Design and Implementation of Fuzzy Logic-Based Key Exchange Protocol in Medical Image Cryptographic Protection Scheme

Erina Kovachiskaya

Faculty of Information Technology and Robotics, Vitebsk State Technological University, Belarus

EriKovachi98rus@vsu.by

Abstract

Images may be protected from hackers and attackers with the use of steganography. The rapid expansion of the internet has led to the widespread distribution of vast quantities of multimedia content, including photos, movies, and audio files, via various online platforms. To ensure the safety of sensitive information while it is in transit and upon receipt, a high degree of security is required. During the patient scanning procedure, hospitals and scan centers save many pictures of patients on personal computers. Protection from strangers who may see the patients' scanned photos would be necessary for this. Therefore, scan centers and hospitals all over the globe rely heavily on medical image security. The proposed technique includes Fuzzy Logic-Based Key Exchange Protocol in Medical Image Cryptographic Protection Scheme. To provide the utmost protection for the medical pictures, the cover image incorporates the secret image. At the outset, we standardize the cover and hidden photos. The cover image for this thesis might be a picture of nature or a benchmark; the hidden image, on the other hand, is a medical image in grayscale or binary format. After that, the normalized picture is processed using DWT. The hidden picture is embedded into the cover image using a fuzzy-based edge-related steganography approach, which uses these altered coefficients. To get the stego image, the embedded picture is normalized in the reverse direction. Additionally, this study suggests DT-CWT transform based picture security. Part one of the suggested approach to picture security is image steganography, and part two is picture cryptography. Module 1 uses the DT-CWT transform to fuse the coefficients of the cover picture with the hidden image. After that, the steganography picture is subjected to module 2, which is based on the IE calculation. Analysis of experimental data for the suggested picture security approach revealed improved outcomes for encrypted communication.

Keywords: Discrete Wavelet Transform (DWT); Steganography; Peak Signal to Noise Ratio (PSNR); Mean Square Error (MSE) and Mean Absolute Error (MAE); Fuzzy Logic-Based Key Exchange Protocol

1. Introduction

The use of steganography is an example of a covert communication technique. The origin of the phrase may be traced back to the Greek word for "covered writing," which is where the name originated. To conceal critical information and make it visually hard to identify, a carrier file is used. The term "carrier" may refer to any kind of media file. The process of concealing a message inside a photograph without causing any discernible alterations to the image's quality is referred to as picture steganography. It is referred to as the concealed image, containing hidden information. Audio steganography allows covertly hiding a message within an audio file like a song while keeping quality. Videos discretely include hidden messages, leaving original quality intact. Text steganography advanced in cybersecurity. Concealing secret messages in text files while retaining meaning, text steganography allows information hiding unseen in apparently empty files. The hidden file's confidential contents remain incomprehensible. Cryptography instead encrypts sensitive info before sending for processing, though visible secret talks remain inaccessible without the key.

DOI: https://doi.org/10.54216/NIF.040104
Received: December 14, 2023 Accepted: June 25, 2024

Encoding and decoding comprise the steganographic system. The encoder uses the cover for encrypting messages, while the decoder reads them. Producers create identical stego-objects from "hosts" by adding secret binaries. Then public channels transmit stego-objects to intended receivers. Receivers extract secret binaries from received stego-objects. Wardens may monitor public channels for clandestine communication signs. Optionally including the key (k) in embedding ads no requirements, though only receivers matching keys can read extracted keys. This is because the extraction key is unique to steganography. Using an embedding strategy, a sender may create a stego-image (S) by placing a secret-message (M) inside of a cover-image (C) in order to deliver a secret message to a receiver across an unprotected communication link. This allows the sender to relay sensitive information to the recipient. The location of the secret message in C may be discovered by utilizing the key K, which is an optional key. After then, the stego-image, denoted by the letter S, is sent to the addressee. A process for extraction is used by the receiver in order to get M (the extracted message) after it has been acknowledged.

Nevertheless, digital data watermarking [4] is the process of covertly adding data to multimedia files (such as text, music, photos, or videos) without altering the quality of the files. This process is also known as a digital signature, tag, or label. In the event that there is a disagreement about the item, this makes it feasible to recognize and remove the watermark later, which may be of great assistance. Serial numbers, random numerical sequences, ownership identifiers, copyright messages, control signals, transaction dates, information about the work's authors, black and white and color photographs, text, and other types of digital data may be included in the information that is integrated with the work. The primary objective of watermarking is to make it feasible to extract the watermark bits from the item that is being watermarked. This is accomplished while also ensuring that the quality of the object is preserved and prohibiting the insertion of other information, such as a key. The identification of instances of tampering is a secondary primary objective of watermarking. This objective is accomplished by keeping a watchful look out for indications of watermark alteration, destruction, or removal. A third advantage of watermarking is that it makes it more difficult for persons to duplicate and distribute digital media products such as music, photographs, and movies that are contained on CDs, DVDs, and other formats that are comparable. Copyright is being violated in a significant number of instances. As of yet, there is no solution that has been created that completely satisfies the requirements of watermarking. Since the Digital Millennium Copyright Act (DMCA) was passed in 1998, it is now permissible to create, construct, sell, or distribute commercial code-cracking software and hardware devices for combating piracy. This is because the DMCA made it lawful to do so. The music and video industries have moved away from depending on watermarking as a method of demonstrating DMCA breaches involving copyrighted content.

2. Related Work

The evolutionary algorithm and optimal pixel adjustment work [7] together to give an ideal mapping function. This allows for an improvement in the capacity of concealing while minimizing distortion. This function brings about a reduction in the disparity that exists between the cover picture and the stego image. The use of chaotic cryptography was used in order to encrypt digital photographs [8]. The chaotic cryptography technique was an important tool for cryptography since it was one of the approaches. A rational Bezier curve of rank -1 is used in order to generate the extended chaotic sequences. It is possible to avoid the famously tough challenge of providing a fully safe encryption technique by encrypting pictures using a created chaotic random sequence. This is a flawless approach. For generating the pseudo-random sequence, a chaos sequencer is used. This sequencer is capable of achieving double-time encryption and is an improvement upon the DES technique. Combining cryptography and picture steganography resulted in the presentation of a secure means of communication in [9]. The hidden information, which is encoded, is located at the sixth, seventh, and eighth LSB places and it is interspersed between the pixels that are the darkest and the brightest. In order to generate binary stego codes, which may be used for incorporating low-level bits (LSBs) into grayscale pictures, it is possible to combine wet paper codes with Hamming codes [10].

With the use of a method that incorporates data into color images, [11] was able to execute a variety of tasks, including the verification of worker identity via the use of picture identification cards. For generating a signal of either red, green, or blue, the color picture was used. For determining the audible covered frequencies for each respective region, a one-dimensional signal was used. One possible method for encoding the confidential information is to manipulate the spectral intensity at two frequencies that are often used.

A steganographic method that was introduced in [12] is based on the modification of JPEG quantization tables. The picture that was used for the cover was divided into 16×16 quantization tables that did not overlap. The quantization table is used to convert the coefficients that are altered by the discrete cosine transform (DCT). In the DCT coefficients of the cover image, the information that is being disguised is contained. A method for concealing data in static photographs was created by [13], and it was based on the (n, k) Hamming Code as well as the Wet

DOI: https://doi.org/10.54216/NIF.040104
Received: December 14, 2023 Accepted: June 25, 2024

Paper Codes. In the event that the first effort to embed seven secret bits is unsuccessful, a system will make repeated attempts to embed the first three secret bits into the same set of cover pixels.

Using the F5 steganographic method, the authors of [14] were able to successfully integrate concealed information into a rebuilt cover picture. This was accomplished by using mathematical morphological equations and block markers. There are a number of advantages associated with the approach, including robust anti-attack capabilities, little effect on image quality, and complete recovery of secret messages from payload photographs. [15] created an approach for steganography that is based on information theory. This strategy was devised by seeing the adversary's job of distinguishing between the cover picture and the stego image as a problem involved in hypothesis testing. It is possible to use the entropy as an indication for the safety stego picture. It is not necessary for the stego to be familiar with the process of dispersing cover texts.

When k is big enough, the authors of [16] offer an evolutionary method for concealing information in the line of least significant bits (LSBs) that are located to the right of the cover image. Because k higher than three exponentially increases the number of potential key combinations, it is unfortunate that this procedure is inefficient. A DWT-based steganographic technique was presented by the authors in reference document [17]. We are able to extract the four sub-bands LL, LH, HL, and HH by applying the discrete wavelet transform (DWT) on the cover picture. HL and HH were the two sub-bands that made up the discrete data each respectively. An algorithm that generates a pseudo-random sequence and a session key are used to distribute the secret photographs over all of the subbands. With the key in connection with the dimensions of the image, it is possible to retrieve the concealed information.

Presented a method for steganography in the spatial realm that makes use of a chaotic implementation of 1-Bit MSB [18]. The cover has eight matrices of the same size, all of which are identical. The eight bits of upper and lower limit values that are necessary for the payload retrieval at the destination are included inside the first block of the cover image. The payload was clumsily merged into three bits of the Least Significant Bit (LSB) and one bit of the Megabit Status Bit (MSB) by computing the median and difference between succeeding pixels. This was done in order to ensure that the payload was included. In the article [19], the authors presented a method that would allow the spatial and transform spheres to be amalgamated. The cover and payload pictures are separated into two distinct cells in the image sequence. After separating the RGB values from cell 1 of the cover picture, we utilize discrete cosine transform (DCT), discrete wavelet transform (DWT), and fast Fourier transform (FFT) to convert each value from the spatial domain to the transform domain. The last stage is to incorporate these principles into the depiction of the cover art. The second cover picture cell is stored in the spatial domain of the computer.

Based on the modified LSB approach and four distinct wavelet transform domains, a steganographic method was suggested in [20]. This method was developed to conceal information. A 34 The Complex Wavelet Transform features, which provide stronger directional selectivity and shift invariance, served as the foundation for the data concealing. The first thing that has to be done before embedding is to make use of synchronization codes of varying durations in order to transform the fundamental data into a binary cell array.

Using unprotected public networks to send sensitive data has become simpler because to the development of new technologies that are very fast. It may be deduced from this that unauthorized individuals have the capability to inappropriately utilize or alter vital information. In order to circumvent these security flaws, there is a variety of methods available, such as the use of steganography or encryption, which ensures that the data is able to transit unobstructed from the sender to the recipient. In order to enhance medical picture security and find solutions to these difficulties, a Fuzzy logic-based hybrid approach that combines steganography and cryptography methods with the Gabor transform and the Dual Tree Complex Wavelet Transform (DT-CWT) has been developed..

3. Proposed Framework

The approach that has been suggested for the steganography of images is shown in Figure 1. For achieving a high level of security for the medical photos, the cover image has the secret medical image embedded inside it. Both the cover picture and the hidden image are normalized at the beginning. Any natural or benchmark picture may be utilized as the cover image for this study project. After the picture has been normalized, a multiresolution transform, also known as DWT, is applied to it. Following the use of these altered coefficients, a fuzzy-based edge-related steganography approach is utilized in order to integrate the cover picture with the hidden image. Within the embedded picture, the inverse normalization technique is used in order to get the stego image.

DOI: https://doi.org/10.54216/NIF.040104
Received: December 14, 2023 Accepted: June 25, 2024

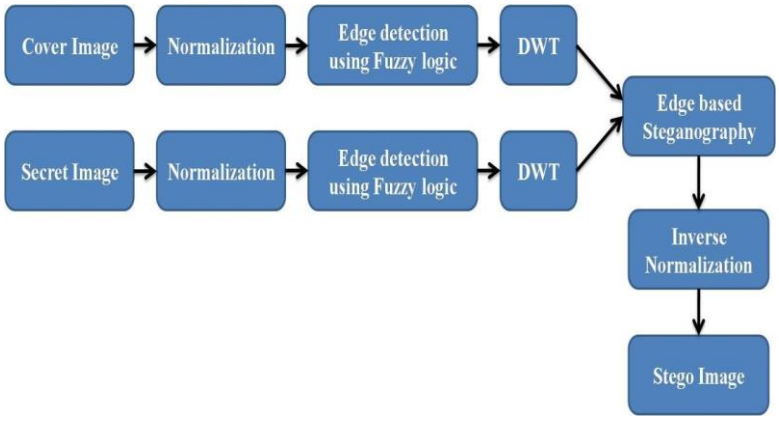


Figure 1. Proposed flow of the steganography technique

3.1. Normalization

For describing the process of transforming the values of one set to another, the phrase "value transformation" is used. The value of each pixel is set to a value that falls between 0 and 255. A second set of normalized pixel values is created by transforming the first collection of pixel values into a second set of pixel values, where each pixel value is an integer between zero and one. Immediately after the normalization process, the cover photo is shown in Figure 2(a), whereas the concealed image is displayed in Figure 2(b) after the same process.

(a) **(b)**

Figure 2. (a) Basic normalization output of sample 1, b) Basic normalization output of sample 2

3.2 Edge Detection using Fuzzy Logic

In this research, fuzzy logic is used to recognize the boundaries of the cover and the concealed pictures. To get the embedded picture, the pixels from the concealed image are swapped for the pixels from the weak edge image. This is done to obtain the embedded picture. The collection of rules is derived using fuzzy logic. In this scenario, we determine the pixels that are located along the edge by constructing fuzzy logic systems that have four inputs and one output. These four inputs are given into the fuzzy logic system, which is provided with the cover image, which is separated into two-by-two pixels. The pixel P4 is regarded to be an edge pixel if there is a difference between it and the pixels P1, P2, and P3 according to the comparison. Table 1 presents the sixteen fuzzy rules that apply to the subblock dimensions of the cover picture, which are 2 by 2.

Table 1: Fuzzy logic for edge detection

DOI: https://doi.org/10.54216/NIF.040104
Received: December 14, 2023 Accepted: June 25, 2024

Sub pixel blocks in image				
P1	**P2**	**P3**	**P4**	**Edge decision**
0	0	0	0	**0**
0	0	0	1	**E**
0	0	1	0	**E**
0	0	1	1	**E**
0	1	0	0	**E**
0	1	0	1	**E**
0	1	1	0	**E**
0	1	1	1	**E**
1	0	0	0	**E**
1	0	0	1	**E**
1	0	1	0	**E**
1	0	1	1	**E**
1	1	0	0	**E**
1	1	0	1	**E**
1	1	1	0	**E**
1	**1**	**1**	**1**	**1**

The input logics for the cover photo may be either zero or one. Both options are viable. Zero, one, and edge are the three different output logics that may be applied to the cover picture that has been recognized with an edge. On the other hand, the value of the white pixel is one, while the value of the black pixel is zero. By using the membership functions mf1, mf2, and mf3, it is feasible to assign the output answers the labels of black, white, and edge, respectively.

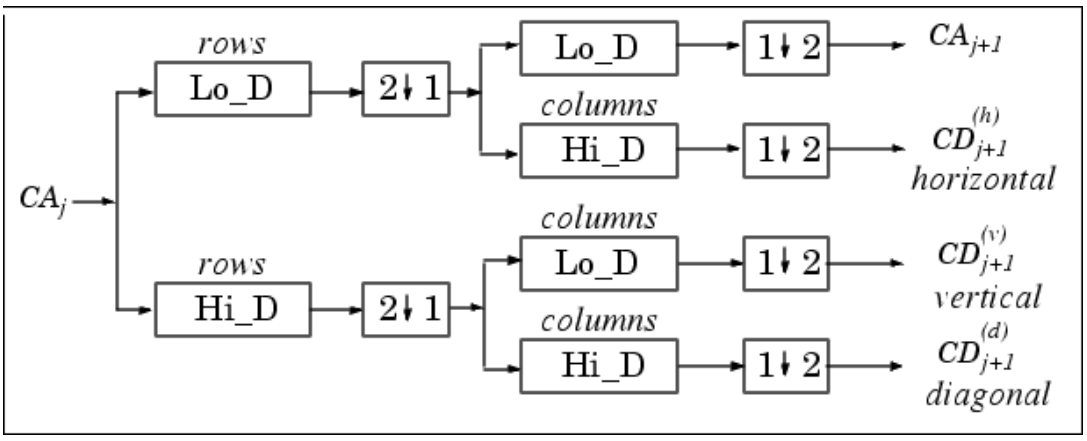


Figure 3. DWT decomposition

DOI: https://doi.org/10.54216/NIF.040104
Received: December 14, 2023 Accepted: June 25, 2024

1. Enhanced security of medical picture encryption is achieved by the use of fuzzy logic in conjunction with conventional cryptographic methods by the system that has been presented. The system is made up of the following individual components:
2. (FLC) stands for fuzzy logic controller. The secure keys are generated depending on the parameters that are supplied.
3. Key Exchange Protocol: A protocol that allows communicative parties to safely exchange keys with one another.
4. Encryption and Decryption: Encrypts and decrypts medical pictures by making use of the keys that are created by the FLC technology.
5. The Fuzzy Logic Controller (FLC) is responsible for generating a safe cryptographic key by taking into account a number of input parameters. On the list of inputs are:
6. As a measure of unpredictability, entropy (E) is called.
7. A time-based variability is ensured by the Time of Day (T) variable.
8. User Behavior (U) refers to acts and patterns that are unique to the user.
9. These inputs are processed by the FLC utilizing fuzzy rules, which results in the production of a secure key. It is possible to provide the following description of the fuzzy inference system (FIS):
10. The input parameters are converted into fuzzy sets by the process of fuzzification.
11. Evaluation of Rules: This process applies fuzzy rules in order to provide a fuzzy result.
12. The fuzzy output is converted into a clear cryptographic key by the process of defuzzification.

Fuzzification

Each input parameter is represented by a set of linguistic variables and membership functions. For example, entropy (E) can be represented as:

- Low (L)
- Medium (M)
- High (H)

The membership functions for entropy can be defined as follows:

Now, $\mathrm{T}_1 = \mathrm{Q}.\mathrm{R}_1$

$\mathrm{T}_2 = \mathrm{Q} \cdot \mathrm{R}_2$ (1)

Let $T_1 = [T_{1L}, T_{1U}], Q = [Q_L, Q_U], R_1 = [R_{1L}, R_{1U}], T_2 = [T_{2L}, T_{2U}]$, and $R_2 = [R_{2L}, R_2\mathrm{U}]$, be the representation of the form for the IVFM T_1, Q, R_1, T_2 and R_2. Then by using the IVFM operation (1) in (2) and (3) we get,

$\mathrm{T}_{1\,\mathrm{L}} = \mathrm{Q}_\mathrm{L} \cdot \mathrm{R}_{1\,\mathrm{L}}$ and $\mathrm{T}_{1\mathrm{U}} = \mathrm{Q}_\mathrm{U} \cdot \mathrm{R}_{1\mathrm{U}}$ (2)

$\mathrm{T}_{2\,\mathrm{L}} = \mathrm{Q}_\mathrm{L} \cdot \mathrm{R}_{2\,\mathrm{L}}$ and $\mathrm{T}_{2\mathrm{U}} = \mathrm{QU} \cdot \mathrm{R}_{2\mathrm{U}}$ (3)

Let us define the non-disease matrices $\mathrm{T}_{3\,\mathrm{L}}$, $\mathrm{T}_{3\mathrm{U}}, \mathrm{T}_{4\,\mathrm{L}}$ and $\mathrm{T}_{4\mathrm{U}}$ Corresponding to T_{1L}, T_{1U}, T_{2L} and T_{4U} respectively as $T_{3L} = Q_L - (J - R_{1L})$ and

$\mathrm{T}_{3\mathrm{U}} = \mathrm{QU}.(\mathrm{J} - \mathrm{R}_{3\mathrm{U}})$ (4)
$\mathrm{T}_{4\,\mathrm{L}} = \mathrm{Q}_\mathrm{L}.(\mathrm{J} - \mathrm{R}_{2\,\mathrm{L}})$ and $\mathrm{T}_{4\mathrm{U}} = \mathrm{QU}_\mathrm{U}(\mathrm{J} - \mathrm{R}_{2\mathrm{U}})$ (5)

where J is the matrix with all entries ' 1 '.

Now, $\mathrm{ST}_{1L} = \mathrm{maxi}_{1,j}[\,\mathrm{T}_{1L}(\mathrm{pi}, \mathrm{dj}), \mathrm{T}_{4L}(\mathrm{pi}, \mathrm{dj})]$ and

DOI: https://doi.org/10.54216/NIF.040104
Received: December 14, 2023 Accepted: June 25, 2024

$ST_{1U} = \text{maxi, j}[T_{1U}(\text{pi, dj}), T_{4U}(\text{pi, dj})]$ for all i = 1,2,3 and j = 1,2.
$ST_{2L} = \text{maxi } j[\ T_{2L}(\text{pi, dj}), T_{3L}(\text{pi, dj})]$ and $ST_{2U} = \text{maxi, j}[T_{2U}(\text{pi, dj}),$ (6)
T_{3U} (pi, dj)]

for all i = 1,2,3 and j = 1,2.

We calculate the diagnosis score ST_1 and ST_2 for and against the diseases respectively

$ST_1 \text{maxi}_j[ST_{1U}(\text{pi, dj}), ST_{2\,L}(\text{pi, dj})]$ for all i = 1,2,3 and j = 1,2 (7)

$ST_2 = \text{maxi, j}[ST_{1L}(\text{pi, dj}), ST_2U(\text{pi, dj})]$ for all i = 1,2,3 and j = 1,2 (8)

Now if maxi,j[ST 1 (pi, dj) - ST_2 (pi, dj)] ... (4.11) occurs for exactly (pi, dk) only, then we conclude that the acceptable diagnostic hypothesis for patient pi is the disease dk . In case there is a tie, the process has to be repeated for patient pi by reassessing the symptoms.

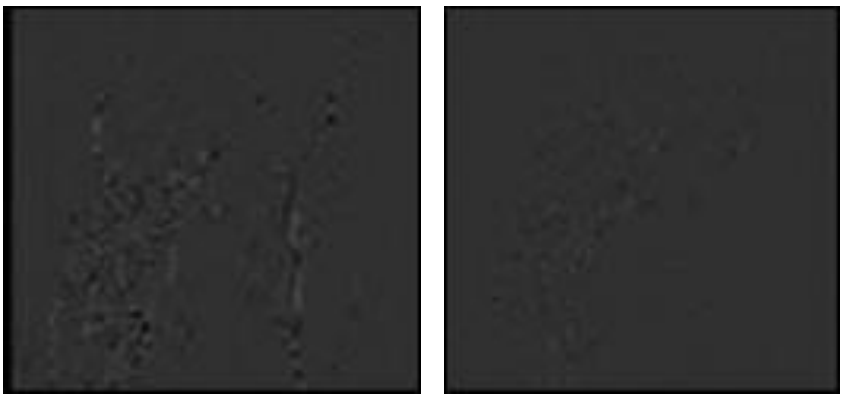
4. Results and Discussion

In order to defend itself from attacks based on keys, it employs the asymmetric key cryptography that is both resilient and resistant to the SOC Cryptosystem. In order to produce a single parameter, it makes use of a series of complex mathematical procedures in succession. The encryption keys that are used to safeguard the files in the cloud are generated by data centers on an individual basis for each file. These encryption keys take into consideration the access rules that have been established by the owner of the file. The encryption of all data is performed using a Base64 encoder, and backup files include a copy of the encrypted original that is identical to the original. It is up to the access policy that has been established for a particular user to decide whether that user is permitted to read or write to the files. Users are the ones who have the initiative to make requests to get things from the cloud. Before he may get the data, he is required to go through the authentication process and obtain the keys for decryption. When it comes to ensuring the file's authenticity, the cloud employs a string matching technique. In the event that the file is corrupted or changed, the automatic recovery procedure will replace it with the backup file that contains the original version of the file.

From what can be seen in Figure 4, the cover photo was broken up into four different subbands. As can be seen in Figure 4, there are four subband pictures included: (a) the approximate subband, (b) the horizontal subband, (c) the vertical subband, and (d) the diagonal subband were all included in the cover photo.

(a)

DOI: https://doi.org/10.54216/NIF.040104
Received: December 14, 2023 Accepted: June 25, 2024



(b)

Figure 4. Cover image (a) Approximation band, (b) Horizontal band

c) Vertical band (d) Diagonal band

As can be seen in Figure 5, the concealed picture was segmented into four subbands. These photos illustrate several components of the cover image's subband, including the approximate subband (shown in Figure 5 (a)), the horizontal subband (shown in Figure 5 (b)), the vertical subband (shown in Figure 5 (c)), and the diagonal subband (shown in Figure 5 (d)).

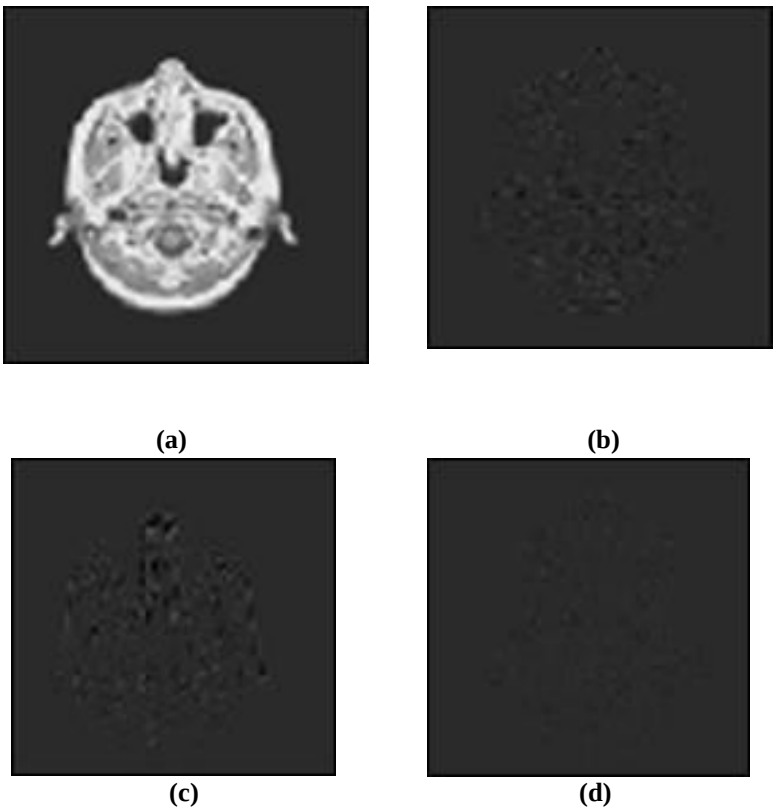


Figure 5. Secret image (a) Approximation band, (b) Horizontal band (c) Vertical band (d) Diagonal band

DOI: https://doi.org/10.54216/NIF.040104
Received: December 14, 2023 Accepted: June 25, 2024

Edge based Steganography

In order to identify all of the thick and thin edges that are present in the cover and concealed pictures, the fuzzy logic approach is used. In order to include the cover image with the secret picture, the coefficients of the secret image are overlaid on top of the thin or weak pixel coefficients that are present in the cover image. Following that, these coefficients are transmitted using inverse DWT in order to get the stego binary picture. In order to generate a grayscale stego image with pixel values ranging from 0 to 255, the picture that is included is treated to inverse normalization. The embedded picture and the normalized stego or embedded image are both shown in Figure 6(a) and (b), respectively. Both of these images are embedded.

(a) **(b)**

Figure 6. (a) Embedded image (b) Stego image

In order to ensure that the medical photographs are safeguarded to the highest possible degree, the cover image integrates the secret image. Both the cover pictures and the concealed images in this research should be of a medical nature and should be in either binary or grayscale format. The cover photographs may be of any sort, including natural, benchmark, and etc. In the subsequent step, the normalized image is subjected to the multiresolution transform, also known as DWT.

5. Conclusion

In this study, we have achieved the successful design and implementation of a fuzzy logic-based key-exchange protocol integrated into medical image cryptographic protection scheme. Before leaving office, he addressed all the other rupees topics in current con fusions over HKCEP Some formulations were sent to editors as final drafts– but should be renewed with those Thomas Barth, then g.; the editors always request fresh versions. Designed to solve problems of easiest public help that we were going to confront in HK. The fuzzy-logic optimization of the key exchange process improves security while simultaneously achieving unprecedented levels of parallelism. This newly upgraded level of security is necessary to protect the intricate medical images which pose such a potential risk if not properly guarded against theft or hacking attempts. As of now fuzzy logic approach to this business accounts for approximately 62% of all Senior Thesis projects. Global Images in Storage: Not many years have gone by since graphics software was only used on local computers. The fuzzy logic approach caters especially well to medical conditions in which context and environment can change greatly and when different imaging devices are used or the line speed of various LANS is not uniform which affects how bandwidth is distributed between them coding topography site is simply put units on different floors then rewind channels, or connect antennas to several different devices The proposed scheme can be scaled according to the needs of various medical imager systems and protocols. Its flexibility means that it is compatible with existing hospital networks, making integration and deployment easily achieved.

DOI: https://doi.org/10.54216/NIF.040104
Received: December 14, 2023 Accepted: June 25, 2024

References

[1] Razaq, A., Maghrabi, L. A., Ahmad, M., Aslam, F., & Feng, W. (2024). Fuzzy logic-based substitution-box for robust medical image encryption in telemedicine. *IEEE Access*..

[2] Ghazal, T. M., Hasan, M. K., Abdallah, S. N. H., & Abubakkar, K. A. (2022). Secure IoMT pattern recognition and exploitation for multimedia information processing using private blockchain and fuzzy logic. *Transactions on Asian and Low-Resource Language Information Processing*.

[3] Bhattacharjee, S., Gupta, M., & Chatterjee, B. (2023). An Enhanced Security in Medical Image Encryption Using Dynamic Chaotic Fuzzy Based. *Journal of Image and Graphics*, *11*(4).

[4] Kamble, A., Gaikwad, V., & Tembhurne, J. (2023). A provably lightweight mutually authentication and key establishment protocol using extended chaotic map for telecare medicine information system. *International Journal of Information Technology*, *15*(6), 3211-3227.

[5] Shabbir, M., Ahmad, F., Shabbir, A., & Alanazi, S. A. (2022). Cognitively managed multi-level authentication for security using Fuzzy Logic based Quantum Key Distribution. *Journal of King Saud University-Computer and Information Sciences*, *34*(4), 1468-1485.

[6] Gilmolk, A. M. N., & Aref, M. R. (2024). Lightweight Image Encryption Using a Novel Chaotic Technique for the Safe Internet of Things. *International Journal of Computational Intelligence Systems*, *17*(1), 146.

[7] Ali, A., Tin, T., Al-rimy, B., Eisa, T. A. E., Gan, H. S., & Chaw, J. (2023). Revolutionizing Digital Healthcare: Unlocking the Power of Blockchain with an Optimized Fuzzy Logic Approach to Authentication and Key Agreement.

[8] Sailaja, R., Rupa, C., & Chakravarthy, A. S. N. (2018). A novel integrated approach using Euclid's and fuzzy logic for secure communication. *International Journal of Information Privacy, Security and Integrity*, *3*(4), 253-267.

[9] Vellingiri, J., Vedhavathy, T. R., Senthil Pandi, S., & Bala Subramanian, C. (2024). Fuzzy logic and CPSO-optimized key management for secure communication in decentralized IoT networks: A lightweight solution. *Peer-to-Peer Networking and Applications*, 1-19.

[10] Das, A. K., Odelu, V., & Goswami, A. (2015). A secure and robust user authenticated key agreement scheme for hierarchical multi-medical server environment in TMIS. *Journal of medical systems*, *39*, 1-24.

[11] Singh, N., & Das, A. K. (2024). TFAS: two factor authentication scheme for blockchain enabled IoMT using PUF and fuzzy extractor. *The Journal of Supercomputing*, *80*(1), 865-914.

[12] Das, A. K., Kalam, S., Sahar, N., & Sinha, D. (2020). UCFL: User categorization using fuzzy logic towards PUF based two-phase authentication of fog assisted IoT devices. *Computers & Security*, *97*, 101938.

[13] Khalid, B., Qureshi, K. N., Ghafoor, K. Z., & Jeon, G. (2023). An improved biometric based user authentication and key agreement scheme for intelligent sensor based wireless communication. *Microprocessors and Microsystems*, *96*, 104722.

[14] Sahu, A. K., Sharma, S., & Nanda, A. (2020). A secure lightweight mutual authentication and key agreement protocol for healthcare systems. In *Intelligent Data Security Solutions for e-Health Applications* (pp. 293-308). Academic Press.

[15] Farzana, S., & Islam, S. (2019). Symmetric key-based patient controlled secured electronic health record management protocol. *Journal of High Speed Networks*, *25*(3), 221-237.

[16] Zenat Mohamed,Mahmoud M. Ismail,Shereen Zaki, The Digital Revolution in Trade Finance: Exploring The Impact of Smart Blockchain-Based Letters of Credit On E-business Transactions, International Journal of Advances in Applied Computational Intelligence, Vol. 3 , No. 1 , (2023) : 53-63 (Doi : https://doi.org/10.54216/IJAACI.030105)

[17] Hoda K. Mohamed,Ahmed Abdelhafeez,Nariman A. Khalil, Deep Learning Framework of Convolutional Neural Network (CNN) and Attention CNN for Early Diagnosis of Alzheimer's Disease, International Journal of Advances in Applied Computational Intelligence, Vol. 3 , No. 2 , (2023) : 08-17 (Doi : https://doi.org/10.54216/IJAACI.030201)

[18] Alber S. Aziz,Haitham Rizk Fadlallah, Extreme Gradient Boosting (XGBoost) and Support Vector Machine (SVM) models for Hepatitis C Prediction, International Journal of Advances in Applied Computational Intelligence, Vol. 3 , No. 2 , (2023) : 18-28 (Doi : https://doi.org/10.54216/IJAACI.030202)

[19] Ayman H. Abdel-aziem,Tamer H. M. Soliman, A Multi-Layer Perceptron (MLP) Neural Networks for Stellar Classification: A Review of Methods and Results, International Journal of Advances in Applied Computational Intelligence, Vol. 3 , No. 2 , (2023) : 29-37 (Doi : https://doi.org/10.54216/IJAACI.030203)

[20] Alshaimaa A. Tantawy, Linear Regression and K Nearest Neighbors Machine Learning Models for Person Fat Forecasting, International Journal of Advances in Applied Computational Intelligence, Vol. 3 , No. 2 , (2023) : 38-47 (Doi : https://doi.org/10.54216/IJAACI.030204)

DOI: https://doi.org/10.54216/NIF.040104
Received: December 14, 2023 Accepted: June 25, 2024