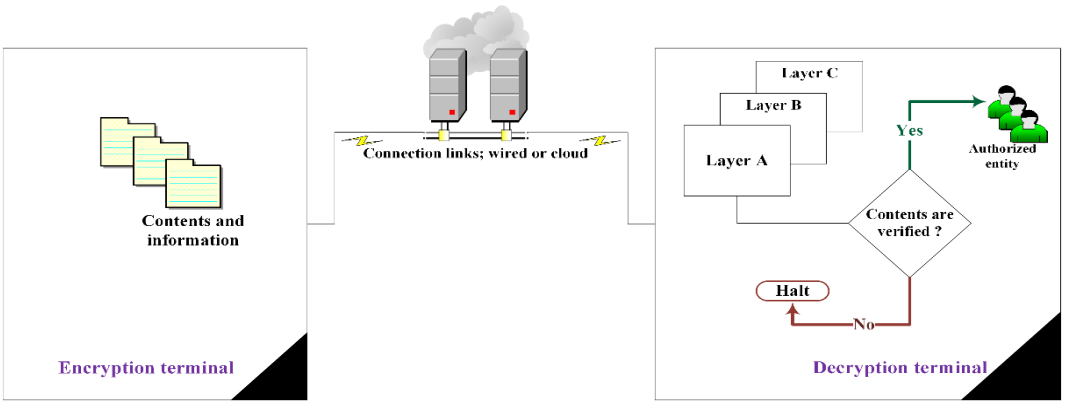

Figure 1. A graphical representation of multi-layer DSS

Information security has applied several procedures for multi-layer DSS to help perform information protection. Verification of information received, as for example, is one of these procedures. In addition, it applies monitoring for information associated activities that might happen attempting to modify or change original contents.

One of the most critical issues that information security continuously tries to overcome or encounter is the handling of threats or unusual actions. In information security, there exist a lot number of threats or actions that behave in a non-authorized manner by which an explicit harmful can be caused to information. Security that is either for data or other contents, applies different kinds of countermeasures in order to prevent/reduce caused loss of information. Sometimes, it applies safeguards to block threats. Usually, threats try to access to information through vulnerabilities. Therefore, one of the measures to prevent threats is to eliminate those vulnerabilities [62, 63].

There are many definitions of security found in the literature. Some are summarized as follows:

One of the best definitions describes security in the form of three objectives [64-66]. In a nutshell information security is the protection of data and information against any disclosure or leak to unauthorized party, any improper changing or modification, and also preventing any unauthorized access to contents of information at any time.

In the literature, there are several studies proposed to achieve information security. One of the examples is to detect the attack which causes the disclosure, modification, and/ or unavailability of information or parts of its contents. In this procedure, it is also important to apply a detection technique that could efficiently and accurately finds out vulnerabilities of information being protected [67].

Another example might be a procedure preventing information from being discoverable or shared with unauthorized parties. Prevention of threats is an important procedure that can keep information secure and protected [68, 69].

In addition, vulnerabilities are considered to be blocked strictly. Usually, this procedure is necessary once the detection is done. Vulnerabilities are open ports that can be exploited by threats by which unusual actions very probably might occur.

5. Conclusions and Future Work

This paper has reviewed a number of methods collected from the literature to provide some insights on the security and protection strategies applied to data and information related to DSSs. In particular, the review has focused on methods for protecting image data. The insights have motivated the investigation towards having more robust DSSs such as being supported by multi-layer encryption mechanism.

References

[1] H. A. Khattak, H. Farman, B. Jan, and I. U. Din, "Toward Integrating Vehicular Clouds with IoT for Smart City Services," *IEEE Network,* vol. 33, no. 2, pp. 65-71, 2019, doi: 10.1109/MNET.2019.1800236.

[2] W. Meng, "Intrusion Detection in the Era of IoT: Building Trust via Traffic Filtering and Sampling," *Computer,* vol. 51, no. 7, pp. 36-43, 2018, doi: 10.1109/MC.2018.3011034.

[3] Q. Lyu, N. Zheng, H. Liu, C. Gao, S. Chen, and J. Liu, "Remotely Access “My” Smart Home in Private: An Anti-Tracking Authentication and Key Agreement Scheme," *IEEE Access,* vol. 7, pp. 41835-41851, 2019, doi: 10.1109/ACCESS.2019.2907602.

[4] W. K. A. Hasan, A. Alraddad, A. Ashour, Y. Ran, M. A. Alkelsh, and R. A. M. Ajele, "Design and Implementation Smart Transformer based on IoT," in *2019 International Conference on Computing, Electronics & Communications Engineering (iCCECE)*, 22-23 Aug. 2019 2019, pp. 16-21, doi: 10.1109/iCCECE46942.2019.8941980.

[5] K. K. Raghuvanshi, S. Kumar, and S. Kumar, "A data encryption model based on intertwining logistic map," *Journal of Information Security and Applications,* vol. 55, p. 102622, 2020/12/01/ 2020, doi: https://doi.org/10.1016/j.jisa.2020.102622.

[6] L. Guo, H. Xie, and Y. Li, "Data encryption based blockchain and privacy preserving mechanisms towards big data," *Journal of Visual Communication and Image Representation,* vol. 70, p. 102741, 2020/07/01/ 2020, doi: https://doi.org/10.1016/j.jvcir.2019.102741.

[7] V. Anjaiah Gujjary and A. Saxena, "A neural network approach for data masking," *Neurocomputing,* vol. 74, no. 9, pp. 1497-1501, 2011/04/01/ 2011, doi: https://doi.org/10.1016/j.neucom.2011.01.002.

[8] G. Qiu, X. Gui, and Y. Zhao, "Privacy-Preserving Linear Regression on Distributed Data by Homomorphic Encryption and Data Masking," *IEEE Access,* vol. 8, pp. 107601-107613, 2020, doi: 10.1109/ACCESS.2020.3000764.

[9] O. Ali-Ozkan and A. Ouda, "Key-based Reversible Data Masking for Business Intelligence Healthcare Analytics Platforms," in *2019 International Symposium on Networks, Computers and Communications (ISNCC)*, 18-20 June 2019 2019, pp. 1-6, doi: 10.1109/ISNCC.2019.8909125.

[10] S. I. Tomashevich and A. O. Belyavsky, "Navigation data transfer in a quadrotor formation via a binary communication channel with adaptive coding and data erasure," in *2017 24th Saint Petersburg International Conference on Integrated Navigation Systems (ICINS)*, 29-31 May 2017 2017, pp. 1-3, doi: 10.23919/ICINS.2017.7995569.

[11] S. Sarkar, J. Banatre, L. Rilling, and C. Morin, "Towards Enforcement of the EU GDPR: Enabling Data Erasure," in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 30 July-3 Aug. 2018 2018, pp. 222-229, doi: 10.1109/Cybermatics_2018.2018.00067.

[12] W. K. A. Hasan, A. M. Abood, and M. Habbal, "A Review of Blockchain-based on IoT applications (challenges and future research directions)," in *2020 5th International Conference on Innovative Technologies in Intelligent Systems and Industrial Applications (CITISIA)*, 25-27 Nov. 2020 2020, pp. 1-7, doi: 10.1109/CITISIA50690.2020.9371814.

[13] A. Umamageswari, M. F. Ukrit, and G. Suresh, "A survey on security in medical image communication," *International Journal of Computer Applications,* vol. 30, no. 3, pp. 41-45, 2011.

[14] Q. Kester, L. Nana, A. C. Pascu, S. Gire, J. M. Eghan, and N. N. Quaynor, "A Security Technique for Authentication and Security of Medical Images in Health Information Systems," in *2015 15th International Conference on Computational Science and Its Applications*, 22-25 June 2015 2015, pp. 8-13, doi: 10.1109/ICCSA.2015.8.

[15] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," in *2010 Proceedings IEEE INFOCOM*, 14-19 March 2010 2010, pp. 1-9, doi: 10.1109/INFCOM.2010.5462173.

[16] S. Ramgovind, M. M. Eloff, and E. Smith, "The management of security in Cloud computing," in *2010 Information Security for South Africa*, 2-4 Aug. 2010 2010, pp. 1-7, doi: 10.1109/ISSA.2010.5588290.

[17] A. Ukil, J. Sen, and S. Koilakonda, "Embedded security for Internet of Things," in *2011 2nd National Conference on Emerging Trends and Applications in Computer Science*, 4-5 March 2011 2011, pp. 1-6, doi: 10.1109/NCETACS.2011.5751382.

[18] A. Mosenia and N. K. Jha, "A Comprehensive Study of Security of Internet-of-Things," *IEEE Transactions on Emerging Topics in Computing,* vol. 5, no. 4, pp. 586-602, 2017, doi: 10.1109/TETC.2016.2606384.

[19] W. K. A. Hasan, Y. Ran, J. Agbinya, and G. Tian, "A Survey of Energy Efficient IoT Network in Cloud Environment," in *2019 Cybersecurity and Cyberforensics Conference (CCC)*, 8-9 May 2019 2019, pp. 13-21, doi: 10.1109/CCC.2019.00-15.

[20] D. Hutchinson and M. Warren, "Security for Internet banking: a framework," *Logistics Information Management,* vol. 16, no. 1, pp. 64-73, 2003, doi: 10.1108/09576050310453750.

[21] F. Dressler and F. Kargl, "Towards security in nano-communication: Challenges and opportunities," *Nano Communication Networks,* vol. 3, no. 3, pp. 151-160, 2012/09/01/ 2012, doi: https://doi.org/10.1016/j.nancom.2012.08.001.

[22] H.-U. Park and I.-Y. Lee, "A Digital Nominative Proxy Signature Scheme for Mobile Communication," in *Information and Communications Security*, Berlin, Heidelberg, S. Qing, T. Okamoto, and J. Zhou, Eds., 2001// 2001: Springer Berlin Heidelberg, pp. 451-455.

[23] S. Yoon and J. Kim, "Remote security management server for IoT devices," in *2017 International Conference on Information and Communication Technology Convergence (ICTC)*, 18-20 Oct. 2017 2017, pp. 1162-1164, doi: 10.1109/ICTC.2017.8190885.

[24] A. Shehab *et al.*, "Secure and Robust Fragile Watermarking Scheme for Medical Images," *IEEE Access,* vol. 6, pp. 10269-10278, 2018, doi: 10.1109/ACCESS.2018.2799240.

[25] U. A. Bhatti *et al.*, "Hybrid watermarking algorithm using Clifford Algebra with Arnold Scrambling and Chaotic Encryption," *IEEE Access,* pp. 1-1, 2020, doi: 10.1109/ACCESS.2020.2988298.

[26] W. Kaswidjanti, H. Himawan, A. O. M. Dewi, M. Y. Florestiyanto, and R. I. Perwira, "Arnold Transformed Position Power First Mapping (AT-PPFM) for Secret Digital Image," in *2019 5th International Conference on Science in Information Technology (ICSITech)*, 23-24 Oct. 2019 2019, pp. 241-245, doi: 10.1109/ICSITech46713.2019.8987521.

[27] T. S. Reddy, D. S. Reddy, A. N. Nihar, M. S. Sumanth, and J. Anitha, "Comparitive Analysis on Transformation based Watermarking," in *2019 2nd International Conference on Signal Processing and Communication (ICSPC)*, 29-30 March 2019 2019, pp. 356-360, doi: 10.1109/ICSPC46172.2019.8976716.

[28] T. Lu, J. Shen, and T. Chang, "Effective Dual-images based Reversible Information Hiding Scheme based on Complexity Analysis and Thresholds Controlling," in *2019 IEEE 10th International Conference on Awareness Science and Technology (iCAST)*, 23-25 Oct. 2019 2019, pp. 1-4, doi: 10.1109/ICAwST.2019.8923492.

[29] G. Indramohan and K. R. Naidu, "A Hybrid Reversible Image Data Hiding Scheme With Symmetric Key Cryptography," in *2019 9th International Conference on Advances in Computing and Communication (ICACC)*, 6-8 Nov. 2019 2019, pp. 278-282, doi: 10.1109/ICACC48162.2019.8986203.

[30] D. Hou, W. Zhang, K. Chen, S. Lin, and N. Yu, "Reversible Data Hiding in Color Image With Grayscale Invariance," *IEEE Transactions on Circuits and Systems for Video Technology,* vol. 29, no. 2, pp. 363-374, 2019, doi: 10.1109/TCSVT.2018.2803303.

[31] M. A. Wahed, H. Nyeem, and M. F. Elahi, "An Improved Interpolation based Reversible Data Hiding for Medical Images," in *2019 International Conference on Electrical, Computer and Communication Engineering (ECCE)*, 7-9 Feb. 2019 2019, pp. 1-6, doi: 10.1109/ECACE.2019.8679278.

[32] K. Chi, "Improvement of the Bit Plane Truncation Image Scheme for Reversible Data Hiding," in *2019 IEEE International Conference on Consumer Electronics - Taiwan (ICCE-TW)*, 20-22 May 2019 2019, pp. 1-2, doi: 10.1109/ICCE-TW46550.2019.8991927.

[33] C. Maiti, D. Baksi, I. Zamider, P. Gorai, and D. R. Kisku, "Data Hiding in Images Using Some Efficient Steganography Techniques," in *Signal Processing, Image Processing and Pattern Recognition*, Berlin, Heidelberg, T.-h. Kim, H. Adeli, C. Ramos, and B.-H. Kang, Eds., 2011// 2011: Springer Berlin Heidelberg, pp. 195-203.

[34] A. Habibi Lashkari, A. Abdul Manaf, M. Masrom, and S. Mohd Daud, "A Survey on Image Steganography Algorithms and Evaluation," Berlin, Heidelberg, 2011: Springer Berlin Heidelberg, in Digital Information Processing and Communications, pp. 406-418.

[35] A. Rehman, T. Saba, T. Mahmood, Z. Mehmood, M. Shah, and A. Anjum, "Data hiding technique in steganography for information security using number theory," *Journal of Information Science,* vol. 45, no. 6, pp. 767-778, 2019, doi: 10.1177/0165551518816303.

[36] R. Bhardwaj and V. Sharma, "Image Steganography Based on Complemented Message and Inverted Bit LSB Substitution," *Procedia Computer Science,* vol. 93, pp. 832-838, 2016/01/01/ 2016, doi: https://doi.org/10.1016/j.procs.2016.07.245.

[37] S. Mukherjee, S. Roy, and G. Sanyal, "Image Steganography Using Mid Position Value Technique," *Procedia Computer Science,* vol. 132, pp. 461-468, 2018/01/01/ 2018, doi: https://doi.org/10.1016/j.procs.2018.05.160.

[38] J. K. Sadié, L. M. Metcheka, and R. Ndoundam, "A high capacity text steganography scheme based on permutation and color coding," *arXiv preprint arXiv:2004.00948,* 2020.

[39] S. Agarwal and S. Venkatraman, "Deep Residual Neural Networks for Image in Speech Steganography," *arXiv preprint arXiv:2003.13217,* 2020.

[40] M. A. Hajjaji, M. Gafsi, and A. Mtibaa, "Discrete Cosine Transform Space for Hiding Patient Information in the Medical Images," in *2019 IEEE International Conference on Design & Test of Integrated Micro & Nano-Systems (DTS)*, 28 April-1 May 2019 2019, pp. 1-6, doi: 10.1109/DTSS.2019.8914880.

[41] Y. Yang, X. Xiao, X. Cai, and W. Zhang, "A Secure and High Visual-Quality Framework for Medical Images by Contrast-Enhancement Reversible Data Hiding and Homomorphic Encryption," *IEEE Access,* vol. 7, pp. 96900-96911, 2019, doi: 10.1109/ACCESS.2019.2929298.

[42] X. Liu *et al.*, "A Novel Robust Reversible Watermarking Scheme for Protecting Authenticity and Integrity of Medical Images," *IEEE Access,* vol. 7, pp. 76580-76598, 2019, doi: 10.1109/ACCESS.2019.2921894.

[43] A. Kannammal and S. Subha Rani, "Two level security for medical images using watermarking/encryption algorithms," *International Journal of Imaging Systems and Technology,* vol. 24, no. 1, pp. 111-120, 2014, doi: 10.1002/ima.22086.

[44] M. R. Ogiela and L. Ogiela, "Cognitive cryptography techniques for intelligent information management," *International Journal of Information Management,* vol. 40, pp. 21-27, 2018/06/01/ 2018, doi: https://doi.org/10.1016/j.ijinfomgt.2018.01.011.

[45] J. Tripathi, A. Saini, Kishan, Nikhil, and Shazad, "Enhanced Visual Cryptography: An Augmented Model for Image Security," *Procedia Computer Science,* vol. 167, pp. 323-333, 2020/01/01/ 2020, doi: https://doi.org/10.1016/j.procs.2020.03.232.

[46] X. Wu and C.-N. Yang, "Probabilistic color visual cryptography schemes for black and white secret images," *Journal of Visual Communication and Image Representation,* p. 102793, 2020/03/11/ 2020, doi: https://doi.org/10.1016/j.jvcir.2020.102793.

[47] Y. Chen, T. Hung, S. Hsieh, and C. Shiu, "A New Reversible Data Hiding in Encrypted Image Based on Multi-Secret Sharing and Lightweight Cryptographic Algorithms," *IEEE Transactions on Information Forensics and Security,* vol. 14, no. 12, pp. 3332-3343, 2019, doi: 10.1109/TIFS.2019.2914557.

[48] Y. Liu, Z. Jiang, X. Xu, F. Zhang, and J. Xu, "Optical image encryption algorithm based on hyper-chaos and public-key cryptography," *Optics & Laser Technology,* vol. 127, p. 106171, 2020/07/01/ 2020, doi: https://doi.org/10.1016/j.optlastec.2020.106171.

[49] J. Li and Q. Zhang, "Design and implement of mobile internet security middleware," in *2013 6th International Conference on Information Management, Innovation Management and Industrial Engineering*, 23-24 Nov. 2013 2013, vol. 2, pp. 150-153, doi: 10.1109/ICIII.2013.6703106.

[50] H. Huang, S. Yang, and R. Ye, "Efficient symmetric image encryption by using a novel 2D chaotic system," *IET Image Processing*, vol. 14, no. 6, pp. 1157-1163. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ipr.2019.0551

[51] R. Ge, G. Yang, J. Wu, Y. Chen, G. Coatrieux, and L. Luo, "A Novel Chaos-Based Symmetric Image Encryption Using Bit-Pair Level Process," *IEEE Access,* vol. 7, pp. 99470-99480, 2019, doi: 10.1109/ACCESS.2019.2927415.

[52] P. Mathur, A. Yadav, V. K. Verma, and R. Purohit, "Paradigms of Image Compression and Encryption: A Review," in *2019 2nd International Conference on Intelligent Communication and Computational Techniques (ICCT)*, 28-29 Sept. 2019 2019, pp. 313-317, doi: 10.1109/ICCT46177.2019.8969039.

[53] N. A. Advani and A. M. Gonsai, "Performance Analysis of Symmetric Encryption Algorithms for their Encryption and Decryption Time," in *2019 6th International Conference on Computing for Sustainable Global Development (INDIACom)*, 13-15 March 2019 2019, pp. 359-362.

[54] A. M. Ahmadian and M. Amirmazlaghani, "A novel secret image sharing with steganography scheme utilizing Optimal Asymmetric Encryption Padding and Information Dispersal Algorithms," *Signal Processing: Image Communication,* vol. 74, pp. 78-88, 2019/05/01/ 2019, doi: https://doi.org/10.1016/j.image.2019.01.006.

[55] A. Hambouz, Y. Shaheen, A. Manna, M. Al-Fayoumi, and S. Tedmori, "Achieving Data Integrity and Confidentiality Using Image Steganography and Hashing Techniques," in *2019 2nd International Conference on new Trends in Computing Sciences (ICTCS)*, 9-11 Oct. 2019 2019, pp. 1-6, doi: 10.1109/ICTCS.2019.8923060.

[56] X. Tang, Y. Huang, C. Chang, and L. Zhou, "Efficient Real-Time Integrity Auditing With Privacy-Preserving Arbitration for Images in Cloud Storage System," *IEEE Access,* vol. 7, pp. 33009-33023, 2019, doi: 10.1109/ACCESS.2019.2904040.

[57] M. Ali, S. U. Khan, and A. V. Vasilakos, "Security in cloud computing: Opportunities and challenges," *Information Sciences,* vol. 305, pp. 357-383, 2015/06/01/ 2015, doi: https://doi.org/10.1016/j.ins.2015.01.025.

[58] J. Laufs, H. Borrion, and B. Bradford, "Security and the smart city: A systematic review," *Sustainable Cities and Society,* vol. 55, p. 102023, 2020/04/01/ 2020, doi: https://doi.org/10.1016/j.scs.2020.102023.

[59] E. K. Szczepaniuk, H. Szczepaniuk, T. Rokicki, and B. Klepacki, "Information security assessment in public administration," *Computers & Security,* vol. 90, p. 101709, 2020/03/01/ 2020, doi: https://doi.org/10.1016/j.cose.2019.101709.

[60] G. Reniers, G. Landucci, and N. Khakzad, "What safety models and principles can be adapted and used in security science?," *Journal of Loss Prevention in the Process Industries,* vol. 64, p. 104068, 2020/03/01/ 2020, doi: https://doi.org/10.1016/j.jlp.2020.104068.

[61] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," *Computer Networks,* vol. 169, p. 107094, 2020/03/14/ 2020, doi: https://doi.org/10.1016/j.comnet.2019.107094.

[62] B. Debnath, J. M. Alghazo, G. Latif, R. Roychoudhuri, and S. K. Ghosh, "An Analysis of Data Security and Potential Threat from IT Assets for Middle Card Players, Institutions and Individuals," Singapore, 2020: Springer Singapore, in Sustainable Waste Management: Policies and Case Studies, pp. 403-419.

[63] D. Maulik and J. Swati, "Importance of Information Security and Strategies to Prevent Data Breaches in Mobile Devices," in *Improving Business Performance Through Innovation in the Digital Economy*. Hershey, PA, USA: IGI Global, 2020, pp. 215-225.

[64] M. Leitner and S. Rinderle-Ma, "A systematic review on security in Process-Aware Information Systems – Constitution, challenges, and future directions," *Information and Software Technology,* vol. 56, no. 3, pp. 273-293, 2014/03/01/ 2014, doi: https://doi.org/10.1016/j.infsof.2013.12.004.

[65] I. O. f. Standardization, *ISO/IEC 27011: Information technology-security techniques-information security management guidelines for telecommunications organizations based on ISO/IEC 27002*. ISO, 2008.

[66] R. Anderson, *Security engineering*. John Wiley & Sons, 2008.

[67] R. Lehtinen and G. Gangemi Sr, *Computer Security Basics: Computer Security*. " O'Reilly Media, Inc.", 2006.

[68] W. Stallings, L. Brown, M. D. Bauer, and A. K. Bhattacharjee, *Computer security: principles and practice*. Pearson Education Upper Saddle River, NJ, USA, 2012.

[69] D. Gollmann, *Computer Security, 3rd Edition*. John Wiley & Sons, Ltd, 2013.