International Journal on Advanced Science Engineering Information Technology

Vol.12 (2022) No. 1
ISSN: 2088-5334

Embedding Data in Non-Important Gabor Ridges

Ali Abdulazeez Mohammed Baqer Qazzaz [a,*], Elaf J. Al Taee [a], Ziena Hassan Razaq Al Hadad [a]

[a] *Department of Computer Science, Faculty of Education, University of Kufa, Najaf, Iraq*
Corresponding author: [*]alia.qazzaz@uokufa.edu.iq

***Abstract*—Hiding information either by steganography or watermarking operation is essential for computer science. It is used as a method for sending secure and important information. It has special features that even if this information is discovered, the third part cannot reconstruct the original information in any way, not famously and commonly nor difficultly and especially by using any technique or algorithm. There are many hiding techniques; each one of them used different paths to ensure standard properties such as optimizing security level, increasing the amount of embedding data, decreasing the ability to reconstruct hidden information by any unwanted part. Here in the following suggested technique, different quantities of bits are hidden in various pixels depending on some discovered constraints by using the famous Gabor filter then divided ridges part in a selected fingerprint image for the purpose of hiding relevant information into important and non-important pixels that laying out of ridges in final images after applying Gabor filter which consider not important regions in fingerprint image for discovering important features from the image. The pixels used in hiding information belong to finger ridges in pure fingerprint images but covert to white pixels (valley) in the matrix after applying the Gabor filter and in original white pixels in both matrices by using different techniques for each type of pixels. The imaging stage constructed after the suggested technique is good and identical to the pure image for the accepted degree as shown in used fidelity metrics (PSNR). It is similar to a pure fingerprint matrix as proved in these metrics for calculating the level of goodness of proposed algorithms. Our algorithm exploits existing pixels in fingerprint image with different levels of importance and avoids pixels with high importance for protected important features from non-deterministic varying.**

***Keywords*—Fingerprint; biometric, Gabor filter; steganography; LSB; PSNR.**

Manuscript received 20 Apr. 2021; revised 19 Aug. 2021; accepted 11 Nov. 2021. Date of publication 28 Feb. 2022.

I. INTRODUCTION

Biometric science is a part of computer science that studies important behavioral and physical fractures for some parts of the human body and analyzes these features in an accepted and perfect way. This science uses to identify people by storing these features in an arranged and smart database. Every Biometrics indicator has some special characteristics, but at the same time, all of them share some basic characteristics. Biometrics indicators are divided into two groups: physical indicators (such as iris retina, fingerprint, palm print, Oder, ear, and face), and the other type is called behavior indicators (such as signature, gait, and sound).

Any specific indicator of these biometrics has its special style that is used to represent the wanted information as binary information. Therefore, any task performed in this information (such as enhancement and compression) must take into consideration the truth that the important wanted features are saving without any bad impact on the system. It is subject to ensure that the automatic technique used in the recognition process is still perfect with an accepted degree in any way [1].

The image of fingerprint has been divided (depending on the shape of some existing regions that construct the final rounded pattern) into two parts that appear parallel: black regions (called ridges) and white regions (called valleys), as illustrated in fig. (1). Many unwanted properties are found in some people's fingerprints, like cracks, cuts, calluses, and bruises [2], as illustrated in figure (1).

Fig. 1 Fingerprint image

The image of fingerprint contains many different and important features, which can be calculated for white (valley part) or black pixels (ridge part) [3]. These features are basically divided into groups as illustrated below [4], [5]

1) A-(Local features): these features were discovered by fetching certain behavior of black ridgeline by taking and analyzing the moving of any ridge as an isolated entity or sometimes in a selected state by discovering the special and specific correlation between wanted separated ridges [6].

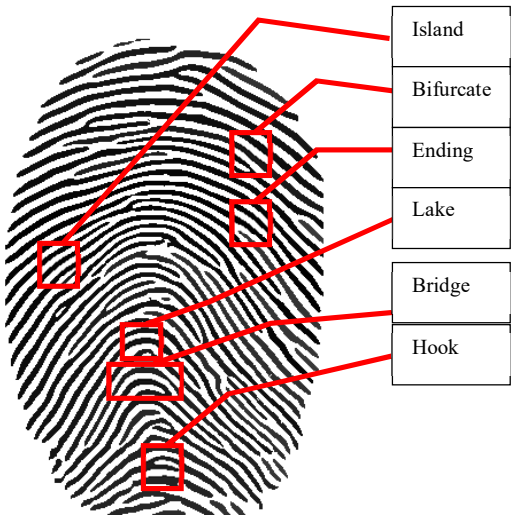


Fig. 2 Local features

The local features that consider as most important and affected in fingerprint images are dot (or island), ending, bifurcation, hook, lake, bridge [7], as illustrated in fig. (2). From previous features, only two of them are originally used in fingerprint systems: ending and bifurcation [8].

2) (Global features): This group of features contains big features (core and delta) [9]. The core is a special region in the top points of the insider ridge. In comparison, the delta region exists as a group of points with three different flow directions and moving in them, as explained in fig. (3). The term singular points or singularities are used by some books to explain this group of features [3], global features used in the process of classification generally into (5) or (6) classes which are right loop, arch, whorl, tented arch, and left loop, and the additional class is (twin loop) [10].

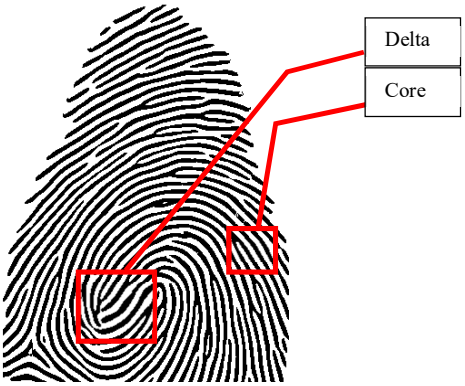


Fig. 3 Global features

To get the best result of detecting the image of a fingerprint, a perfect and useful (valid) method must be used. The usage is with the finger image to avoid distortion of either high or low pressure of human on the screen of the device of recording person print. In order to get wanted results, the contextual filters (like Gabor filter) should be performed either instead of or side by side with a fixed filter that uses various filters for enhancing pixels instead of a fixed filter for all pixels to create a large number of true features [11].

$$G(x, y, f, \theta) = \text{Exp}\left\{\frac{-1}{2}\left[\frac{x_1^2}{\delta_x^2} + \frac{y_1^2}{\delta_y^2}\right]\right\}\cos(2\pi f x_1) \quad (1)$$

$$x_1 = x\cos\theta + y\sin\theta \quad (2)$$

$$y_1 = -x\sin\theta + y\cos\theta \quad (3)$$

Where, (f) is the frequency of the wave with the orientation (θ) calculated from the x-axis,(δ_x *and* δ_y) are the Gaussian constants along x and y axes, respectively [12], in suggested method (variables fixed as $f = 0.1$, $\delta x = 4$ and $\delta y = 4$).

It is a science that deals with hiding or embedding information in appropriate cover by using an alterable method [13]. The main purpose of this process is to prevent anyone from accessing confidential information, and this hiding information can be restored only by a right and wanted person. Steganography science is concerned with two file types which are the message (secret file) and carrier (cover file) [14]. In addition, the steganography task consists of two steps (phases) the first phase for hiding the secret data to create stage-object, and the second step for extracting the secure data from the stage-object after acceptance stage-object by the meant destination [15].

The categorizing of steganography techniques includes three ways below:

1) Depending on the types of the cover file [16]: the steganography method is divided into four groups depending on the type of the cover file (Text, image, audio, steganography) [17]. There are many techniques for text steganography, such as coding of shift-line (SLC), of shift-word (SWC), and of the features (FC). The Least Significant Bit (LSB) is the important and essential technique for hiding secure data within a suitable carrier (image) cover is the Least Significant Bit (LSB). The four important techniques generally used in the hiding process using least-significant-bit are blind hide, hide seek, filter first, and battle steganography. In methods of audio steganography, secure data is embedded within audio media. Some known techniques using audio cover are parity coding, LSB Coding, Echo Hiding, Spread Spectrum, and Phase Coding [18]. Video files have two types of data: images and sound information, so hiding secure data by using audio files or image files can be used in hiding data in video files [19]. The advantage of embedding secure data in this type of file is the permitting of hiding a huge amount of secure data in this type of media [20].

2) Depending on the methods of hiding secure information: the steganography method is divided depending on the hiding techniques into insertion, substitution, and generation [21]. Using the first technique, secret data is hidden in the cover media by searching for suitable place in this media that is never taken into account by the programs used for reading this file. Using the second technique, secret data is hidden in the carrier (cover) file by changing non-

important components in the carrier media with secret message bits, ensuring that noise quantity stills in accepted rate in the file after the hiding process [22]. Using the third technique, secret data is hidden by constructing stage files depending on the secure data in the message file.

3) Depending on the used key: by this technique stage-methods divided into methods:

- Pure Steganography methods: This method is simple and considered insecure in communication for sending very important messages and works depending on the principle of fixing stage-key during stage-operation [23].
- Secret key methods: involve the process of exchanging the stage-key either pre or post-sending the wanted message. Only the decided partners have the used key, so extracting the message can be done only by the wanted person [19].
- Public key method: exploit the special relation between (public and private) keys to ensure the process of increasing the security level of the message file where one person has a public key and performs embedding process while the other person has a private key and performs extracting the wanted data. This method considers a strong one in hiding data because of using two related and different keys [24].

Steganography involves hiding secure data in a suitable carrier by a computable method to make it very difficult for any person to detect or remove important information. Relating to the previous idea, three essential features used for calculating the efficiency of these secure techniques:

- The ability to hide more data into a fixed-size carrier file reflects a good algorithm.
- Increasing the ability to resist the processes of discovering and changing secure data in the cover file reflect perfect algorithm
- Increasing the ability to resist removing secret messages from the cover file after detection. It provides an index of the degree of compactness in the algorithm.

The techniques of hiding data have become important in many fields, such as:

- Medical sides incorporate a name or/and wanted person information in the medical image without adding bad effects(noise) [25].
- Military sides for sending secure messages without still ability from any third part to detect embedding message [26].
- Intelligent sides.
- In lawful sides to discover some malicious changing in important papers or by other words forgery detecting.

This study proposed a suggested method by using steganography and encryption to code and hide secret information in a particular image by using binary bits and pixels values of the selected image. After performing the proposed technique, constructed results could be suitable and perfect—suggested method tested by using proven metrics to be checking in the pixels of the wanted carrier.

Abujar *et al.* [17] suggested a suitable method for sending very secret and sensitive messages in the channel by exploiting the process of hiding wanted data in the non-understandable image that encrypted by using a suitable encryption method to increase security in the transmission process, the retrieving operation of secret information can be done by reversing hiding stage. This search explained some important works on the side of hiding data and encryption images, so many techniques are discussed scientifically. This study suggests and introduces a good image steganography algorithm by exploiting the signature idea in embedding secret data. The work in this algorithm consists of two parts, the first one related to hiding data after performing many correlative steps as follows:

- Preprocess operation (for carrier and secret message),
- Divided images into blocks and exploited chain code concept with similarity calculations for blocks,
- Apply (DCT) transform,
- Signature measuring,
- Finally, performing suggested technique for hiding and constructing stage image).

While the second part is related to extracting confidential data after applying reversible steps compared to the embedding steps. This study suggests a new and suitable algorithm depending on Wavelet Transform (WT) and Arnold filter (AT) usage. The Arnold filter hides information in a calculated manner by using deterministic and reversible ways like the Arnold filter. The discovery of good cover depends on (WT), so the data could be hidden into wavelet coefficients. The previous method is robust against attacks ways such as cropping stage-image. Results proved with high and accepted peak -signal-noise -ratio level.

This study also proposed an algorithm by exploiting the concept of deep NNs because they are very sensitive to any changes in the input images. The algorithm works by learning designed NN with some patterns of data with existing variations for performing best quality and a great quantity of secret data. They exploit the idea of performing both encoder and decoder in the networks. An indistinguishable image could be calculated in the encoder operation, while in the decoder operation, the process of retrieving the message could be performed. The previous operations can be considered as competitive operations, and the algorithm has a good robust degree against noise and compression operation. The designed NN model in extracting process learned for constructing secret data in the image. Finally, they proved the level of quality for the stage objects.

The new method is suggested in this study to save secret data over the internet by sealing binary goods to ensure the availability of goods and emphasize the good acceptance and the process of distinguishing from the unaccepted goods. The process of hiding data aims to provide a good level of efficiency and security in the transmission of confidential data like commercial data.

II. MATERIALS AND METHOD

The proposed method generally consists of two (2) stages. Each stage can be divided into many steps or processes to perform the essential stages (hiding and extracting) so the proposed system can be explained as parts divided into processes for performing one task each time, as illustrated in fig. (4).

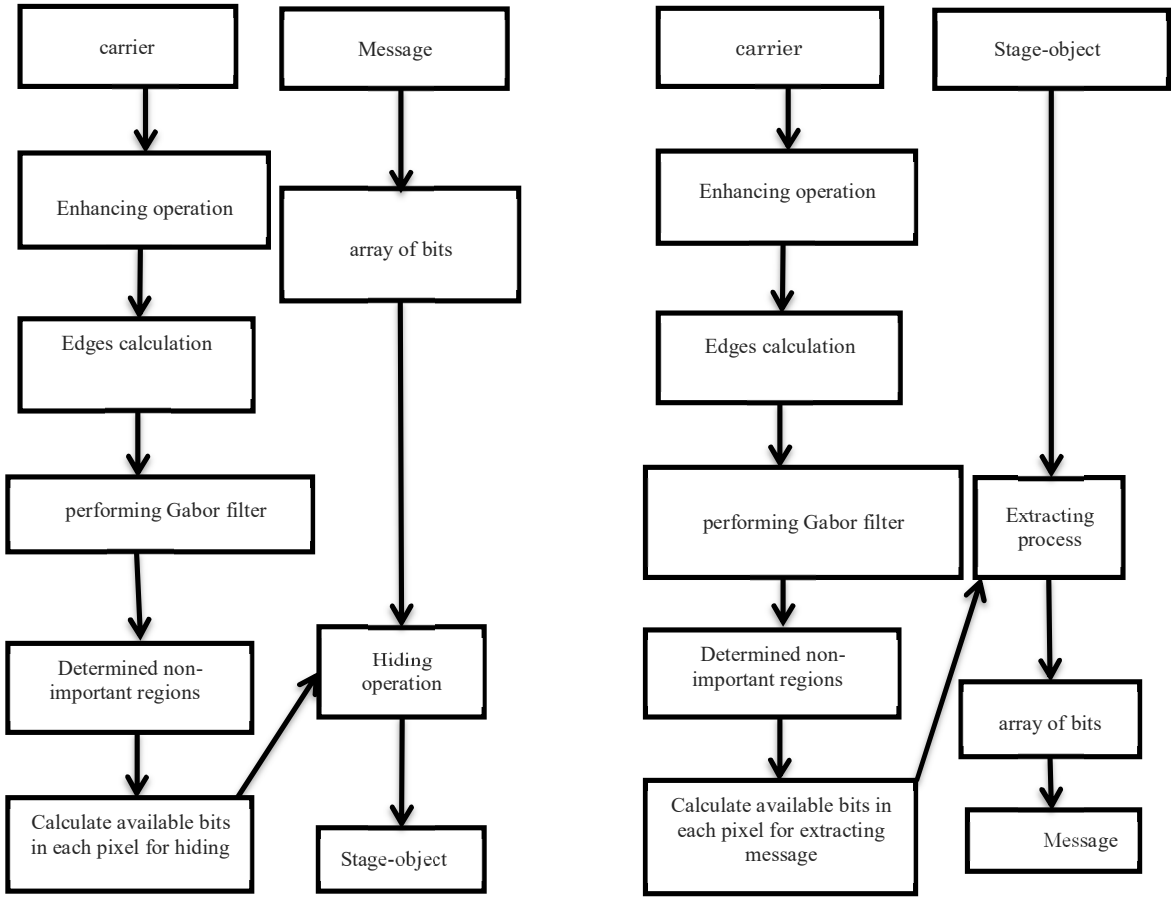


Fig. 4 Proposed system diagram

A. Hiding Operation

- Enhancement operation for the pure image.
- Perform one of the edges detection filters such as Sobel (SEDF).
- Perform Gabor filter (GF) on the pure input image (FPI) to fill gaps in it.
- Determined regions out of regions of interest of Gabor regions.
- Calculate bits number for use in the hiding operation.
- Convert the secure message into an equivalent array of bits.
- Hiding bits in one dimension array bits into decided pixels and the decided number of bits for each pixel in the carrier file.
- Sending stage image to the required person.

For producing stage-object by merging a cover image with the secret message in a suitable and calculable method and consist of the following steps

1) Enhancement process for pure image: The proposed system enhanced fingerprint image by performing a median filter among every pixel in FPI. It is eight neighbors as known by arranged 9-pixels in any order and selecting the pixel in a central position to exchange pixel value with this value of the fifth position as illustrated in fig. (5).

Fig. 5 Image enhancement

2) Perform one of the edges detection filters such as Sobel (SEDF): in this process of the proposed system, vertical and horizontal Sobel edge detection could be applied for enhancing FPI as illustrated in fig. (6) and fig. (7).

3) Perform Gabor filter (GF) on the pure input image (FPI): this process consists of many operations that are:

- Determined orientation in the pixels after applying Sobel filters in both (x and y) direction and determined all edges orientation in all image pixels. Where:

$$\theta = \tan^{-1}(\frac{dy}{dx}) \quad (4)$$

- Portioning finger matrix into suitable and decided blocks, then determining the orientation for each block.
- Converting FPI in Gabor matrix into only two colors (binary images) by proposed the mean of final fingerprint image in the matrix as a threshold as explained.

Fig. 6 Sobel filters

Determining (GF) values for each pixel in the enhanced fingerprint matrix by proposed values for some variables as a moveless value for making the total calculations accepted from the side of simplification and complexity as explained in fig. (7).

Fig. 7 Performing Gabor filter

4) Calculate non-important Gabor regions: this process determined the pixels that can be considered as important non- regions in the fingerprint image. So, each white pixel in the binary image and still white in Gabor image consider non –import pixels as well as black pixels in a binary image that become white pixels because these pixels do not share in extracting important features in finger image, and these regions illustrated in fig. (8).

Fig. 8 Non-important regions

5) Calculate bits number for using in the hiding operation: bits number could be determined after calculating the variance value between each pixel in the Gabor matrix and its neighbors because of hiding operation in the pixels owning high variance with its neighbor make changes in the total matrix insensible so

- Block Variance value is too large→ hide by using 5 least significant bits,
- Block Variance value is large → hide by using 4 least significant bits,
- Block Variance value is medium → hide by using 3 least significant bits,
- Block Variance value is small → hide by using 2 least significant bits,
- Block Variance value is too small→ hide by using 1 least significant bit,

6) Convert the secure message into an equivalent array of bits: by translating pixels value into eight bits representation and taking into account the number of bits used in constructing fingerprint image.

- Hiding bits in one dimension array into decided pixels and the decided number of bits for each pixel in the carrier file as shown in fig. (9)
- sending stage-object to the required person.

B. Extracting Operation

Extracting stage consist of the same operations as in the hiding stage but in the reverse fashion, and this stage finally constructs the secure message.

- Enhancement process for stage-object.
- Perform filter for detection edges.
- Perform Gabor filter to stage-object to discover Gabor regions.
- Decided non-important regions.
- Calculate several bits used in Extracting operation.
- Extracting operation and constructing secure bits of message by taking a number of bits that are used in hiding operation for each pixel.
- Forming secure message array.

Fig. 9 Stage object

III. Results and Discussion

After applying the suggested system on various FPIs, the following results was determined:

A. Case (1)

a. Pure image

b. Binary image

c. Gabor image

d. non-important regions

e- Message

f-Stage-object

Fig. 10 First case results

The image with a label (d) in figure (10) explained the pixels with a low level of importance that could be used in hiding suggested information (image (f)) only as an indicator for the place. This means that we used an image (d) to decide non-important pixels but used original pure image (a) to hide information as we suggest out of important Gabor ridges. The fidelity indicator (PSNR) peak-signal-to-noise-ratio in case (1) is (36.415), and the number of hidden points is (9072) points, and this value of the performance metric is accepted and reflects a good degree of similarity between original and stage images.

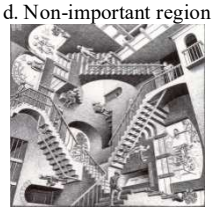
B. Case (2)

a. Pure image.

b. Binary image

c. Gabor image

d. Non-important region



e. message

f. Stage-object

Fig. 11 Second case results

The main novel aspect in the above images is that the stage image is identical to the original image in ridges that could extract important features from fingerprint images age like global and local ones. The fidelity indicator (PSNR) peak-signal-to-noise-ratio in case (2) is (42.931), and the number

of hiding points is (10890) points. In case (2), the performance metric is better than its value in case (1). This state can be interpreted easily because of the bits of the message (d). In case (2) are more similar to bits of non-important pixels in fingerprint image labeled (a) than in case (2). For that reason, the performance metric (PSNR) is better in case (2). This state is exploited by many researchers in putting facility constraints for selecting a good or better cover for a specific message that makes the final stage file more similar to the original one.

IV. Conclusion

The results of the proposed system explained the main efficiency metric for reflecting any unaccepted noise in the stage object. It is compared to the pure fingerprint matrix PSNR and decided that the distortion in stage-matrix is accepted and in the perfect region of this matrix. If the value of this matrix is higher than the accepted value, then the additional noise is the accepted level, and this fixed value depends on the application used for changing images.

The proposed system solves one of the most important problems in hiding systems by proving an important level for each pixel in the cover image and hiding information in pixels with a low level of suggested metrics. The proposed metrics depend on the nature of the cover image, the wanted degree of the compactness in the biometric system, and the amount of information prepared for hiding.

The proposed system used, in general, two undeclared keys. The first one is used only in determining places for hiding information in a deterministic way that can be reversible in the second stage. In comparison, the second key is used only for deciding many bits that could be used in hiding operation depending on the suitable way that can be reversed in the extracting stage without any noticeable problem, so these keys provide a strong security level for the proposed system.

The suggested method for hiding out of Gabor filter ensures that important regions in fingerprint images stay without any changes. Hence, the fingerprint system work without any side effects from the hiding system, and this state make the finger system work for discovering important local and global features with a high degree of efficiency and more reliability. Hiding secret messages in the noisy region with a high variance value makes the hiding process more unnoticeable and perfect because changing after the hiding operation happened between pixels with high variance.

References

[1] C. Chen *et al.*, "Review helpfulness prediction with embedding-gated cnn," *arXiv Prepr. arXiv1808.09896*, 2018.

[2] F.-T. Hong, W.-H. Li, and W.-S. Zheng, "Learning to detect important people in unlabelled images for semi-supervised important people detection," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2020, pp. 4146–4154.

[3] M. Wang, J. Zhang, S. Jiao, X. Zhang, N. Zhu, and G. Chen, "Important citation identification by exploiting the syntactic and contextual information of citations," *Scientometrics*, vol. 125, no. 3, pp. 2109–2129, 2020.

[4] Z. Yang, C. Zhu, and W. Chen, "Parameter-free sentence embedding via orthogonal basis," *arXiv Prepr. arXiv1810.00438*, 2018.

[5] C. M. Childs and N. R. Washburn, "Embedding domain knowledge for machine learning of complex material systems," *MRS Commun.*, vol. 9, no. 3, pp. 806–820, 2019.

[6] N. Van Tu, J.-H. Yoo, and J. W.-K. Hong, "PPTMon: Real-Time and Fine-Grained Packet Processing Time Monitoring in Virtual Network Functions," *IEEE Trans. Netw. Serv. Manag.*, vol. 18, no. 4, pp. 4324–4336, 2021.

[7] R. Hidayat, F. N. Jaafar, I. M. Yassin, A. Zabidi, F. H. K. Zaman, and Z. I. Rizman, "Face detection using Min-Max features enhanced with Locally Linear Embedding," *TEM J.*, vol. 7, no. 3, p. 678, 2018.

[8] M. S. Shim, H. Hu, and P. Li, "Reversible Gating Architecture for Rare Failure Detection of Analog and Mixed-Signal Circuits," in *2021 58th ACM/IEEE Design Automation Conference (DAC)*, 2021, pp. 901–906.

[9] N. R. Aljohani, A. Fayoumi, and S.-U. Hassan, "A novel focal-loss and class-weight-aware convolutional neural network for the classification of in-text citations," *J. Inf. Sci.*, p. 0165551521991022, 2021.

[10] S. Thakur, A. K. Singh, and S. P. Ghrera, "Encryption Based DWT-SVD Medical Image Watermarking Technique Using Hamming Code," in *Proceedings of ICETIT 2019*, Springer, 2020, pp. 1091–1099.

[11] J. Im and S. Cho, "Distance-based self-attention network for natural language inference," *arXiv Prepr. arXiv1712.02047*, 2017.

[12] H. K. Sharaf, M. R. Ishak, S. M. Sapuan, N. Yidris, and A. Fattahi, "Experimental and numerical investigation of the mechanical behavior of full-scale wooden cross arm in the transmission towers in terms of load-deflection test," *J. Mater. Res. Technol.*, vol. 9, no. 4, pp. 7937–7946, 2020.

[13] H. K. Sharaf, S. Salman, M. H. Dindarloo, V. I. Kondrashchenko, A. A. Davidyants, and S. V Kuznetsov, "The effects of the viscosity and density on the natural frequency of the cylindrical nanoshells conveying viscous fluid," *Eur. Phys. J. Plus*, vol. 136, no. 1, pp. 1–19, 2021.

[14] S. H. Raheemah, K. I. Fadheel, Q. H. Hassan, A. M. Aned, A. A. T. Al-Taie, and H. Kadhim, "Numerical Analysis of the Crack Inspections Using Hybrid Approach for the Application the Circular Cantilever Rods," *Pertanika J. Sci. Technol.*, vol. 29, no. 2, 2021.

[15] N. S. Tawfik and M. R. Spruit, "Evaluating sentence representations for biomedical text: Methods and experimental results," *J. Biomed. Inform.*, vol. 104, p. 103396, 2020.

[16] D. S. Kumar and V. M. Rao, "Simultaneous feature selection and classification using fuzzy rules," in *2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT)*, 2018, pp. 125–130.

[17] S. Abujar, A. K. M. Masum, M. Mohibullah, Ohidujjaman, and S. A. Hossain, "An Approach for Bengali Text Summarization using Word2Vector," in *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, Jul. 2019, pp. 1–5, doi: 10.1109/ICCCNT45670.2019.8944536.

[18] A. A. Ismail, M. Gunady, H. Corrada Bravo, and S. Feizi, "Benchmarking deep learning interpretability in time series predictions," *Adv. Neural Inf. Process. Syst.*, vol. 33, pp. 6441–6452, 2020.

[19] M. T. Gençoğlu and S. B. Hasan, "Combining of Cryptography and Steganography for Improving of Security."

[20] A. A. Ismail, M. Gunady, L. Pessoa, H. Corrada Bravo, and S. Feizi, "Input-cell attention reduces vanishing saliency of recurrent neural networks," *Adv. Neural Inf. Process. Syst.*, vol. 32, 2019.

[21] R. Bakthula, S. Shivani, and S. Agarwal, "Self authenticating medical X-ray images for telemedicine applications," *Multimed. Tools Appl.*, vol. 77, no. 7, pp. 8375–8392, 2018.

[22] H. Zhu and T. Huang, "A novel deep quality-aware CNN for image edge smoothening," *Futur. Gener. Comput. Syst.*, vol. 113, pp. 468–473, 2020.

[23] B. B. Hazarika, D. Gupta, and P. Borah, "An intuitionistic fuzzy kernel ridge regression classifier for binary classification," *Appl. Soft Comput.*, vol. 112, p. 107816, 2021.

[24] W.-H. Li, F.-T. Hong, and W.-S. Zheng, "Learning to learn relation for important people detection in still images," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2019, pp. 5003–5011.

[25] D. V Zubarev and I. V Sochenkov, "Cross-language text alignment for plagiarism detection based on contextual and context-free models," in *Proc. of the Annual International Conference "Dialogue*, 2019, vol. 1, pp. 799–810.

[26] F. Yang, Y. Zhao, and R. Cui, "Recognition Method of Important Words in Korean Text Based on Reinforcement Learning," in *China National Conference on Chinese Computational Linguistics*, 2020, pp. 261–272.