Indonesian Journal of Electrical Engineering and Computer Science
Vol. 11, No. 2, August 2018, pp. 733~739
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v11.i2.pp733-739

A Review on Structured Scheme Representation on Data Security Application

Siti Norussaadah Mohd Salleh[1], Roshidi Din[2], Nur Haryani Zakaria[3], Aida Mustapha[4]
[1,2,3]School of Computing UUM College Arts and Sciences, Universiti Utara Malaysia,
06010, Sintok, Kedah, Malaysia
[4]Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia,
Parit Raja, 86400 Batu Pahat, Johor, Malaysia

Article Info

Article history:

Received Feb 1, 2018
Revised Apr 18, 2018
Accepted Apr 28, 2018

Keywords:

Steganography scheme
Cryptography scheme
Structured scheme

ABSTRACT

With the rapid development in the era of Internet and networking technology, there is always a requirement to improve the security systems, which secure the transmitted data over an unsecured channel. The needs to increase the level of security in transferring the data always become the critical issue. Therefore, data security is a significant area in covering the issue of security, which refers to protect the data from unwanted forces and prevent unauthorized access to a communication. This paper presents a review of structured-scheme representation for data security application. There are five structured-scheme types, which can be represented as dual-scheme, triple-scheme, quad-scheme, octal-scheme and hexa-scheme. These structured-scheme types are designed to improve and strengthen the security of data on the application.

Corresponding Author:

Siti Norussaadah Mohd Salleh,
School of Computing UUM College Arts and Sciences, Universiti Utara Malaysia,
06010, Sintok, Kedah, Malaysia.
Email: roshidi@uum.edu.my

1. INTRODUCTION

The growth of the Internet and the tremendous usage of Internet have led to arise of security issue. It makes people struggle on improving the security of the data during transferring information in a communication. As data is transferred via a digital medium, the primary concern is to protect data from intruders. Basically, when the data is transmitted over the unsecured channel, it will be exposed to illegal use, copyright violation and etc. [1]. It is crucial to protect the data from the unwanted access. Thus, data security is a study of methods of protecting data in computer and communication systems [2]. It is a practice of keeping data protected from corruption and unauthorized access. The focus is to ensure privacy while guarding the data. For this purpose, various methods including cryptography, steganography and so on have been used to provide data security where their aim is to secure communication between parties.

Steganography is a technique of hiding information. The hidden message is transferred through various kinds of the medium such as image, text, audio, and video, which can be called as a cover message. Steganography enable the message to be delivered from sender to recipient without being investigated as it is unnotice by interceptors [3]. Thus, steganography can be described as the process of embedding secret message from sender to receiver and verifies that message without being detected by others [4].

On the other hand, cryptography is a technique of converting information into a non-readable message. The purpose is to ensure people cannot understand the transmitted message. The message is not hidden as it is known by others in the communication. Cryptography also involves various methods and implementations. Thus, cryptography can be described as the process of scrambling the secret message from sender to receiver so that the content of the message is protected from others [5]. Subsequently, at the point

when scrambled information is transmitted from sender to recipient, it could make a motivating force for outsiders to reveal the information or to hinder the communication [6].

In short, steganography involves hiding the message, which is known as encode and decode while cryptography is scrambling the content of the message, which is known as encrypt and decrypt. Besides, in steganography people are not aware of the existence of the secret message as it appears like a normal message. Meanwhile, in cryptography, people are aware of the presence of the secret message but the message is unreadable as it is being encrypted during the process. Table 1 shows a comparison between steganography and cryptography including the steps of each.

Table 1. Comparison between steganography and cryptography

Steganography	Cryptography
Medium – image, text, audio, video.	Encryption – encrypt the message into non-readable form.
Hidden message – message that needs to be hidden into a cover message.	Transferring message – send the message to the recipient
Function to be used to hide the message and its inverse to retrieve message	Decryption – decrypt the message into the original form.
Optional key or password to authenticate or to hide and unhide message.	

Based on Table 1, the steganography and cryptography process stress out the transferring information need to be protected through hiding or encryption. Thus, it shows that data security is important for securely transferring message in any communication. Currently, there are two major schemes in the implementation of data security application, which are steganography scheme, and cryptography scheme, which will be discussed further in Section 2.

The rest of this paper is organized as follows: Section 2 reviews the related works of data security schemes; the structured-scheme types are discussed in detail in Section 3; Section 4 provides the discussion; and the conclusion is presented in Section 5.

2. DATA SECURITY SCHEMES

2.1 Steganographic Scheme

One of the schemes used in steganography is called chaotic asymmetric steganographic (CAS) for image steganography [7]. The focus is on the enhancement of the security of secret message through offering authentication on the recipient part. This scheme aims at combining the encryption and signature. It will gain the advantages in terms of security against exhaustive and inverse attacks and trustworthy data that can prevent fraud. However, this scheme is still lacking, as it does not consider the color image that would give the increment in the total message payload.

Next scheme that is used in steganography is referred to as Huffman coding scheme [8] that is designed to hide image into an audio signal. This scheme is introduced as the existing schemes have a less steganographic algorithm for MPEG-2/4 Advance Audio Coding (AAC). They are more focusing on MPEG-1 Layer III (MP3). Thus, the purpose of this scheme is to have a new steganographic scheme for AAC by using the characteristic of Huffman coding. The benefit gained from this scheme is its ability to hide message without affecting its normal process of encoding. However, this scheme causes the AAC file becomes slightly larger after the hiding process. Accordingly, it affects the performance of this steganographic scheme.

The third steganography scheme used is Unicode space character [9] which is mainly for text steganography. The scheme is introduced to improve the capacity in hiding and the efficiency in embedding. It stresses out the combination of Unicode space characters and regular space, which are able to avoid awkward presence on visual attacks. Through this scheme, higher hiding capacity can be achieved and provide better embedding efficiency. Enough robustness also gained from this scheme.

Another scheme that is used in steganography is called Huffman compression scheme [10]. Its purpose is to further increase the hiding capacity and security in text steganography through email based method. The scheme utilizes Huffman compression to make optimal use of email addresses to hide the secret message. Through this scheme, the communication cost is being minimized while security of message is preserved.

Furthermore, the secret image sharing scheme [11] is focusing on improving the quality of the steganographic image. The scheme applies optimal pixel adjustment process to enhance image quality under

different payload capacity and various authentication bit condition. Through this process, it is able to minimize the embedding error while achieving high visual image quality. Also, high authentication capability of the steganographic image can be accomplished. Nevertheless, this scheme is still lacking, as it cannot recover the original state of the cover image.

Besides, there is another image-based scheme that is known as the index-color image. The issue is to provide high embedding capacity with low distortion in the index-color image that is suitable for the Internet environment. This scheme is based on the number of colors and secret bits length [12]. However, the scheme is constrained by the number of colors that should not be more than 128 to avoid the occurrence of distortion. Thus, even the scheme is able to achieve higher embedding capacity, it must meet a requirement in order to prevent distortion.

Lastly, the scheme that is used in steganography is known as exploiting modification direction (EMD). The purpose of this scheme is to improve hiding capacity in QR code steganography. The scheme utilizes the concept of EMD embedding scheme [13] to conceal higher payload of the confidential data into QR tag by modifying QR modules directly. Thus, it will achieve secret protection and feasibility for lower-power barcode readers and mobile devices. Consequently, it will enhance the embeddable secret payload with low computational complexity.

2.2 Cryptographic Scheme

There are also kinds of schemes that have been used in cryptography. One of them is known as proxy signature scheme [14]. In a proxy signature scheme, the proxy signer has the ability to be the representative of the original signer as endorsed by the original one [15]. In order to overcome the security threats and weakness in existing scheme, this scheme introduces a new proxy scheme that is based on elliptic curve cryptography (ECC). As the existing scheme is lack of the secrecy protection for proxy signer and having a vulnerability to coalition attack, this scheme is able to render effective protection by utilizing probability encryption algorithm. It uses enhanced one-way hash function that based on elliptic curve discrete logarithm probability (ECDLP). This scheme is successful in delivering a scheme that produces small key size and low computational cost. Nonetheless, this scheme is needed further research as it should generalize the scheme to the distributing environment when there is no help of a dealer or a trusted party.

The second scheme used in cryptography is called anti-counterfeiting scheme. It is introduced to overcome the problems such as low code security, lacking in mutual authentication, data storage redundancy and long-term faced security loopholes. This scheme is based on chaotic cryptography where a new chaotic encryption algorithm is used to generate commodity anti-counterfeiting code and verification code [16]. It manages to present a new type of checking algorithm that can support multiple and repeating queries. Thus, this scheme is considered to be reliable, effective, and practical. Still, this scheme is hopeful to have improved towards the achievement of higher security value with the ability to combine all types of advanced technology.

The next scheme used in cryptography is known as quantum cryptography voting scheme. The aim of this scheme is to achieve a perfect voting scheme that acquires highly secure process while at the same time transparent for the purpose of legitimacy. This scheme is able to transfer voting information from voting machine into a secure location with the avoidance of modification and eavesdropping. Generally, in the scheme which utilizes quantum key distribution (QKD) [17], the votes are transferred in real time to a predetermined secure location. In this scheme, a novel latency examination technique is being proposed in order to detect thwart man-in-the-middle attacks that might be employed to hack QKD system. As a result, it promotes no delay in declaring the voting results as it readily available right after the last person votes. Thus, maximum security is achieved for the secure location. For the future, this scheme is considering to build encryption method using multivariate public key cryptography in the post-quantum era.

The last scheme in cryptography which is copyright protection scheme is forwarded to protect the rightful ownership of digital data. As this scheme is focused on digital images, it attempts to overcome the weakness of existing system such as the alteration that happened to the host image and also to improve the robustness of some attacks. The scheme is based on visual cryptography (VC) where it employs sampling distribution of means (SDM) to generate a binary master share from a gray-level image [18]. Consequently, this scheme is able to avoid the occurrence of alteration of the host image. Besides, it produces identification of rightful ownership without a requirement of the original image. Moreover, the scheme enables multiple secret images to be cast into a single host image without causing any damage to the other hidden images.

Lastly, the secret image is allowed to be of any size. Through utilization of VC, the security of the scheme is guaranteed which makes it robust against several attacks. Although with a number of benefits gained from this scheme, it still lacking as it only deals with bilevel secret images. A necessary further work should extend its method toward gray-level or even to the color secret image.

3. STRUCTURED-SCHEME TYPES

One of the bestfit approaches to strengthen the data security application either through steganographic scheme or cryptographic scheme is called structured-scheme. This structured-scheme is based on number representation system.

Basically, number representation systems symbolize any notation for the representation of numbers. There are different ways to represent number systems. Most systems have a base number. Thus, number systems can be represented as a decimal system (base 10), a binary system (base 2), an octal system (base 8) and a hexadecimal system (base 16). Decimal system contains ten possible digits from 0 to 9. For the binary system, it is based on two possible digits which are ones and zeroes. Furthermore, the octal system consists of 8 octal characters from 0 to 7. Besides, there is also an octal notation that can be used for writing binary numbers.

Lastly, the hexadecimal system is comprised of normal digits 0 to 9 plus six more alphabets from A to F. It helps for the handling of binary data easily. Indeed, there is a scheme for number representation systems that have been applied in the area such as in computer science and in information security. That scheme which had been utilized in others prominent area is known as the structured-scheme type. There are five types of structured-scheme which can be denoted as dual-scheme, triple-scheme, quad-scheme, octal-scheme and hexa-scheme.

3.1 Dual-Scheme

A dual scheme has been introduced in the watermarking area. This dual watermarking scheme is reinforced with encryption. The purpose of this scheme is to improve the robustness and protection along with security. This scheme is based on Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) [19] along with the chaos-based encryption technique. There are four modules involved in the proposed scheme. First, is by embedding a secondary watermark into the primary watermark. Second is encryption of watermarked primary image and embedding in the host image. The third module is called attacks, as the aim is to investigate the robustness of the algorithm. Finally, the last one is the extraction of the primary and secondary watermark from the host image. Based on the findings, the chaos encryption scheme is able to supply a wide key space and high key sensitivity. Also, the cipher can resist brute force attack and statistical analysis. Moreover, the scheme showed robustness through a variety of attacks.

Besides, there is a novel audio watermarking scheme [20] which is based on echo hiding technique by exploiting dual echo kernels. The echo hiding method is a watermarking scheme which embeds watermark bits in inaudible echo delays. Echo kernels are used with different echo delays for increasing watermarking payload. In this scheme, dual backward-forward echo kernel is introduced to increase the robustness of the proposed algorithm. Thus, multiple echo delay is proposed instead of previous two echo delay for embedding more than one bit per audio section. During data embedding procedure, the original audio signal is first segmented into sequential sections. Next, watermark data sequence is encrypted by using a pseudo-random generator and as a secure key before divided into 3-bits binary groups. Then, echo delay is calculated for each audio section. Lastly, the sections are concatenated to form watermarked audio signal. Cepstrum Analysis is applied to analyze the proposed scheme mathematically. The results of the scheme showed that it was mathematically proven that proposed echo kernel has larger peaks in decoding step thus it has more robustness against attacks. Besides, this new echo kernel provides better detection rate through analysis.

3.2 Triple-Scheme

A triple image encryption scheme has been introduced by use of fractional Fourier transform domains [21]. This scheme is a combination of amplitude encoding with phase encoding. It applied optical implementation of a triple image encryption algorithm where it is presented with an electro-optical hybrid structure. The process started with an original image is encoded in amplitude part. Other two images are encoded into phase information. The key of encryption algorithm is obtained from the difference between the third image and the output phase of the transform. Indeed, the fractional order is also regarded as key. Numerical simulation is employed to test the capability and security of the proposed scheme. The outcome of this scheme showed that the encrypted images can stand against the attack of brute force decryption. Besides, a multiple image encryption (MIE) is obtained based on this triple image encryption. Thus, this scheme provides efficiency and security of their algorithm.

Also, a Wireless Sensor Network (WSN) authentication scheme has been proposed to provide high security resilience, scalability, and quick message authentication. This scheme is based on Timed Efficient Stream Loss-tolerant Authentication (TESLA) protocol, Elliptic Curve Diffie-Hellman (ECDH) key agreement scheme, and Elliptic Curve Digital Signature Algorithm (ECDSA) [22]. Each of them serves a

different purpose. For instance, TESLA helps reduce delay and loss while ECDSA quicken the signature verification process based on coordination between the sensor nodes. The flow of the scheme started with organizing nodes and set up the initial level of parameters.

Next is the generation of an auxiliary key, which is based on a random number and Hilbert number. This auxiliary key produces the signature according to its approach. On the other hand, ECDH key agreement protocol provides private/public key and then the concatenation of these keys results in the hash key, which is broadcasted in the WSN. When the key is validated and estimated to be a valid key, the corresponding node starts to forward the packet to the remaining nodes in the network. When the key is not valid, the packets are discarded and the status is reported to the base station.

A comparison is done with various existing broadcast authentication and security schemes in WSN to analyze the schemes. As a result, the scheme performs better in term of accuracy, detection of attacks, resiliency, memory consumption, nodal detection, and an average of total transmission energy consumed per node.

3.3 Quad-Scheme

A quad-scheme known as optical frequency quadrupling scheme has been introduced to be as a low cost scheme for generation of 40-GHz milimeter-wave signals which based on Radio-over-Fiber (RoF) system [23]. This scheme enables to broaden the preferred bandwidth through utilization of two cascading dual drive Mach-Zehnder Modulator (DD-MZM). The scheme sustained the 64QAM-OFDM format, which led to the achievement of RoF system's efficacy.

3.4 Octal-Scheme

An octal biasing scheme [24] is proposed in previous research to overcome the problem in the performance of Digital-to-Analog-Converter (DAC). This scheme utilized bias cells that are not directly connected with other. They are 8 separate and independent bias cells in 4x2 array structure that help to reduce input code nonlinearity. Through this method, the on-chip bandgap current reference circuit is used to provide bias voltage for current sources. Bias generators are divided into 8-bias cells places in 4x2 arrays. So, there is no direct connection between any two bias cells (non-correlated cells). The current sources connected with different bias cells are independent, not affected due to switching the current sources connected with other bias cells. Thus, this scheme reduces correlated noise among current sources. Besides, better linearity is achieved and an improvement in the spectral performance.

In addition, a new regular radix-8 scheme for elliptic curve scalar multiplication without pre-computation is proposed to achieve the fastest scalar multiplication result and deriving faster Elliptic Curve Cryptography (ECC) formula for parallel architecture [25]. This scheme combined three approaches in scalar multiplication. It allows one to compute each of 3 bits of a scalar with 5 points arithmetic operation in unified sequence. Based on the author's findings, this scheme generates less computation time, minimize energy expenditure. Besides, it increases the speed of computation. Its security hold against both Simple side-channel attacks (SSCAs) and safe-error (or C-safe) fault attacks.

Furthermore, Quantum Octal Logarithmic Approximation Keying (QOLAK) scheme has been presented for securing AS-PATH of inter-domain routing [26]. This scheme is a combination of octal logarithmic approximation keying scheme and quantum cryptography. The process is started with obtaining the key through octal logarithmic key technique. Then, the input key is split into blocks of 8-bits key. Next, quantum key cryptography technique is applied to strengthen the key. The output key is obtained in form of qubits where the multiple blocks of qubits key concatenate into single qubit key. The results obtained from previous works showed that better convergence time is achieved.

3.5 Hexa-Scheme

There is a hexa-scheme that modified ElGamal Elliptic Curve Cryptosystem using hexadecimal representation [27]. The objective is to propose a new efficient method to encrypt/decrypt data using ECC. The Modification of ElGamal Elliptic Curve Cryptosystem (MEGECC) depends on speeding up the computation on ElGamal Elliptic Curve Cryptosystem (EGECC). The number of doubling and adding operations in the encryption process has been reduced through this method. The encryption and decryption of any text are by using the hexadecimal ASCII value for each character. The proposed algorithm includes three steps which are key scheduling, encryption, and decryption. There are two essential results obtained by the former researchers after comparing the proposed method with another method [28].

The proposed method needs less operation Also, the improvement percentage increases when the plaintext size increases.

4. DISCUSSIONS

As mentioned above, the schemes used in data security are reviewed in which have been detailed further according to data security categorization namely steganography and cryptography. In steganography scheme, the major strength that is highlighted in the scheme is recognized as the capacity of hiding the message. Meanwhile, the main advantage in cryptography scheme is known to be the robustness against the attacks.

Furthermore, this paper reviewed the applications of structured-scheme types. The structured-scheme has been applied to different areas such as watermarking, broadcasting and engineering. Nonetheless, they are found intersected in the areas mentioned earlier. For instance, watermarking application utilized dual-scheme and triple-scheme. Meanwhile, engineering application is found in dual-scheme and octal-scheme.

Based on the previous research on these structured-scheme types, they are certain measures that are counted for improving the schemes. Besides providing security in their schemes, the schemes also promoting other values such as robustness, flexibility, and effectiveness. All these values are measured to indicate the performance of the scheme involved.

5. CONCLUSIONS

This paper presented a review on schemes used in data security, which can be classified into steganography scheme and cryptography scheme. Based on that review, steganography is being different with cryptography in general through a tabular form. Besides, each scheme from steganography and cryptography has portrayed its strengths and weaknesses. The main aim of this paper is to introduce the structured-scheme based on the works done by former researches. Five types of structured-scheme have been identified, which are dual-scheme, triple-scheme, quad-scheme, octal-scheme, and hexa-scheme. Hence, this structured-scheme can be represented in Figure 1.

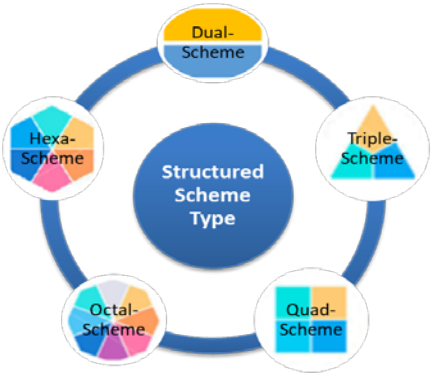

Figure 1. Structured-scheme classification

It is expected in the near coming future that bestfit algorithm in steganography will be produced from the structured-scheme type. A performance evaluation can be executed by applying structured-scheme representation in letter-based technique which has been proposed by [29]. Therefore, this study believes that the text steganography can utilize the structured-scheme in order to enhance the level of security in transferring the data and protect the intrusion from any unauthorized parties.

ACKNOWLEDEMENT

This research is jointly supported by the Fundamental Research Grant Scheme (FRGS), MoHE under SO Code 13576 Universiti Utara Malaysia and Vot 1557 Universiti Tun Hussein Onn Malaysia.

REFERENCES

[1] S. Paliwal and K. N. Rajesh, "A Survey & Applications of Various Image Steganography Techniques," vol. 7, no. 1, pp. 204–209, 2016.

[2] D. E. Robling Denning, *Cryptography and Data Security*, no. May. Addison-Wesley Longman Publishing Co., Inc., 1982.

[3] M. R. PourArian and A. Hanani, "Blind Steganography in Color Images by Double Wavelet Transform and Improved Arnold Transform," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 3, no. 3, pp. 586–600, 2016.
[4] N. S. Sikarwar, "A Model for Performance Enhancement of Steganography through Dynamic Key Cryptography," *Int. J. Adv. Netw. Appl.*, vol. 3, no. 6, pp. 1395–1401, 2012.
[5] R. Kumar and A. J. Singh, "Understanding Steganography over Cryptography and Various Steganography Techniques," *Int. J. Comput. Sci. Mob. Comput.*, vol. 4, no. 3, pp. 253–258, 2015.
[6] E. Alrashed and S. S. Alroomi, "Hungarian-puzzled Text with Dynamic Quadratic Embedding Steganography," *Int. J. Electr. Comput. Eng.*, vol. 7, no. 2, pp. 799–809, 2017.
[7] D. Lou and C. Sung, "A Steganographic Scheme for Secure Communications Based on the Chaos and Euler Theorem," *IEEE Trans. Multimed.*, vol. 6, no. 3, pp. 501–509, 2004.
[8] J. Zhu, R.-D. Wang, J. Li, and D.-Q. Yan, "A Huffman Coding Section based Steganography for AAC Audio," *Inf. Technol.*, vol. 10, no. 10, pp. 1983–1988, 2011.
[9] R. Kumar, S. Chand, and S. Singh, "An Efficient Text Steganography Scheme using Unicode Space Characters," *Int. J. Forensic Comput. Sci.*, vol. 10, no. 1, pp. 8–14, 2015.
[10] R. Kumar, A. Malik, S. Singh, and S. Chand, "A High Capacity Email based Text Steganography Scheme using Huffman Compression," in *3rd International Conference on Signal Processing and Integrated Networks (SPIN)*, 2016, pp. 53–56.
[11] C. Wu, S. Kao, and M. Hwang, "A High Quality Image Sharing with Steganography and Adaptive Authentication Scheme," *J. Syst. Softw.*, vol. 84, no. 12, pp. 2196–2207, 2011.
[12] S.-M. Kim, Z. Cheng, and K.-Y. Yoo, "*A New Steganography Scheme based on an Index-color Image*," in 6th International Conference on Information Technology: New Generations, 2009, pp. 376–381.
[13] P.-Y. Lin and Y.-H. Chen, "*QR Code Steganography with Secret Payload Enhancement*," in IEEE International Conference in Multimedia & Expo Workshops (ICMEW), 2016, pp. 1–5.
[14] X. Sun and M. Xia, "*An Improved Proxy Signature Scheme Based on Elliptic Curve Cryptography,*" in International Conference on Computer and Communications Security, 2009, pp. 88–91.
[15] S. Verma and B. K. Sharma, "New Proxy Blind Multi Signature based on Integer- Factorization and Discrete-Logarithm Problems Problem," *Bull. Electr. Eng. Informatics*, vol. 1, no. 3, pp. 185–190, 2012.
[16] S. Sheng and X. Wu, "*A New Digital Anti-counterfeiting Scheme Based on Chaotic Cryptography,*" in International Conference on ICT Convergence (ICTC), 2012, pp. 687–691.
[17] D. S. Sundar and N. Narayan, "*A Novel Voting Scheme using Quantum Cryptography,*" in IEEE Conference on Open Systems (ICOS), 2014, pp. 66–71.
[18] V. R. Bolla and D. T. V. Gopal, "*A Two Phase Copyright Protection Scheme for Digital Images using Visual Cryptography and Sampling Methods,*" in International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), 2016, pp. 2041–2046.
[19] R. Dhanalakshmi and K. Thaiyalnayaki, "Dual Watermarking Scheme with Encryption," *Int. J. Comput. Sci. Inf. Secur.*, vol. 7, no. 1, pp. 248–253, 2010.
[20] A. Delforouzil and M. Pooyan, "Increasing Payload of Echo Hiding Scheme Using Dual Backward and Forward Delay Kernels," *IEEE Int. Symp. Signal Process. Inf. Technol.*, vol. 2, no. 1, pp. 375–378, 2007.
[21] Z. Liu, J. Dai, and S. Liu, "Triple Image Encryption Scheme in Fractional Fourier Transform Domains," *Opt. Commun.*, vol. 282, no. 4, pp. 518–522, 2009.
[22] M. R. Kumar and S. G. Dhas, "An Expedited Triple Key Broadcast Authentication Scheme based on TESLA, ECDH, and ECDSA," *J. Theor. Appl. Inf. Technol.*, vol. 58, no. 3, pp. 506–516, 2013.
[23] X. Gao, J. Chen, X. Chen, H. Li, L. Fu, and Shihuan Zou, "Generation of 40-GHz Millimeter-Wave Signals based on Radio-over-Fiber System Employing Optical Frequency Quadrupling Scheme," in *Communications and Photonics Conference and Exhibition*, 2011, vol. 8309, pp. 1–7.
[24] S. Sarkar and S. Banerjee, "A 10-bit 500 MSPS Segmented DAC with Distributed Octal Biasing Scheme," *Opt. Express*, vol. 18, no. 3, pp. 2503–2508, 2010.
[25] E. A. H. Abdulrahman and A. Reyhani-masoleh, "New Regular Radix-8 Scheme for Elliptic Curve Scalar Multiplication without Pre-Computation," *IEEE Trans. Comput.*, vol. 64, no. 2, pp. 438–451, 2015.
[26] K. Vidya and V. R. Uthariaraj, "Quantum Octal Logarithmic Approximation Keying (QOLAK) Scheme for Securing AS-PATH in Inter-Domain Routing," *Inf. Technol. J.*, vol. 10, no. 9, pp. 1725–1732, 2011.
[27] Z. E. Dawahdeh, S. N. Yaakob, and A. M. Sagheer, "Modified ElGamal Elliptic Curve Cryptosystem using Hexadecimal Representation," *Indian J. Sci. Technol.*, vol. 8, no. 15, pp. 1–8, 2015.
[28] S. M. C. Vigila and K. Muneeswaran, "*Implementation of Text based Cryptosystem using Elliptic Curve Cryptography,*" in 1st International Conference on Advanced Computing (ICAC), 2009, pp. 82–85.
[29] R. Din and S. Utama, "*Critical Review of Verification and Validation Process in Feature-Based Method Steganography,*" in International Conference on E-Commerce, 2017, pp. 15–19.