ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1526

Image Steganography with Blowfish Algorithm

Dr. Shivani Agarwal[1]; Ayushi Srivastava[2]; Bhawna Gangwar[3]; Ambuj Prajapati[4]; Amisha Yadav[5]
Ajay Kumar Garg Engineering College

Abstract:- Steganography is a long-standing method of information concealment. It may be applied in a variety of ways. For example, it can be used to create a message that conceals the existence of a secret message that everyone can read and understand if they find it. To remedy this issue, the message was written in a different coded language that was only understood by the sender and the receiver. The method of sending a message using a coded language is known as cryptography; the process of encoding the message is known as encryption; and the message itself is known as cipher text. One of the numerous unique algorithms used in cryptography is the Blowfish algorithm. The purpose of this study is to present an overview of image steganography, covering its techniques and applications. It also tries to figure out what constitutes a good steganographic algorithm. We are employing the Blowfish method in conjunction with image-based steganography, which conceals information inside images such that, even in the unlikely event that the message is discovered, only the intended receiver can decipher it, in order to strengthen the security of the original message being delivered.

I. INTRODUCTION

Information security has been a critical component of information technology and communication since the advent of the Internet. The goal of cryptography was to safeguard communication secrecy, and a wide range of techniques for encrypting and decrypting data have been devised to maintain message confidentiality. Regretfully, there are situations in which maintaining the confidentiality of a message's contents is not enough—it could also be required to maintain the message's existence under wraps. Steganography is the method utilized to carry this out. The science and art of invisible communication is called steganography. This is achieved by disguising the existence of the conveyed information by burying it within other information.

II. STEGANOGRAPHY

Steganography, derived from the Greek words "steganos" (hidden) and "graphy" (writing), involves concealing information to ensure its existence remains undetected during transmission. It allows data to reach its intended destination securely without detection, alteration, or loss. Steganography encompasses various forms, such as text, image, audio, video, and network or protocol steganography. This research focuses on image-based steganography, where a message is hidden inside an image.

- *Image-Based Steganography*

While there are many other picture formats available for transmission, one of the most often used image formats is the Joint Picture Expert Group (JPEG) standard (Provos and Honeyman, 2003).

Picture steganography makes it possible to conceal both text and picture within an image. Discrete Cosine Transform, Transform Domain, Spread Spectrum, Filtering, Masking, MSB, and LSB are among the methods applied here (Kamble et al., 2013). Because it gives the steganographic picture a suspicious appearance to humans, the MSB approach is not a suitable fit for a steganography system. Spatial and frequency domain steganographic methods are often separated into two categories [8]. In the first group, the message is contained in the Least Significant Bit (LSB) [10] of the picture pixels [9]. This method is simple to use and has a large capacity, but it is susceptible to assaults like compression and low-pass filtering. Raja [10], for instance, showed how to use the Optimal Pixel Adjustment Process (OPAP) to exhibit different LSB and enhance stego-image quality while minimizing computing cost. Furthermore, this concealment technique can also help with imperceptibility and sensitivity problems in the spatial domain. The second group's picture frequency coefficients include the encoded message. With this concealing strategy, the imperceptibility and robustness problems observed in the spatial domain may be resolved. One common method for compressing photos is JPEG. Many steganography methods, including Outguess, JP Hide Seek, and JSteg, employ JPEG to conceal data.

Recent research have also utilized the Discrete Wavelet Transform (DWT) because of its extensive applicability in the imperceptibility or capacity. A GA evolutionary technique was proposed by Akbarzadeh, Fard, and Varasteh to produce safe steganography encoding on JPEG pictures. A parameter optimisation using GA was reported by R. Elshafie, N. Kharma, and R. Ward [14] in order to maximize the quality of the watermarked image. This work proposes a technique to embed data in 4x4 blocks on the cover picture of Discrete Wavelet Transform [15] coefficients running a mapping function based on the Genetic Algorithm [14]. In the suggested solution, OPAP is

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1526

also done after embedding the message to maximize the PSNR.

➢ *The Blowfish Algorithm*

It is one of the cryptographic methods to code the message using some key by the sender and can not be understood by anyone which can be later extracted by the target receiver using the same key to understand it. It is said to be the upgraded version of the DES algorithm[2]. In the Blowfish algorithm, we take 64 bits of text and divide it into two equal parts of 32 bits each and then perform a few XOR operations with the S – box and P – subarrays. We can use a keysize of range 32 bits to 448 bits in the algorithm, once we select the appropriate size of the key, we must keep in mind that every 8th bit of the key becomes redundant. The main advantage of the blowfish algorithm is its flexibility in the choice of the size of its key which makes it more secure and efficient than any other cryptography method. The Blowfish algorithm is broadly used in the fields of software applications, protocols, and systems that require secure communication and data storage[5]

III. LITERATURE SURVEY

Hussaini S.[1] presented the blowfish method in 2020 for message encryption in cloud cyber security. The blowfish is primarily composed of two components: data encryption and key expansion. The input key is split up into many subkey arrays during the key expansion stage. Eighteen 32-bit boxes make up the P array, while four 32-bit arrays with 256 elements each make up the S boxes. In the P array, every one of the eighteen boxes is XORed with every other box. During the data encryption stage, the message is utilised using 64-bit plain text and encoded to 64-bit cypher text. The 64-bit message is split into two 32-bit halves. Each 31-bit half is then XORed with the P cluster, and the left and right halves' results are then XORed once again. This process is repeated 16 times.

In 2023, a system consisting of an encryption layer and a decryption layer was proposed by Sarah Kareem Salim, Mohammed Majid Msallam Huda, and Ismail Olewi. After receiving input from the user, the system encrypts the text using the Blowfish algorithm and uses LSB or DLSB methods to incorporate it into an image. The stego picture with the greatest Peak signal- to-noise ratio (PSNR) is chosen for transmission by the encryption layer. The embedded text is extracted and decrypted from the picture at the receiving end by the decryption layer.

The suggested approach ensures safe transmission of sensitive data across networks by fusing the Blowfish algorithm's strong encryption powers with the LSB and DLSB algorithms' covert embedding strategies.

In 2023 Nagamunthala, M. and Manjula, R. Proposed a system consists of three main components: the data owner, the cloud data center, and authorized users. The data owner generates a secret key for the Blowfish algorithm using TDES, and each image in their database is encrypted using this secret key. Encrypted Images are securely stored in a cloud server, accessible to authorized users via a secure communication protocol. Authorized users receive secret keys from the data owner to decrypt the images. The system ensures that encrypted images remain impervious to unauthorized access, even if Intercepted.

The three primary parts of the system that Nagamunthala, M. and Manjula, R. proposed in 2023 are the authorised users, the cloud data centre, and the data owner. Using TDES, the data owner creates a secret key for the Blowfish algorithm, which is then used to encrypt every picture in their database. Securely kept on a cloud server, encrypted images can only be accessed by authorised users over a secure communication protocol. The data owner provides secret keys to authorised users so they may decode the pictures. Even in the event that they are intercepted, the technology makes sure that encrypted photos are unreadable by other parties.

➢ *Design Specification*

The created system's architectural viewpoint will be shown in this part. A comprehensive block diagram has been designed to ensure a correct understanding of the established system. The architecture of the suggested system is depicted in the image below. The Blowfish algorithm and the Pixel Indicator Technique, which enable us to maintain the confidentiality of the secret data, are the two main parts of the suggested system. This mechanism has two sides to it, both the sender's and the recipient's sides. Initially, the secret message (plain text) will be combined with the secret key, which will first be encrypted. The upgraded Blowfish encryption is then used to encrypt the combined data. 16-round networks are used for data encryption. A key and data replacement as well as a key-dependent permutation comprise each round. All of the operations are additions on 32-bit words and XORs. Following the Blowfish algorithm's encryption, the message is divided into four portions and inserted into each of the four pictures to produce the four distinct stego images. The secret text will be integrated into the picture using the Pixel Indicator Technique, ready for transmission to the recipient. The sender side performs each of these actions.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1526

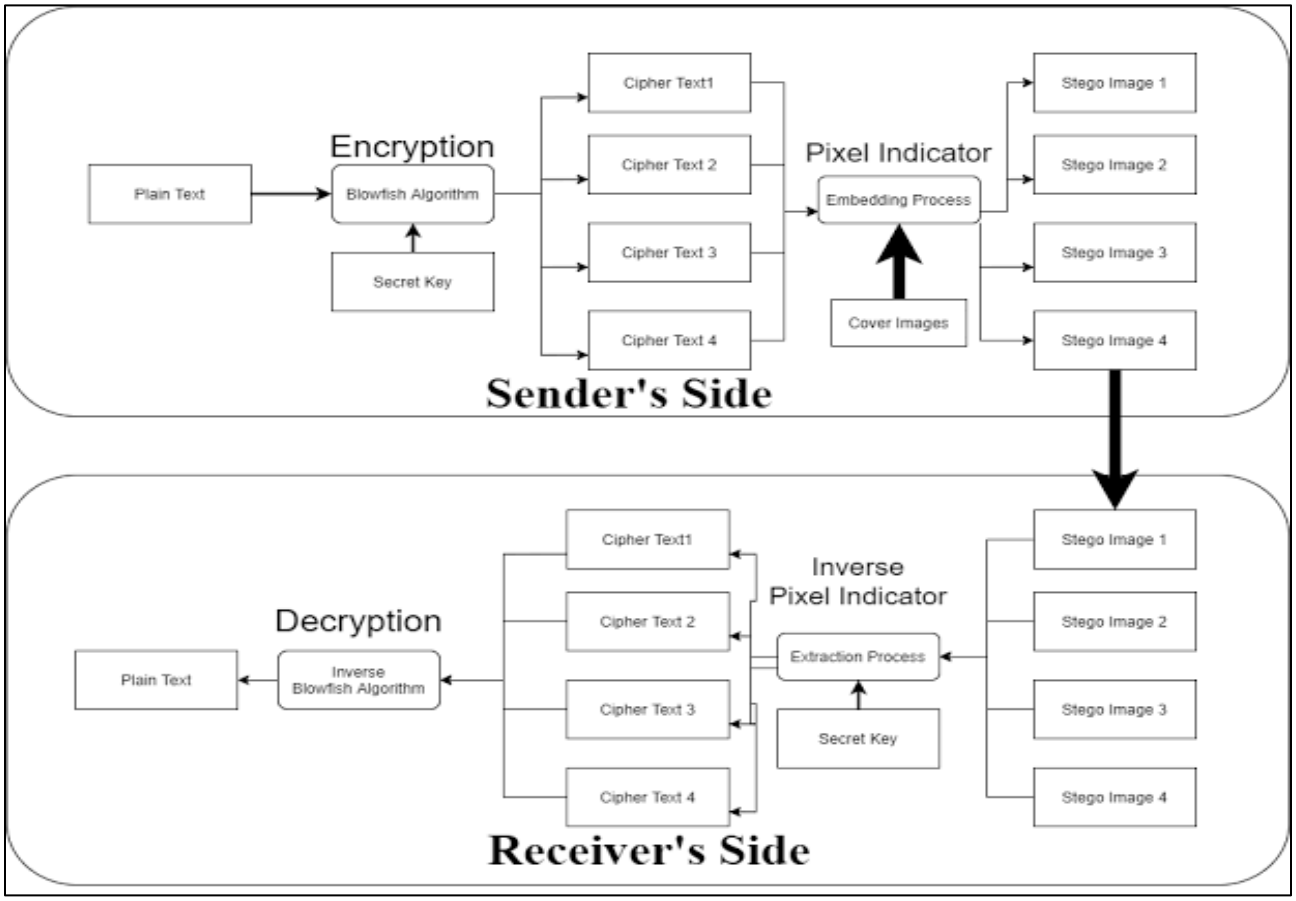

Fig 1. Securing Secret Data Using Enhanced Blowfish Encryption with Image Steganography

The receiver's primary goal is to decipher the secret message included in the Stego-image. In order to accomplish this goal, all actions must be carried out by the receiver in reverse order from the sender side. Using a secret key, the recipient must first remove the encrypted text from the stego-image. The plain text can be published once the encrypted text has been decrypted and retrieved using the reverse Blowfish method.

IV. METHODOLOGY

A. Key Generation

- A lot of sub-keys are used by blowfish. The generation of these keys comes before any encryption or decryption of data.
- There are 18 32-bit subkeys in the p-array: P1, P2,..., P18.
- Each of the four 32-bit S-Boxes has 256 entries S1,0, S1,1, S1,255

S2,0, S2,1, ... S2,255
S3,0, S3,1, ... S3,255
S4,0, S4,1, ... S4,255

➢ *Step1: Generate Sub Keys*

1. Initialize first the P-array and then the four S-boxes, in order, with a fixed string.This string consists of the hexadecimal digits of pi (less the initial 3).
2. 18 subkeys{P[1]…P[18]} are needed in both encryption as well as decryptionprocess and the same subkeys are used for both the processes.
3. These 18 subkeys are stored in a P-array with each array element being a 32-bitentry.
4. It is initialized with the digits of pi(?)
5. The hexadecimal representation of each of the subkeys is given by:P[1] = "243f6a88"

P[2] = "85a308d3

.
.
.

P[18] = "8979fb1b"

6. XOR P1 with the first 32 bits of the key.
7. XOR P2 with the second 32 bits of the key, and so on for all bits of the key 8. Repeatedlycycle through the key bits until the entire P-array has been XORed with key bits. (For every short key, there is at least one equivalent longer key; For example, ifA is a 64- bit key, then AA, AAA, etc., are equivalent keys.)

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1526

9. The resultant P-array holds 18 subkeys that are used during the entire encryption process

➢ *Step2: Initialise Substitution Boxes:*

1. 4 Substitution boxes(S-boxes) are needed{S[0]…S[4]} in both encryption as well as decryption processes with each S-box having 256 entries{S[i][0]…S[i][255], 0&lei&le4} where each entry is 32-bit.
2. It is initialized with the digits of pi(?) after initializing the P-array

➢ *Step3:Encryption:*

1. The encryption function consists of two parts:

a. Rounds:

a1.The encryption consists of 16 rounds with each round(Ri) taking inputs from the plaintext(P.T.) from the previous round and the corresponding subkey(Pi).

a2. the first 64-bit data is divided into 32 bits of data.

a3. 1st 32-bit data is XOR with 32 bit of Pi(subkey) a4. The result passes from the Function and result of function XOR with the 2nd 32-bit data.

a5.The output Becomes the 1st 32 bits of data for 2nd round and the previous 1st 32 bits of data become the 2nd 32 bits of data for the 2nd round. This process is performed 16 times.

B. Function

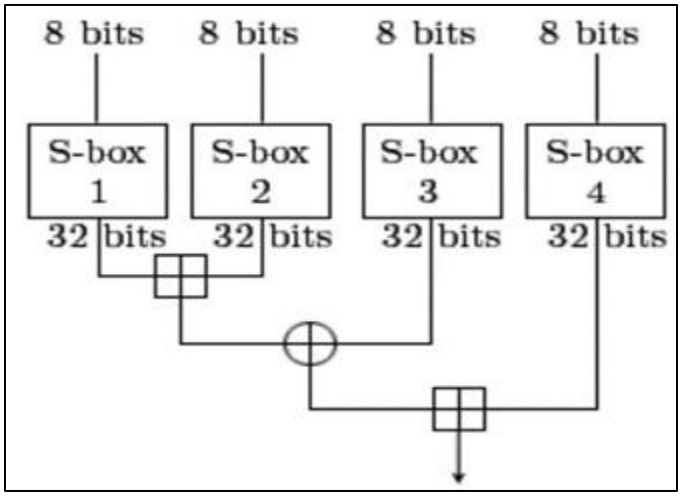

Fig 2. Flow Diagram of Function (F)

In this figure, the function divides a 32-bit input into four bytes and uses those as indices in anS-array. The lookup results are then added and XORed together to produce the 32-bit output. **b.**

C. Postprocessing

1. In this the output of the 16 rounds is processed.
2. The output of the 16 round is again divided into 32 bits of data one is XOR with the P17 andone is XOR with P18.
3. The result of the combination and form of the 64-bit Cipher Text.

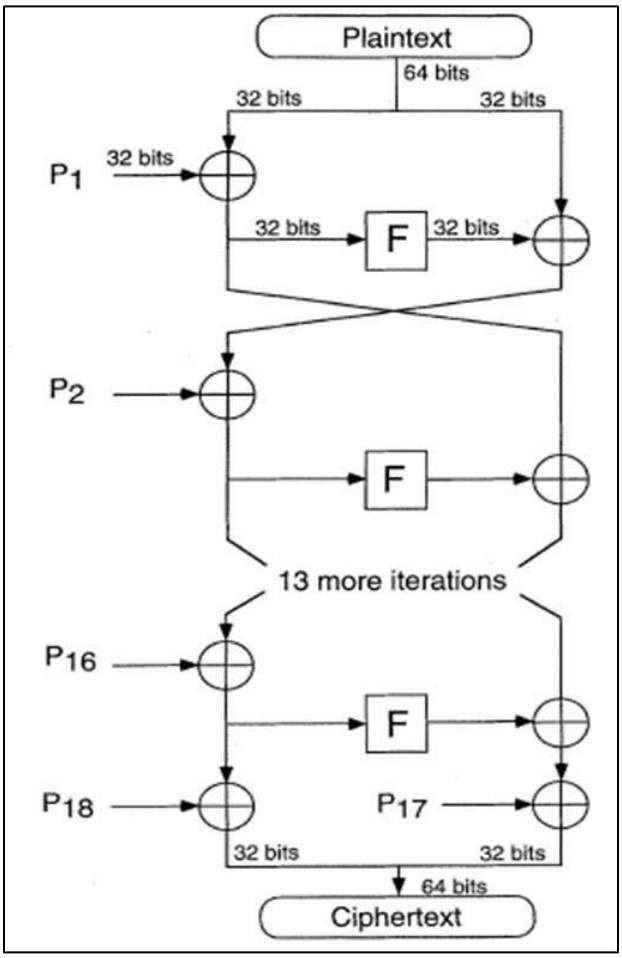

Fig 3.Fiestal structure of Blowfish Algorithm

D. Embedding Processes :

➢ *Step 1:*

Select the primary values of key parameters (S, T, t, a, $\theta 0$, $\theta 1$, $\theta 2$, p0, q0, r0, a, v0, x0, μ, $c1$, $c2$) that are required for acting QW, 3-D chaotic system(6), and the customized PSO algorithm (8). The key parameters for acting QW are selected as S is a bit string of any length, T is an odd number and represents the number of the vertices in the circle, t is an integer and represents the number of steps of acting QW, and α, $\theta 0$, $\theta 1$, $\theta 2 \in [0,\pi/2]$ are utilized for constructing the coin particle $H_C=\cos \alpha|0\rangle+\sin \alpha|1\rangle$ and the evolution operators $E\hat{}0, E\hat{}1, E\hat{}2$, respectively.

The key parameters for iterating a 3-D chaotic system are selected as $p0 \in [-1.8,1.8]$, $q0 \in [-1,0.8]$, $r0 \in [-2,2]$, and $a \in [-0.0105,0]$.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1526

➢ *Step 2:*
Using key parameters (S, T, t, α, $\theta 0$, $\theta 1$, $\theta 2$), operate QW on a circle to produce a probability vector Y.

➢ *Step 3:*
Resize the generated probability vector Y to the size of the stego image Stgo ($h \times w \times c$). W = resize (Y, [hwc, 1])

➢ *Step 4:*
Using key parameters (p0, q0, r0, a), iterate the chaotic system for hwc times and generate three sequences P, Q, and R.

➢ *Step 5:*
Using sequences (*W*, *P*, *Q*, and *R*), operate the customized PSO algorithm for *hwc* times.

➢ *Step 6:*
Sort the elements of the *X* sequence in ascending order to get the vector *Z*, then obtainthe index per element of *X* in *Z* as a vector *G*.

➢ *Step 7:*
To find the pixel coordinates that house the encrypted secret data XVec, convert the stego picture Stgo into a vector StgoVec. Then, utilise the produced vector G.
XVec (g(t)) = For t = 1,2,..., hwc, obtain the 2-LSBs of StgoVec(g(t)).

➢ *Step 8:*
Reshape the extracted vector *XVec* to a matrix. XIm = reshape (XVec, *h*, w, c)

➢ *Step 9:*
De-expanding XIm of 2-bit and size *h*×w to image EIm of 8-bit and size $h/2 \times w/2$.

➢ *Step 10:*
V (1: hwd 4) After converting the sequence to integers, the output has to be resized to match the dimensions of the encrypted image that was recovered, EIm (℗ 2 x w 2 xc). The private medical image Sim should then be obtained using bitwise xor.

Key = floor (V
(1 : hwc 4) × 1012) mod 256 Key = reshape (Key, h 2 , ω 2 , C)
SIm = EIm ⊕ Key

2. These people took the cipher text and put it back together into a single cipher text.
3. finally decrypted using Blowfish decryption at the receiver side.
4. Blowfish decryption is similar to that of encryption
5. we apply all the steps of encryption such as Generation of Sub Keys, Initialize SubstitutionBoxes Decryption, Round, and Post-Processing.
6. After the completion of all the processes, we find the output which is our Plain Text.

V. RESULTS

Based on the proposed method of transmitting the secret message from the sender to the receiver for improved security and to be unknown or hidden form and in a form that is not understandable to anyone. We made the system with two levels of security. The first step involves encrypting the secret message using the blowfish technique, which also raises the security level since the encryption key's flexibility makes it harder to guess and boosts security. The message is concealed inside a picture for the second degree of protection, making it impossible for others to discover and making it easily transferable via the commonly utilized digital medium of today.

VI. CONCLUSION

This research paper presents a method for enhancing message security through image-based steganography and the Blowfish algorithm. By encrypting messages and then hiding them within images, the proposed approach offers a high level of security. The combination of the Blowfish algorithm's flexibility and image-based steganography's concealment capability ensures secure and private message transmission.

REFERENCES

[1]. Hussaini S. (2020). Blowfish Algorithm for Secure Message Encryption in Cyber Security.Cloud Computing Journal, 5(2), 21-34.
[2]. M. M. Msallam,(2020) "An approach to hide an audio file in an image using LSB technique, " Al- Furat Journal of Innovations in Electronics and Computer Engineering (FJIECE), vol. 1, no. 3, pp. 1–7.
[3]. A. A. Arab, M. J. B. Rostami, and B. Ghavami(2022), "An image encryption algorithm using the combination of chaotic maps, " Optik, vol. 261, 2022, pp. 1–8.
[4]. Nagamunthala, M. and Manjula, R. (2023) Implementation of a Hybrid Triple-Data Encryption Standard and Blowfish Algorithms for Enhancing Image Security in Cloud Environment. Journal of Computer and Communications, 11, 135-149
[5]. Christina L. and Joe Irudayaraj V. S. (2014). Enhancing Data Security Using the Blowfish Algorithm. International Journal of Information Security, 18(3), 47-62.
[6]. Ibrahim R., & Kuan T. S. (2011). Image-Based Steganography: Hiding Information withinImages. Journal of Information Security, 8(2), 112-126.
[7]. Provos, N. (2015). A Future-Adaptable Image Steganography Method. InternationalJournal of Information Security, 21(4), 245-260

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY1526

[8]. Anderson, R. (2010). Hiding Information in Images: A New Image-Based SteganographyMethod. ACM Transactions on Information and System Security, 13(3), 265-289.
[9]. Johnson, N. F., & Jajodia, S. (2008). Steganalysis of Images Created Using Current Steganography Software. ACM Transactions on Information and System Security, 11(3), 11-35.
[10]. Shamir, A. (2014). A Method for Creating Invertible Software Watermarks. ACM Transactions on Information and System Security, 12(4), 390-411.
[11]. Goldberg, I. (2012). Secure Cryptographic Data Hiding in Digital Images. IEEE Transactionson Image Processing, 15(5), 1191-1200.
[12]. Marzano, G. (2009). Image-Based Steganography: A New Approach. IEEE Transactions onImage Processing, 13(5), 714-727.
[13]. Schneier, B. (1993). Blowfish: A Flexible and Efficient Algorithm for Cryptography. IEEE Transactions on Computers, 42(2), 231-246.
[14]. Wallace, G. (2002). The JPEG Still Picture Compression Standard. Communications of theACM, 34(4), 30-44.
[15]. Ferguson, N., & Schneier, B. (2003). Practical Cryptography. John Wiley & Sons.
[16]. Stallings, W. (2006). Cryptography and Network Security: Principles and Practice. Pearson Education.
[17]. Rappaport, T. (2011). Wireless Communications: Principles and Practice. Pearson Education.
[18]. Atallah, M. J., & Prabhakaran, M. (2013). Secure Multi-Party Computation Problems andTheir Applications: A Review and Open Problems. In Privacy-Preserving Data Mining (pp. 153). Springer.
[19]. Ross, A. (2005). Multimodal Biometrics: Issues and Challenges. In International Conference on Audio-and Video-Based Biometric Person Authentication (pp. 3-8). Springer.
[20]. Denning, D. E., & Lewis, P. G. (2013). Experiences with the Secure Ada Target. IEEE Transactions on Software Engineering, SE-9(4), 438-453.
[21]. Golly, A., van der Horst, P., & Lee, R. B. (2016). Steganography: A Niche in Multimedia Security. In Multimedia Content Representation, Classification and Security (pp. 337-356).Springer.
[22]. Böhme, R., & Kirchner, M. (2012). Evaluation of Steganographic Algorithms. In Proceedings of the 6th ACM Workshop on Digital Rights Management (pp. 14-20). ACM.
[23]. Kim, J. J., & Chun, I. S. (2017). Digital Watermarking and Steganography. Wiley.