*Transactions on Emerging Telecommunications Technologies*

WILEY

RESEARCH ARTICLE

# Secure Communication Using Steganography and Improved Blowfish Cryptographic Methods

K. Ravindra Reddy | Vijayalakshmi P

Department of Electronics and Communication Engineering, VELS Institute of Science, Technology & Advanced Studies, Pallavaram, Chennai, Tamilnadu, India

**Correspondence:** K. Ravindra Reddy (ravindra.kalvapalli@gmail.com)

**Received:** 2 April 2025 | **Revised:** 20 December 2025 | **Accepted:** 31 December 2025

**Keywords:** 3-level discrete wavelet transform | Bernoulli's map | modified Arnold | modified blowfish | steganography

## ABSTRACT

In today's digital world, with increasing threats of cyberattacks and unauthorized data access, protecting confidential information demands more robust security mechanisms. Cryptography and steganography are two prominent techniques employed to secure data. However, conventional steganography suffers from reduced embedding capacity and the risk of image distortion. To overcome these challenges, this research proposes a novel hybrid framework to enhance data security and embedding efficiency. The approach comprises two phases including the embedding phase and the extraction phase. In the embedding phase, both the cover and secret images undergo a 3-level discrete wavelet transform (DWT) using the Daubechies wavelet. Region selection in the transformed cover image is optimized by extracting and leveraging various features, including color, shape, deep features, and local Gabor transitional pattern (LGTrP) features. These features are processed via a modified Bidirectional Long Short-Term Memory (Bi-LSTM) model, enhanced with architectural improvements, which boost feature learning. Simultaneously, the secret image undergoes transformation using a modified Arnold map integrated with a Bernoulli map allows faster execution. The modified Arnold function's outcome is subjected to an encryption process. The embedding process is done after the encryption process; the modified Blowfish algorithm is used for the decryption process. Subsequently, the inverse Bernoulli map is utilized, with the resultant output given to the inverse Arnold map. Finally, an inverse 3-level DWT reconstructs the original secret image. Comparative evaluations demonstrate the proposed framework attains lower KPA and KCA rates of 0.12 and 0.15, respectively, which underscores the innovation of integrating a steganography-cryptography model in securing sensitive data against sophisticated attacks.

## 1 | Introduction

The internet is crucial for exchanging and transferring data. Because it was a widely used and shared medium, some confidential information could have been taken, copied, changed, or even destroyed [1, 2]. Data security has emerged as a serious concern for internet users due to the recent rapid rise of technology [3–5]. Cryptography and steganography are prevailing and commonly used techniques that manipulate data in order to encipher or hide it, respectively [6]. Cryptography was employed to encrypt and decode the data for safe transmission over the internet to increase data security. However, steganography and image cryptosystems have recently taken over some channels for data transmission. Watermarking video and audio content with steganography has made it possible to trace digital prints and prevent unauthorized copying [7–9].

Techniques like Steganography and cryptography might be applied to safeguard data. Steganography was a method of concealing data within another data, whereas cryptography was a method of protecting data by converting the contents into a character that wouldn't be understood by the other party [10–12]. Their efficacy may be diminished when used separately as opposed to when used jointly [13]. Steganography was a technique used to safeguard messages from unauthorized users by enclosing sensitive data or messages inside other carrier data [14–16]. Cryptography was a way of changing data such that only the people for whom it was meant could read and understand it [16–18]. It encrypts a message so that it cannot be recognized [19, 20].

For preserving security in different marketplaces, banking and finance, media, and government organizations, there were several security measures available. Among them, the AES was frequently employed to carry out the encryption process, preventing unwanted third parties from accessing the transmitted and stored data [21–23]. To add patent data, like author's rights, and so forth, to digitalized image, video, or audio files, a method known as watermarking was used. Digital watermarks were created with the intention of protecting digitally stored intellectual property against infringement [24–26]. For instance, color cover images are divided into three color channels using a Cellular Automata (CA)-based image watermarking system based on the Discrete Cosine Transform (DCT). The watermark is then strengthened and made safer by encrypting it using CA rule-15 [27]. Additionally, the use of RSA cryptography along with DWT, Huffman coding, and steganography can be successful [28, 29]. Through the conversion of a cover image into frequency coefficients, the frequency domain offers a hiding technique. Though the frequency domain steganography has some challenges, such as lower embedding capacity, as well as higher computational and implementation complexities. Frequency domain steganography typically offers lower hiding capacity compared to spatial domain techniques, as fewer coefficients are available for embedding secret information. Transforming the cover object to the frequency domain and modifying the coefficients requires more computational resources than spatial domain methods, resulting in increased processing time [30]. DWT and Discrete Cosine Transformation are well-known transformation techniques in this field. The secret message is generally better protected from venomous attacks by frequency domain-based hiding methods. However, the consequence of computational complexity for those schemes is rather high [31].

To ensure that a suitable Pseudo Random Number Generator (PRNG) is selected for cryptographic applications, any random generator can be used to assess the quality of unpredictability. A weak system used for encryption results from poor random generator selection [32]. Data security requires the use of robust encryption algorithms when transmitting data over any kind of communication channel. Data transfer must be secured, safe, and secure in light of current information technology trends and advancements. The intended outcome of data protection was not achieved by the traditional encryption methods. Using a combination of letters and numbers to create unique IDs and passwords is a simple method. Due to its intrinsic benefit of improved security with less implementation complexity, AES has become a leading and efficient algorithm. DWT functions as a typical means for its data reduction ability after substantial study in picture coding for image compression applications. Here, the whole image is compressed and converted into a single object via a wavelet compression method. Upon achieving the whole image, the compression mistake will be distributed uniformly throughout the image. To overcome the above-mentioned issues, the proposed model is used.

The contribution is depicted below:

- Introduces an SDT scheme using DW-based Steganography and improved BF Cryptography, where a new modified Arnold map is deployed during the embedding phase.
- Deploys a modified Bi-LSTM after performing region selection upon the cover images.
- Employs a new modified Blowfish-based encryption and decryption processes.

Section 2 elucidates extant SDT schemes. Section 3 depicts the SDT scheme using proposed DW-based Steganography and improved BF cryptography, and Section 4 describes modified Blowfish-based encryption. The results and conclusion are in Sections 5 and 6.

## 2 | Literature Review

### 2.1 | Related Works

In 2021, Alrikabi and Hazim [1] have primarily depended on utilizing the DWT wavelet transform to convert the image, which needs to be protected into a composite image. The procedure of zeroing sites and storing their contents was deployed to carry the elements of the foremost image. Next, the exponential function was used to process them numerically. This procedure yields an image that was completely encrypted. The encrypted picture concealed the image that had to be shielded from discrimination and detection. There were two algorithms in the suggested system. The second method was made to efficiently restore and decode the primary image to its original condition, while the initial method was employed for encryption and concealment.

In the DCT sector, a safe and blind watermarking approach was proposed by Kumar et al. [26]. The watermark was given a double layer of protection by using the AT&CE. The watermark is strengthened further by this guard band. The variance among the adjacent block coefficients served as the foundation for the recommended embedding strategy. On adjusting the variance among two mid-frequency coefficients that were previously chosen, a watermark bit was implanted: first from the reference and the other from the successor blocks. The integrated watermark's dual layer of security ensures that the system is extremely safe.

In 2024, Valluri et al. [33] have outlined a plan for safeguarding sensor data throughout its transmission and after nodes have received it. This study suggested the EKbNV-SDT-AC model, which is an exceptional key-oriented node verification for safe data transfer employing asymmetrical cryptography. To safely transfer data from its source to its destination, this study encrypts,

decrypts, and validates nodes in the WSN. In terms of data node verification and safe data transmission, the suggested paradigm outperformed the conventional model.

In 2024, Singh et al. [34] have outlined a method for creating a VMIE system that integrates steganography, digital signatures, and encryption as three security levels. The goal of the current system was to achieve an equitable performance in terms of operational efficiency, security, and resilience. First, an MHM and the RSA cryptosystem were used to partly encrypt the original picture. In the second step, the RSA cryptosystem and a hash function were used to create a digital signature. Additionally, a "3D Arnold cat map" was applied to the partly encrypted image with a digital signature to create the private encrypted image in order to improve confusion and diffusion.

Alkhudaydi and Gutub [35] have suggested an effective security method in 2021 that included both ATS and LWC to conceal sensitive Arabic textual data on components with minimal power for processing. The task was to secure sensitive text data using a layer of LWC cryptography on devices with insufficient resource allocation. In this study, the authors employ a two-layer approach, first encrypting the Arabic confidential textual data using the LWC algorithms AES, DES, and IDEA to test their efficacy, and then inserting the encrypted information into the Arabic text that serves as diacritics. The study examined the viability of adopting DES, IDEA, and AES encryption's LWC security on the assumption that their effects on text stego-cover would be appropriate.

In 2025, Jiang et al. [36] have created the SIA-DTS approach. SIA-DTS uses elliptic curves for improved safety and efficiency, applies compact hash processes to reduce computing burden, and uses an authentication mechanism to enable safe authentication while protecting identity privacy. In order to protect data transfer, it created secure session keys using DHKE. As demonstrated by the modal and informal analysis, SIA-DTS is secure and satisfies a number of security standards. Additionally, performance research shows that SIA-DTS improves operating efficiency by drastically lowering computation and communication overhead.

For video steganography, Sangeetha et al. [16] has suggested the Hash-based LSB algorithm in 2021. With little adjustments, the LSB insert technique integrates data in the lowest bits of RGB pixels of video. Data masking was the practice of incorporating information into a video without affecting its perceived quality and preventing knowledge of the message's existence. The LSB bits' insertion point was chosen using a function called a hash. In addition to this, anyone may currently hack into systems and alter and misuse vital information.

Peter et al. [37] has created the QRM in 2022 as a unique encryption and decryption method. The suggested system employs two techniques, namely the rapid reaction method and the shifting approach, to address both performance and safety challenges. The data concealing capacity was increased by using the shifting approach. In this approach, the encryption component uses steganography to hide the secret image, while the decryption component recovers the original image. It was established that the suggested system was much superior to the existing systems through analysis and comparison.

A hybrid DES-AES method with image steganography was created in 2022 by Ab et al. [29]. AES and DES are the foundation of the 128-bit key CBA-128, which additionally employs SBE to boost the security of the data while it is being sent over the network. The suggested approach gives the data better protection to thwart unauthorized access.

In 2023, Srinivasu et al. [38] have developed a method of safe data transfer by fusing cryptography with steganography. It uses the discrete wavelet transform (DWT) in conjunction with a statistical encryption approach. The constraints "modus pointer," "reckoning pointer," "check matrix," and "error correction model" must be taken out of the secret data in order to improve data transmission security. Long-length binary data produced by the constraints is transformed into code-words. The resulting code-words are then subjected to error correction algorithms to produce the encrypted data. A 2-level DWT was deployed, and the RPE technique was used to bury the encrypted data in the diagonal sub-band.

In 2023, Ngom et al. [39] have deployed a method for protecting patients' private information that combines multi-scale signal analysis with data encryption techniques. First, an ECG signal is subjected to the DWT. Next, the Advanced Encryption Standard (AES) technique is used to encrypt the patient's private data and the electrocardiogram (ECG) signal. The stego image was formed by hiding the encryption output in an image and sending it to a medical server. Steganography improves security while cryptography guarantees the privacy of the data altered during the encryption process.

In 2020, Hureib and Gutub [40] have investigated the ways to strengthen the security of medical health data against hacking by encrypting and concealing sensitive information. This was accomplished by combining two techniques: steganography and ECC. In the first step, the text would be encrypted using ECC. Steganography was employed in the second stage to hide the text within an image. The strategy was used by any individual, group of individuals, or institution to hide and safeguard their significant business data, lab secrets, or crucial sensitive information.

In 2019, Samkari et al. [41] have presented a 3-layer security system for the protection of medical records during the Hajj period, addressing the unique requirements of a multicultural environment. The focus of this work was on securing Electronic Medical Records (EMRs) specifically tailored for the Hajj context. Initially, a new and user-friendly 3-layer security model was proposed to enhance the protection of Hajj EMRs. The proposed system combined hybrid cryptography with steganography to strengthen overall security. It verified the identity of the requesting user, whether a patient or staff member, and ensured confidentiality through the implementation of the three-layer security process.

## 2.2 | Research Gaps

In this context, securely transmitting personal data from one party to another is a significant difficulty. The existing literature in image encryption and secure data embedding methods highlights several strengths. Despite advancements in cryptographic and steganographic techniques, notable gaps remain

in addressing efficiency and scalability. The DWT [1] efficiently encrypts the image and preserves secret data; it lacks a comprehensive comparison with a broader range of existing methods, which limits its validation in diverse scenarios. The EKbNV-SDT-AC model [33] offers reduced encryption time and high accuracy in node validation, but it does not address the scalability for handling longer key lengths effectively due to its lack of hashing mechanisms. The RSA-MHM method [34] achieves good computational efficiency and lossless image quality, but it is not designed to handle the embedding of multiple images, limiting its application in multimedia security. While the LWC and ATS method [35] offers acceptable security, it lacks sufficient enhancements to the security process, particularly in requiring stronger resistance against cryptanalysis. The SIA-DTS model [36] achieves improved operational efficiency, but it lacks effective security policies for group users, which could limit its effectiveness in collaborative systems. Moreover, the Hybrid DES-AES algorithm [29] improves data privacy but lacks lightweight encryption methods, which would enhance the model's efficiency for resource-constrained environments. The ECC-based method [40] achieves high PSNR and security but suffers from computational complexity, which affects its efficiency in practical scenarios. 3-layer security [41] relies on a symmetric key for both encryption and decryption. So, managing and distributing encryption keys can be complex. These limitations found in the existing studies motivate the development of a new integrated method combining Steganography and Cryptographic Methods based on a 3-level DWT approach, leveraging an improved Blowfish algorithm and the modified Bi-LSTM model. This combined approach offers a robust solution that outperforms existing methods in terms of embedding efficiency, security and computational efficiency. Table 1 shows the review of existing works.

## 3 | SDT Scheme Using Proposed DWT-Based Steganography and Improved BF Cryptography

With the rapid growth of Internet usage and the increasing volume of data transmission, ensuring secure communication has become a critical concern for both users and online services. To address this, cryptography and steganography are widely employed as complementary techniques for protecting sensitive information. Cryptography secures data by converting plaintext into ciphertext using encryption algorithms such as the Advanced Encryption Standard (AES), which operates on fixed-size data blocks and provides a high level of security [42]. In contrast, steganography conceals the very existence of information by embedding it within a cover medium — typically multimedia content such as images, audio, or video, without introducing noticeable changes [43]. The information message is directly inserted into each pixel of the cover image through Least Significant Bit (LSB) is a widely used transformation. This method has advantages, which are more resistance to various manipulations. Actually, the most important thing in steganography is imperceptibility. This method maintained improved imperceptibility [44]. Popular image steganography techniques include Least Significant Bit (LSB) substitution, transform domain approaches, and adaptive methods, each offering different trade-offs between capacity, imperceptibility, and robustness [43]. Although transform domain techniques like the discrete wavelet transform (DWT) tend to show greater resistance to compression and signal processing attacks [45]. The integration of cryptography and steganography significantly enhances security by ensuring that, even if the hidden data is detected, its contents remain protected through encryption. Compared to simpler methods such as LSB insertion, masking, or filtering [46], the DWT enables multi-resolution analysis by decomposing an image into low and high-frequency sub-bands. This allows for more effective identification of regions suitable for data hiding, maintaining high visual quality and low distortion. This research leverages the 3-level DWT to perform domain transformation by transforming image data from the spatial domain into the wavelet domain, enabling secure and efficient communication. By embedding secret data in wavelet sub-bands, visual distortion in the cover image, leading to higher PSNR and SSIM values. Additionally, a modified Arnold map is integrated to enhance the security and complexity of the embedding process through fast permutation in the transformed domain, thereby increasing resistance to cryptanalysis and unauthorized data extraction. The proposed work includes two phases such as:

1. Embedding phase
2. Extraction phase

During the embedding phase, the 3-level DWT technique is applied to the cover image as well as the secret image. The ratio between the secret image and the color image is considered to be 1:2. After applying 3-level DWT to the cover image, region selection is carried out by extracting features like color features, deep features, shape features, and LGTrP features. These features are then subjected to a modified Bi-LSTM. Further, a modified Arnold map is deployed on the DWT-applied secret image. The modification in Arnold's map is done with the integration of Bernoulli's map. Then, encryption is done, during which the modified Blowfish algorithm will be calculated after the modified Arnold function. The output of the modified Arnold function serves as the input of the encryption process. Subsequent to the encryption process, the process of embedding is done. After encryption, the decryption process is calculated using modified Blowfish decryption. Then the inverse Bernoulli's map is applied, and the output of the inverse Bernoulli's map is taken as the input of the inverse Arnold map. As the next step, a 3-level IDWT is applied to get the final extracted secret image. Figure 1 shows the architecture of the proposed work.

### 3.1 | 3-Level DWT

DWT [47, 48] seems to be an arithmetic method for deconstructing an image hierarchically. Compared to the spatial methods like LSB and pixel value differencing (PVD) are compact methods; however, they have some limitations: it is easy to guess when a stego image has been detected as well as it is not resistant to steganalysis attacks [49]. To address this concern, the DWT method is selected for this study. This DWT technique transforms the digital image from the spatial domain into the transform domain; the high sub-bands can be used to hide messages without causing significant damage to the image and offers greater resistance to

**TABLE 1** | Reviews of extant steganography and cryptography models for SDT.

| References | Methodologies | Feature | Limitation |
|---|---|---|---|
| Alrikabi and Hazim, [1] | DWT | • Efficiently encrypts the image<br>• Better results on secret data and preservation. | • Need an analysis of the proposed method with the varied existing methods |
| Valluri et al. [33] | EKbNV-SDT-AC | • Less encryption time<br>• 98% accuracy in node validation | • Need hash methods for increased key lengths |
| Singh et al. [34] | RSA-MHM | • Good computational efficiency.<br>• Lossless image quality | • Need to consider videos and multiple images |
| Alkhudaydi and Gutub [35] | LWC and ATS | • It provides acceptable security | • Should enhance the security process |
| Jiang et al. [36] | SIA-DTS | • It achieves reduced computation overhead<br>• Improves operational efficiency. | • Need security policies to support group users. |
| Sangeetha et al. [16] | Hash-based least significant bit technique | • It provides a good, efficient method for securing the data from hackers<br>• Sends data to the destination in a safe manner. | • High running time is the major disadvantage. |
| Peter et al. [37] | Quick Response Method | • The PSNR value was greater | • Less payload capacity is the drawback |
| Ab et al. [29] | Hybrid DES-AES algorithm | • It improves data privacy | • Need to improve the model with an enhanced lightweight encryption method to provide security for any applications. |
| Kumar et al. [26] | Secure and Blind watermarking scheme | • It provides a high security process | • It is necessary to test the model in real-time applications |
| Hureib and Gutub [40] | ECC | • High PSNR<br>• Efficient security | • Computational complexity needs to be solved |

compression and signal processing attacks. By means of a DWT, the data is divided into 2 parts depending on frequency. When the low-frequency section is split into higher and lower-frequency parts, the high-frequency part offers information on the edge components. High-frequency elements are often deployed for watermarking due to the decreased sensitivity of individual eyes to edge differences. In a double-dimensional situation, the DWT is first performed primarily in perpendicular motion before moving to its parallel plane. Here, the Daubechies wavelet is deployed. Following initial decomposition, there might be 4 sub-bands: "LL 1, LH 1, HL 1, and HH 1". All succeeding decomposition steps employ the input from the LL subband of the prior level. To attain the 2nd stage of decomposition that splits the LL 1 band into the subbands "LL 2, LH 2, HL 2, and HH 2," the DWT is employed on the LL 1 band. The DWT is employed in the LL 2 band that splits the band into 4 sub-bands: "LL 3, LH 3, HL 3, and HH 3." Thus, the 3rd tier decomposition is accomplished.

## 3.2 | Region Selection via Varied Features

After applying 3-level DWT to the cover image, region selection is carried out by extracting the following features:

- Color features
- Deep features
- Shape features and
- LGTrP features.

### 3.2.1 | Deep features

The deep features, including VGG-16 and Resnet, are extracted from the 3-level DWT applied cover image, denoted by $X'$.

### 3.2.2 | VGG16

It includes "five convolutional layers, three FC layers, three max-pooling layers, and numerous other layers including ReLU, dropout, and normalization layers" that make up its deeper architecture, which consists of 25 levels. The fundamental characteristic of VGG16 is that it only uses $3 \times 3$ kernels for all convolutional layers, guaranteeing constant feature extraction while preserving the model's depth. High-level features are extracted using the FC

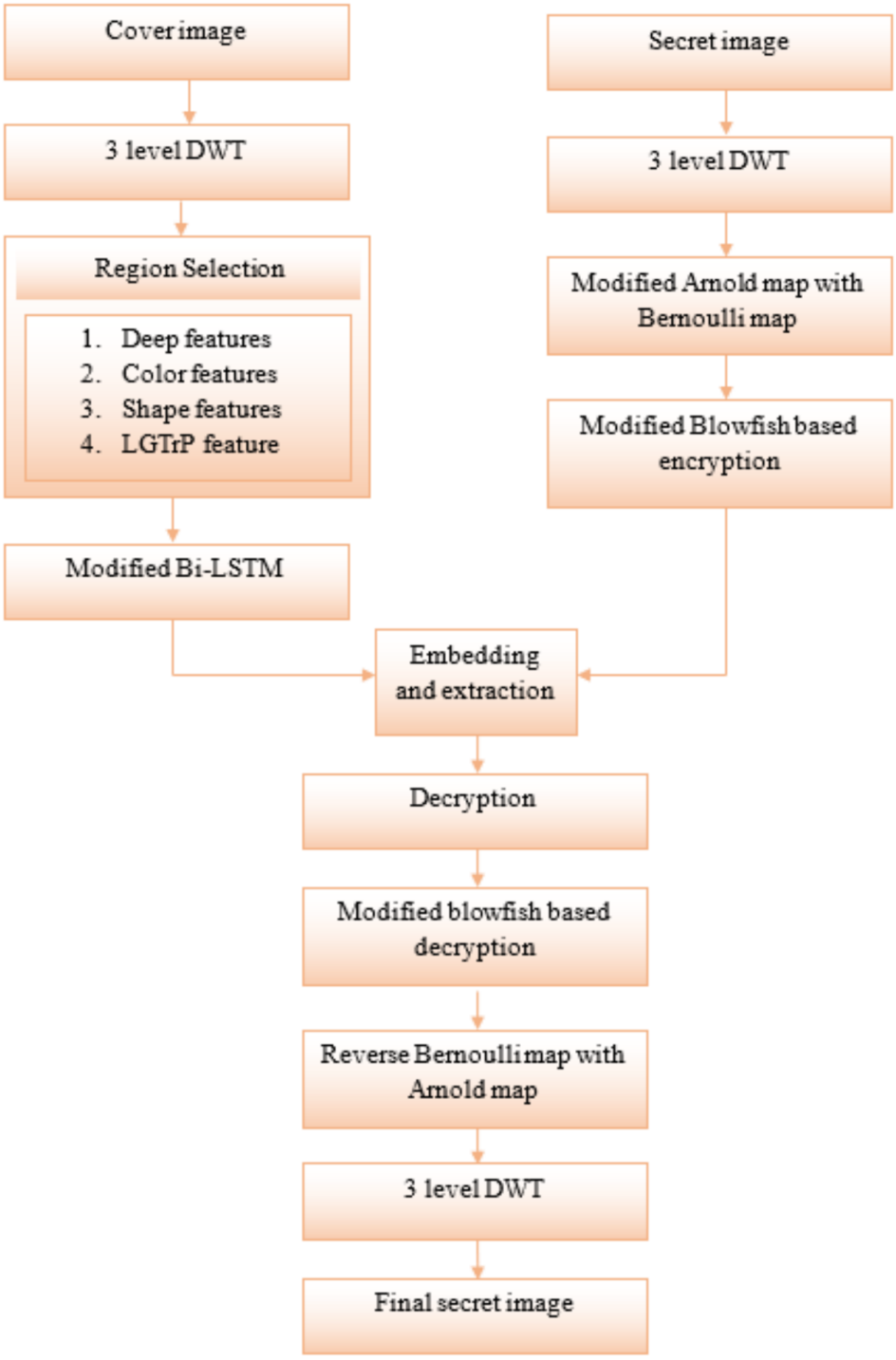


**FIGURE 1** | Architecture of proposed model.

6 and 7 activation layers of VGG16. Compared to conventional feature extraction techniques, the deep features retrieved using VGG16 are more reliable and comprehensive.

### 3.2.3 | ResNet

A DL model called ResNet [50] solves the degradation problem, in which the model's accuracy initially increases before plateauing or declining as the network depth rises. By using residual connections, which let the model bypass layers and send data straight from older layers to subsequent ones, ResNet gets around this problem. This makes training deeper networks possible and more effective by enabling the network to acquire residual functions instead of the original functions. It has been demonstrated that ResNet enhances the performance by deepening the network, which enables it to collect more intricate features from $X'$.

### 3.2.4 | Color Features

These characteristics are crucial for differentiating various areas of a picture [51]. The RGB color that is frequently utilized for the extraction of features in image processing applications is employed in this study to extract color characteristics from $X'$. In particular, the arrangement of pixel intensity in the "red, green, and blue" channels is captured using the RGB color histogram. This technique offers information about the overall composition of color in the 3-level DWT applied cover image.

### 3.2.5 | Shape Features

The considered shape attributes include orientation, area, perimeter, eccentricity, and equivalent diameter [52].

- **Area:** It represents the total pixels inside the RoI.
- **Eccentricity:** It measures the variation of shape from circularity.
- **Perimeter:** It represents the length of the edge or boundary of the region.
- **Orientation:** It represents the rotational angle of the image.
- **Equivalent diameter:** It represents the width of a circle having a similar area as the object being computed in the image, basically offering a standardized, single size value

### 3.2.6 | LGTrP Features

LGTrP [53] offers a more thorough encoding of the image's texture information by examining the intensity changes across adjacent pixel levels and orientations. In a particular direction, the LGTrP compared the intensity of central pixel of $X'$ with two nearby pixels at varying distances. The bit is configured to 1 if both of its neighbors are more or less intense than the central pixel, and to zero otherwise. By taking into account intensity transitions at various levels, this procedure aids in the encoding of texture information.

The entire features (deep features, shape features, color features and LGTrP features) extracted during region selection are denoted by *Xf*. These features are then trained to select the region from a 3-level DWT image.

## 3.3 | Modified Bi-LSTM

The features *Xf* are provided to a modified Bi-LSTM [54] for better selection of region from a 3-level DWT image. Bi-LSTM is much more effective in determining longer-term sequential relationships from *Xf*. Bi-LSTMs get data from 2 directions concurrently. At time $t$, Bi-LSTM is well-defined as in Equation (1), in which $\left[\overrightarrow{Xf_t}, \overleftarrow{Xf_t}\right]$ indicates forward and backward LSTM outcomes. $\left[\overrightarrow{Xf_t}, \overleftarrow{Xf_t}\right]$ are calculated as in Equations (2) and (3), in which, $c$ indicates bias and $w$ indicates weight. The resultant Bi-LSTM output is modeled as in Equation (4), in which, $\sigma$ implies a sigmoid function.

$$\mathrm{X}f_t = \left[\overrightarrow{Xf_t}, \overleftarrow{Xf_t}\right] \tag{1}$$

$$\overrightarrow{\mathrm{X}f_t} = F\left(w_{\Re\overrightarrow{\mathrm{X}f}}\Re_t + w_{\overrightarrow{\mathrm{X}f}\overrightarrow{\mathrm{X}f}}\overrightarrow{Xf_{t-1}} + c_{\overrightarrow{\mathrm{X}f}}\right) \tag{2}$$

$$\overleftarrow{\mathrm{X}f_t} = F\left(w_{\Re\overleftarrow{\mathrm{X}f}}\Re_t + w_{\overleftarrow{\mathrm{X}f}\overleftarrow{\mathrm{X}f}}\overleftarrow{\mathrm{X}_{t-1}} + c_{\overleftarrow{\mathrm{X}f}}\right) \tag{3}$$

$$y_t = \sigma\left(w_t\mathrm{X}f_t + c_t\right) \tag{4}$$

Although Bi-LSTM offers fine outcomes, it suffers from high computing complexity as well as slower training duration. Moreover, it poses poor application upon large-scale data and requires to be stronger in maintaining time series while dealing with complex patterns.

Thereby, a new modified model is developed in this work. The modified Bi-LSTM model comes up with varied modifications, like the inclusion of additional layers as well as certain enhancements in additional layers.

In the modified Bi-LSTM model, rather than passing the output from the forward layer to a sigmoid operation, here, we pass the output from the forward layer to newly added layers, namely, a conv layer and a BN layer, respectively. The output from the BN layer is then provided as input to a new W-HH-BN layer, whose output is supplied as input to the sigmoid operation, and the final output is obtained.

### 3.3.1 | W-HH-BN Layer

The computation of W-HH-BN involves the following steps:

**Step 1:** Compute HH as shown in Equation (5), where, $u$ refers to input from prior layer.

$$f(u) = \begin{pmatrix} -1, & if\ u < -1 \\ u, & if\ u \le 1 \\ 1, & if\ u > 1 \end{pmatrix} \tag{5}$$

**Step 2:** Compute W-HH as shown in Equation (6), where, weight $\varpi_3$ is evaluated as in Equation (7) and subsequent weight parameters $\varpi_1$ and $\varpi_2$ are computed as in below equations. Here, $it = \infty$.

$$f'(u) = \left[f(u) \times \varpi_3\right] \tag{6}$$

$$\varpi_3 = 1 - \varpi_1 - \varpi_2 \tag{7}$$

$$\varpi_1 = \cos\theta \tag{8}$$

$$\varpi_2 = \frac{1}{2}\sin\theta.\cos\varphi \tag{9}$$

$$\theta = \frac{2}{\pi}\arccos\frac{1}{3}.\arctan(it) \tag{10}$$

$$\varphi = \frac{1}{2}.\arctan(it) \tag{11}$$

**TABLE 2** | Hyperparameters of classifier models.

| Classifier models | Hyperparameters | | | |
|---|---|---|---|---|
| | Learning rate | Loss | Optimizer | Activation |
| Modified Bi-LSTM | 0.001 | MAE | SGD | Linear |
| CNN | 0.001 | MSE | Adam | Linear |
| LinkNet | 0.001 | MSE | Adam | Linear |
| Lenet | 0.001 | MSE | Adam | Linear |
| PolyNet | 0.001 | MSE | SGD | Linear |
| LSTM | 0.001 | MSE | Adam | Not applicable |
| GRU | 0.001 | MSE | RMSprop | Linear |

**Step 3:** Compute W-HH-BN as shown in Equation (12), where, $\gamma_b$ and $\sigma_b^2$ denotes mean as well as variance of $u_i$, $\varepsilon$ denotes a constant.

$$\widehat{u} = \left\{ \left[ \frac{u_i - \gamma_b}{\sqrt{\sigma_b^2 + \varepsilon}} \right] + f'(u) \right\} \tag{12}$$

Thus, the modified Bi-LSTM could learn the features of data from diverse directions more than a single-layered Bi-LSTM. Moreover, a modified Bi-LSTM could interpret several features and deal with high-dimensional complexities. The modified Bi-LSTM is designed to manage effectively the vanishing gradient issue and to capture long-term dependencies. Thus, the training was done to select the regions from a 3-level DWT image. The hyperparameters of the classifiers are shown in Table 2.

### 3.4 | Modified Arnold Map

Vladimir Arnold created the traditional Cat Map in 1962 [55]. In general, this method of image encryption uses a chaotic map. The shifting of the pixel location is the fundamental idea underlying Cat Map. It involves creating a permuted image in which each pixel in the original image is moved to a different location by utilizing the equation shown in Equation (13).

$$\begin{bmatrix} \vec{q} \\ \vec{p} \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} q \\ p \end{bmatrix} \bmod M \tag{13}$$

Equation (13), $M$ refers to the image's height and width, $q$ and $p$ points out the position of the pixel in the original image and $\vec{q}$ and $\vec{p}$ points out the position of the pixel after mapping, $a$ and $b$ points out the parameters of the system. The result of shuffling is mainly dependent upon the parameters of the system. The typical value of the parameters are $a = b = 1$.

As per the modified function, both Arnold's map as well as Bernoulli's map are hybridized. The Bernoulli map is modeled as in Equation (14), in which, $C_k$ refers to the input image. The modified Arnold map during encryption is shown in Figure 2.

$$BM = \left(C_k - 0.6\right)/0.4 \tag{14}$$

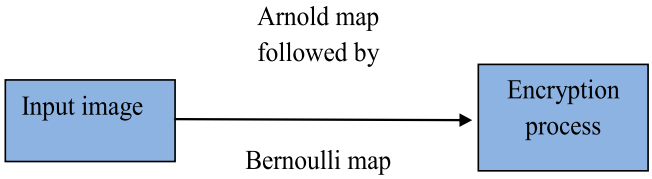


**FIGURE 2** | Modified Arnold map during encryption.

## 4 | Modified Blowfish-Based Encryption

After the modified Arnold map function, the modified Blowfish algorithm is adopted during the encryption process.

### 4.1 | Modified Blowfish Algorithm

BF is a 64-bit block cipher with a key of variable length [56, 57]. A key extension part and a data encrypting portion make up the algorithm. A key of no more than 448 bits can be expanded into many sub-key arrays of 4168 bytes. By using a 16-round Feistel system, the data is encrypted. A key-based permutation, as well as a key and data-based replacement, are both included in each round. On 32-bit words, every operation is XOR and addition. The 4-index array data lookups are the only new operations performed in every cycle.

**Sub keys:** Blowfish makes extensive use of subkeys. Before any data is encrypted or decrypted, these keys must be computed in advance

1. There are 18 32-bit subkeys in the $s$ array:$s$ 1, $s$ 2 . . . $s$ 18.
2. Each of the four 32-bit $P$ boxes has 256 entries:

$P$ 1, 0, $P$ 1, 1 . . . $P$ 1, 255;

$P$ 2, 0, $P$ 2, 1 . . . $P$ 2, 255;

$P$ 3, 0, $P$ 3, 1 . . . $P$ 3, 255;

$P$ 4, 0, $P$ 4, 1 . . . $P$ 4, 255.

The $F$ function is described as below:

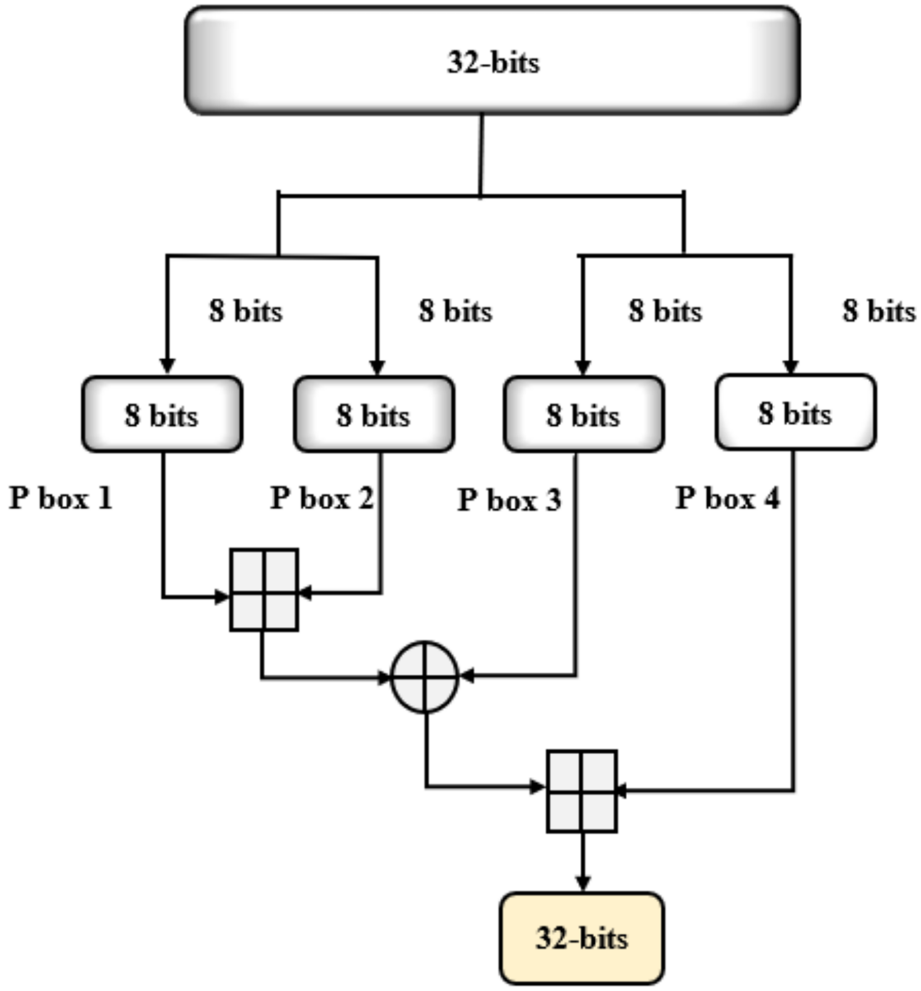


**FIGURE 3** | General diagram of blowfish.

Conventionally, $xl$ is divided into 4 8-bit blocks: $a, b, c$ and $d$. The operation $F(xl)$ is exposed as in Equation (15).

$$F(xl) = \left(\left(P_{1,a} + P_{2,b} \bmod 2 \wedge 32\right) \oplus P_{3,c}\right) + P_{4,d} \bmod 2 \wedge 32 \quad (15)$$

Figure 3 shows the common illustration of a blowfish.

However, in conventional Blowfish, these operations significantly lengthen the execution time of the algorithm. The conventional algorithm relies on pre-defined S-boxes that do not adapt to the key. This static nature can make the cipher more vulnerable to cryptanalysis techniques that exploit known patterns in the S-boxes. In order to address these issues, a new modified BF model is proposed. In the modification, the F function combines additions and XOR operations on the outputs of the four S-boxes. Additionally, the modular arithmetic prevents overflow issues and maintains the values within the 32-bit word size, which aligns with Blowfish's structure. Overall, this modification strengthens the F function's role in producing complex, non-linear outputs, making the encryption more secure while still being computationally efficient. The function $F$ was chosen to avoid time-consuming operations since it is the main source of algorithm security. Therefore, we model a new modified BF model that will offer additional security. As per the improved BF model, $F(XL)$ is modeled as in Equation (16). Figure 4 shows the modified illustration of Blowfish.

$$MF(XL) = \left(\left(P_{1,a} + P_{3,c} \bmod 2 \wedge 32\right) \oplus P_{4,d}\right) + P_{2,b} \bmod 2 \wedge 32 \quad (16)$$

## 4.2 | Embedding

After the encryption process, the embedding process is done. The embedding course involves a modified Bi-LSTM applied cover image and a 3-level DWT applied secret image. The embedding process is exposed in Equation (17), where, $Em1$ stands for secret image, $\mathrm{K}, \mathbb{Q}$ stands for scaling factors, $ll2$ refers to level 2 decomposed cover image, and $Em2$ refers to the lower frequency element of secret image.

$$Em1 = (\mathrm{K} \times ll2) + (\mathbb{Q} \times Em2) \quad (17)$$

## 4.3 | Extraction Process

The extraction process is performed as shown in Equation (18).

$$Ex = (Em1 - \mathrm{K} \times ll2) \quad (18)$$

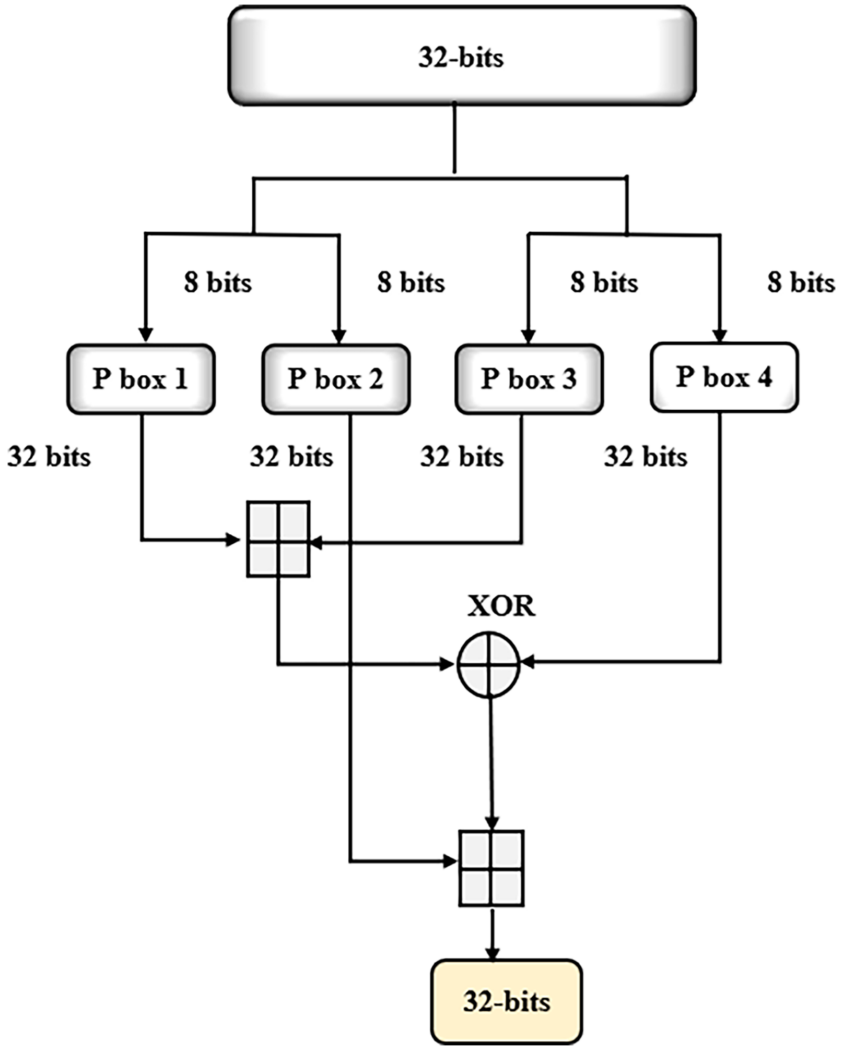


**FIGURE 4** | Improved diagram of blowfish.

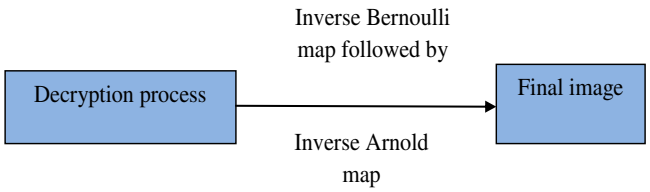


**FIGURE 5** | Modified Arnold map during decryption.

### 4.4 | Decryption

After the extraction process, decryption is performed using modified Blowfish decryption. After decryption, inverse Bernoulli's map is applied as shown in Equation (19), where $D_k$ refers to a decrypted image.

$$\mathrm{IBM} = \left(D_k \times 0.4\right) + 0.6 \tag{19}$$

The output of the inverse Bernoulli's map is taken as the input of the inverse Arnold map. The modified Arnold map during decryption is shown in Figure 5.

Finally, a 3-level IDWT is exploited to get the absolute secret image.

## 5 | Result and Discussion

### 5.1 | Experimental Setup

The SDT using DW-based Steganography and an improved BF Cryptography model was done in Python. The conservative schemes (Blowfish, RSA [1], ECC [40], 3-layer security scheme [41], Fernet [58] and Elgammal models [59]) were assessed over the improved Blowfish technique to prove the effectiveness of improvisation. In addition, improved BF is compared over Blowfish [60], RSA [61], ECC [62], Fernet, and Elgammal models regarding decryption as well as encryption times. Since all methods were tested under identical experimental conditions, including the same image sets.

#### 5.1.1 | Dataset Description

NWPU VHR-10 Dataset [63]—North-western Polytechnic University Very High-Spatial Resolution (NWPU VHR-10) dataset. This dataset contains 650 VHR optical RSIs, in which 565 images were obtained from Google Earth, where each image has a size of $1000 \times 1000$ pixels with the resolution ranging from $0.5 \times 2$ m,

and 85 pan-sharpened infrared images with 0.08 m resolution. The dataset includes ten manually annotated classes. This dataset included a total of 50 remote sensing images. During testing, 50 images are used, while for training, 10, 20, 30, and 40 images are deployed respectively.

#### 5.1.2 | MIAS Mammography Dataset

The data is images and labels/annotations for mammography scans [64]. More about the database can be found at MIAS. By popular request, the original MIAS Database (digitized at 50-μm pixel edge) has been reduced to 200-μm pixel edge and clipped/padded so that every image is $1024 \times 1024$ pixels. The images have been centered in the matrix.

#### 5.1.3 | GPR1200 ataset

Over the past 10 years, deep learning models have dominated the field of content-based image retrieval (CBIR), much like most vision-related problems [65]. Nevertheless, the majority of the research that seeks to optimize neural networks for CBIR uses domain-specific datasets for model training and testing. Therefore, whether such networks can be employed as a general-purpose image feature extractor is unknown. For selecting the personally constructed GPR1200, an accessible and user-friendly benchmark dataset containing 1200 categories and 10 class instances, after examining well-known image retrieval test sets. In order to ensure significant class diversity and clear class boundaries, classes and photos were hand chosen from six publicly accessible datasets of various image areas.

Figure 6 shows the sample image revealing the original image, watermark image, Arnold map, encryption image, decryption image, inverse Arnold, and reconstructed image. Figures 7 and 8 show the sample image from the medical domain and natural domain, revealing an improved Arnold map, improved encryption image, improved decryption image, improved inverse Arnold, and improved reconstructed image.

### 5.2 | Analysis of CCA

This section gives an explanation of SDT using DW-based Steganography and an improved BF Cryptography model using improved Blowfish over other schemes such as Blowfish, RSA [1], ECC [40], 3-layer security scheme [41], Fernet and Elgammal models. "A CCA is an attack model for cryptanalysis where the cryptanalyst can gather information by obtaining the decryptions

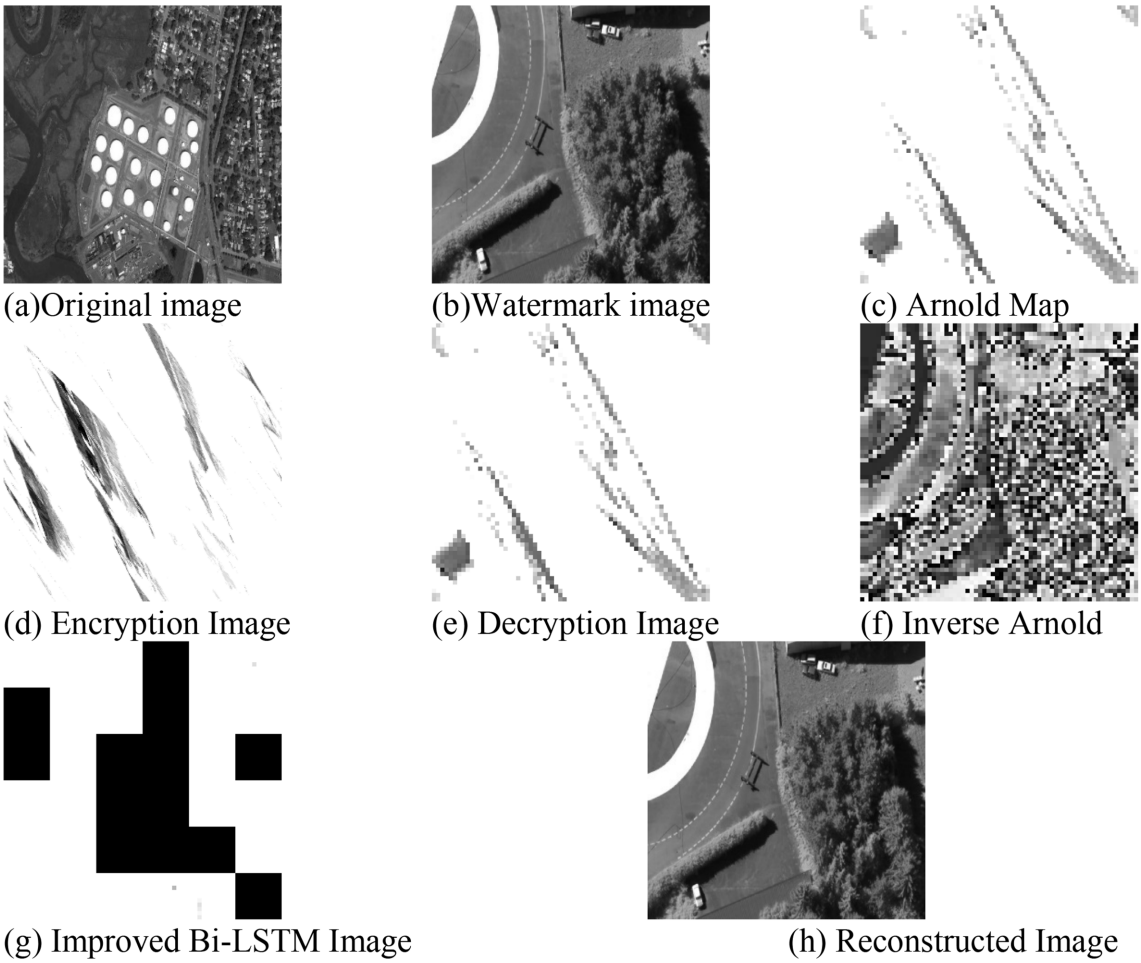


**FIGURE 6** | Sample images of NWPU VHR-10 dataset (a) original image, (b) watermark image, (c) Arnold Map, (d) Encryption Image, (e) Decryption Image, (f) Inverse Arnold, (g) improved Bi-LSTM Image and (h) reconstructed Image.

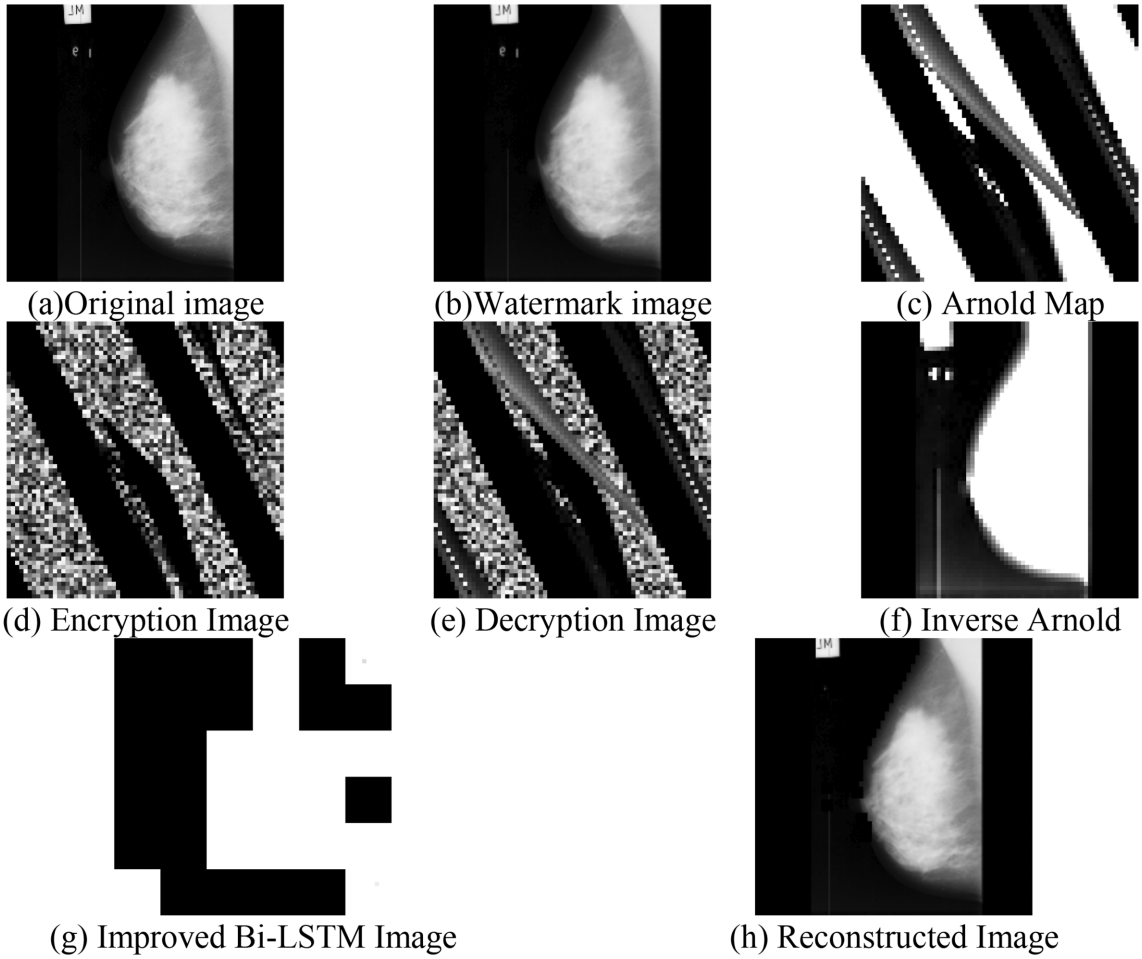


**FIGURE 7** | Medical images based on MIAS Mammography dataset revealing (a) original image, (b) watermark image, (c) Arnold Map, (d) encryption Image, (e) decryption Image, (f) inverse Arnold, (g) improved Bi-LSTM image and (h) reconstructed Image.

of chosen cipher texts. From these pieces of information, the adversary can attempt to recover the hidden secret key used for decryption." Figure 9 demonstrates the analysis of CCA for SDT using DW-based Steganography and an improved BF Cryptography model using improved Blowfish over other encryption schemes. In Figure 9, the CCA is low for improved Blowfish over Blowfish, RSA [1], ECC [40], 3-layer security [41], Fernet and Elgammal models. Next to improved Blowfish, existing Blowfish gained lower CCA values, and then ECC attained the third lowest CCA values. The CCA for improved Blowfish is $< 0.28$, as the suggested SDT using DW-based Steganography and improved BF Cryptography model uses a new modified Arnold map during the embedding phase. In addition, the newly modified Blowfish-based encryption and decryption processes ensure better SDT.

### 5.3 | Analysis of CPA

The study on CPA for SDT using DW-based Steganography and improved BF Cryptography model using improved Blowfish over Blowfish, RSA [1], ECC [40], 3-layer security [41], Fernet and Elgammal models is displayed in Figure 10. "A CPA is an attack model for cryptanalysis which presumes that the attacker can obtain the cipher texts for arbitrary plaintext. The goal of the attack is to gain information that reduces the security of the encryption scheme." In Figure 10, the CPA is low for improved Blowfish over Blowfish, RSA [1], 3-layer security [41], ECC [40], Fernet and Elgammal models. Next to improved Blowfish, Blowfish gained a low CPA value with a value of around 0.256. Next to improved Blowfish and Blowfish, ECC has the third-lowest CPA value of 0.30. The CPA for improved Blowfish is low, around 0.20. The CPA is lower as a modified Arnold map is employed during the embedding phase in this work. Also, encryption and decryption using modified Blowfish ensure superior SDT.

### 5.4 | Analysis of KCA

Figure 11 describes the KCA examination of the suggested SDT using DW-based Steganography and improved BF Cryptography model using improved Blowfish over Blowfish, 3-layer security [41], RSA [1], ECC [40], Fernet and Elgammal models. "The KCA or COA is an attack method used in cryptanalysis when the attacker has access to a given set of cipher text. The attacker does not have access to the corresponding clear text in this method; however, COA is successful when the corresponding plaintext can be determined from a given set of cipher text". The analysis on KCA is exposed in Figure 11. In Figure 11, the KCA is

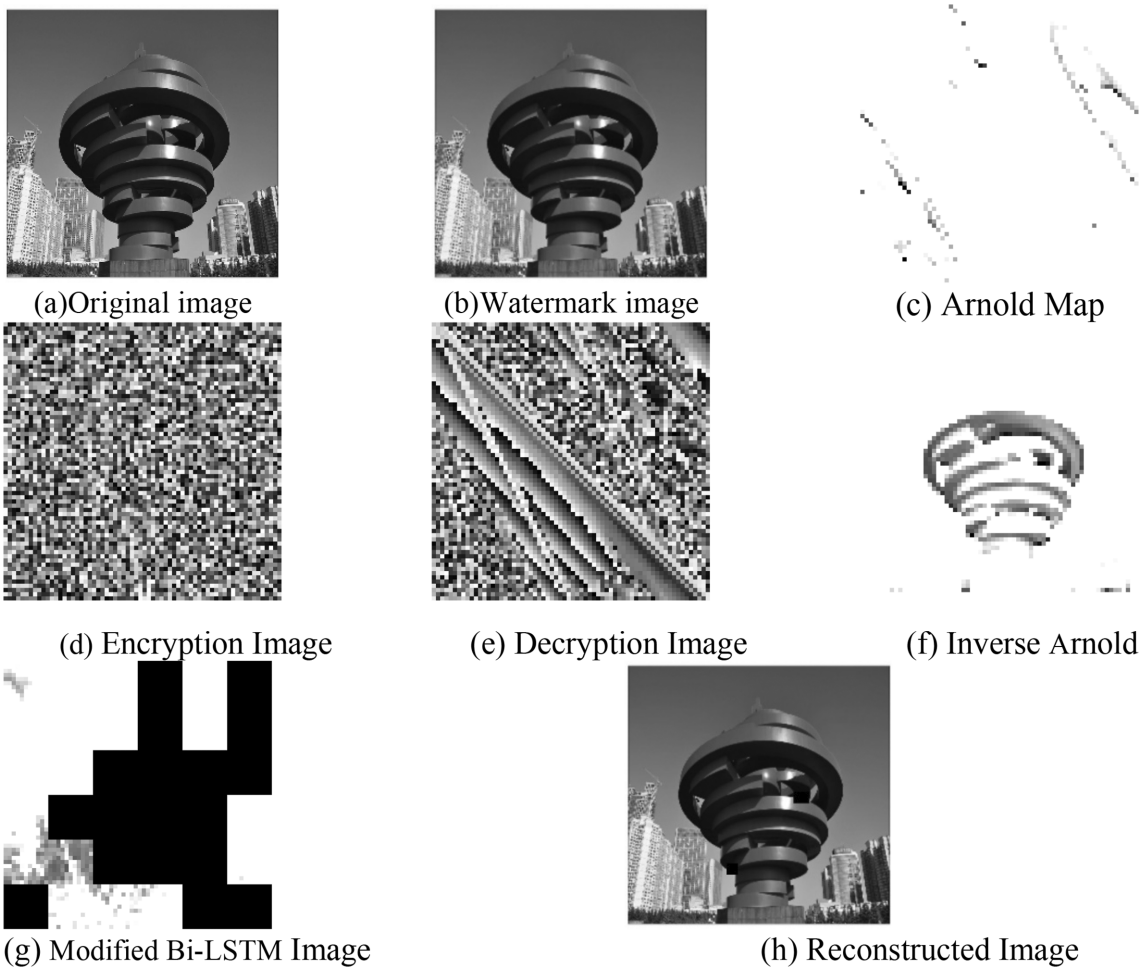


**FIGURE 8** | Natural image based on GPR1200 dataset revealing (a) original image, (b) watermark image, (c) Arnold Map, (d) encryption image, (e) decryption image, (f) inverse Arnold, (g) improved Bi-LSTM image and (h) reconstructed Image.

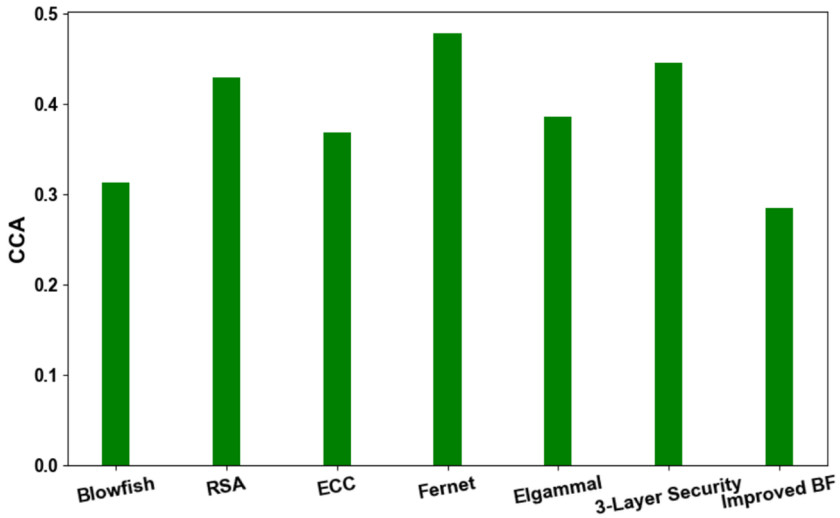


**FIGURE 9** | CCA analysis for SDT using DW-based steganography and improved BF cryptography model using improved blowfish over other schemes.

low for improved Blowfish over Blowfish, 3-layer security [41], RSA [1], ECC [40], Fernet and Elgammal models. Followed by improved Blowfish, conventional Blowfish attained lower KCA values, and then Fernet attained third lowest KCA values. The KCA for improved Blowfish is about 0.15 lower. This is due to modified Blowfish-based encryption and decryption. Moreover, the suggested modified Arnold map during the embedding phase ensures superior SDT.

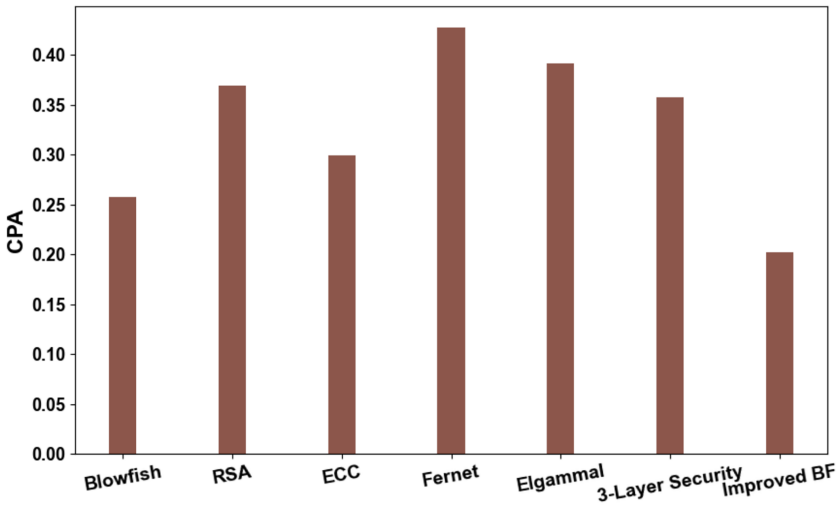


**FIGURE 10** | CPA analysis for SDT using DW-based steganography and improved BF cryptography model using improved blowfish over other schemes.

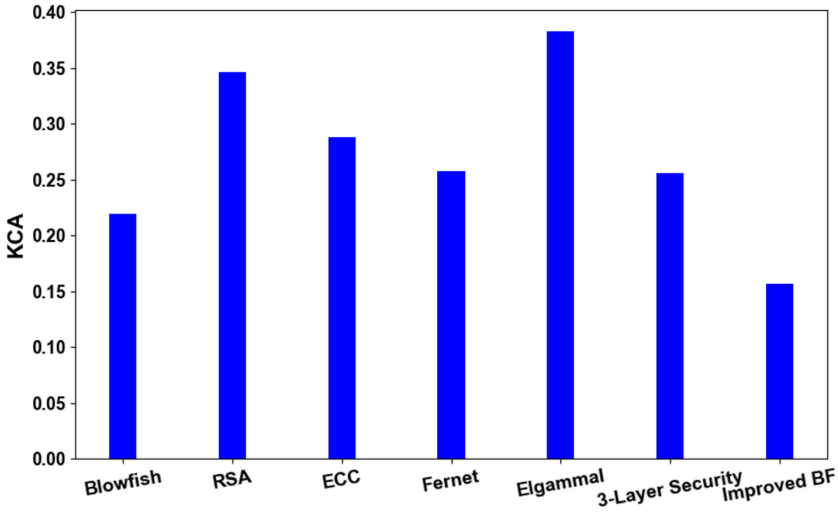


**FIGURE 11** | KCA analysis for SDT using DW-based steganography and improved BF cryptography model using improved blowfish over other schemes.

## 5.5 | Analysis of KPA

Figure 12 explains the KPA evaluation of the suggested SDT using DW-based Steganography and an improved BF Cryptography model using improved Blowfish over other schemes. The presented model was compared against Blowfish, 3-layer security [41], RSA [1], ECC [40], Fernet and Elgammal. "The KPA is an attack model for cryptanalysis where the attacker has access to both the plaintext (called a crib), and its encrypted version (cipher text). These can be used to reveal further secret information, such as secret keys and code books." In Figure 12, the KPA is low for improved Blowfish over Blowfish, 3-layer security [41], RSA [1], ECC [40], Fernet and Elgammal. The KPA values for improved Blowfish are low, around 0.12. This is owing to modified Blowfish-based encryption and decryption. The application of 3-level DWT and the modified Arnold map gives higher SDT rates. Next to improved Blowfish, conventional Blowfish attains a lower KPA value, and then ECC attains a third lower KPA value.

## 5.6 | Analysis of Encryption Time

Table 3 depicts the evaluation of the encryption time of the suggested SDT using DW-based Steganography and an improved BF Cryptography model using improved Blowfish over other schemes. Here, the encryption time is analyzed in seconds. The evaluation is done against Blowfish, RSA [1], 3-layer security [41], ECC [40], Fernet and Elgammal schemes. "The encryption time is used to calculate the throughput of any process of encryption, which is calculated as the total encrypted plaintext (in bytes) divided by the encryption time (in ms)." In Table 3, the time for encryption is less for improved Blowfish than the time for encryption using Blowfish, 3-layer security [41], RSA [1], ECC [40], Fernet and Elgammal schemes. Next to improved Blowfish, conventional Blowfish has shown less encryption time of 3.19797 s and then ECC has occupied less time for encryption of around 3.698906 s. While the 3-layer security [41] has shown a higher encryption time of 5.010049 s. The encryption time for improved

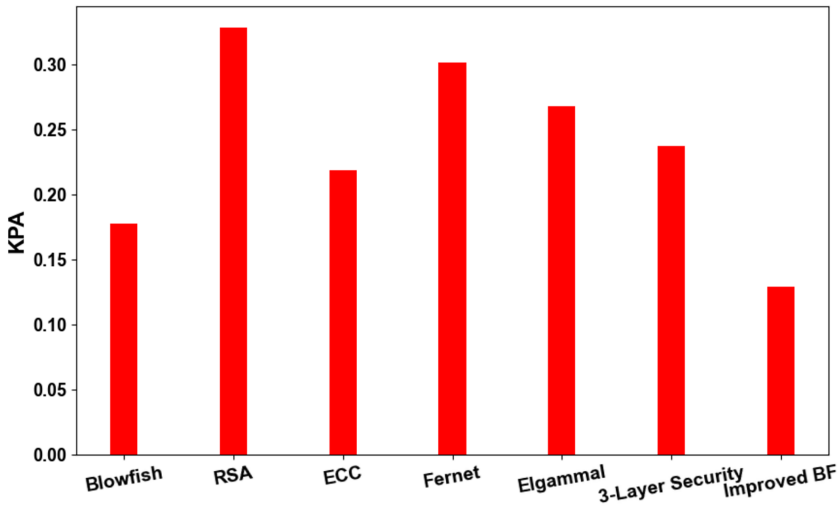


**FIGURE 12** | KPA analysis for SDT using DW-based steganography and improved BF cryptography model using improved blowfish over other schemes.

**TABLE 3** | Analysis of Encryption time (sec) for SDT using DW-based steganography and improved BF cryptography model using improved blowfish over other schemes.

| Methods | Encryption time (s) |
|---|---|
| Blowfish | 3.198 |
| RSA [1] | 4.688 |
| ECC [40] | 3.699 |
| Fernet | 5.299 |
| Elagammal | 4.287 |
| 3-layer security | 5.010 |
| Improved Blowfish | 2.488 |

**TABLE 4** | Analysis of decryption time (s) for SDT using DW-based steganography and improved BF cryptography model using improved blowfish over other schemes.

| Methods | Encryption time (s) |
|---|---|
| Blowfish | 3.377 |
| RSA [1] | 3.880 |
| ECC [40] | 4.979 |
| Fernet | 5.788 |
| Elgammal | 4.289 |
| 3-layer security [41] | 4.482 |
| Improved Blowfish | 2.679 |

Blowfish is around 2.48794 s. This is due to the employed modified Arnold map during the embedding phase in this work. Also, encryption and decryption using modified Blowfish ensure superior SDT.

## 5.7 | Analysis of Decryption Time

Table 4 describes the examination of the decryption time of the suggested SDT using DW-based Steganography and an improved BF Cryptography model using improved Blowfish over other encryption schemes. The decryption time is examined in seconds. "The conversion of encrypted data into its original form is called Decryption. It is generally a reverse process of encryption. It decodes the encrypted information so that an authorized user can only decrypt the data because decryption requires a secret key or password." In Table 4, the decryption time is less for improved Blowfish over Blowfish, RSA [1], ECC [40], 3-layer security [41], Fernet and Elgammal. The application of 3-level DWT and the modified Arnold map gives higher SDT rates. Next to improved Blowfish, conventional Blowfish attained a low decryption time value of 3.376869 s, and then RSA attained a third low decryption time of 3.87979 s. Here, Elgammal and 3-layer security [41] attained a high decryption time of 4.2889 s and 4.482397 s, respectively. The decryption time for improved Blowfish is low, around 2.67868 s. The less decryption time is owing to the modified Blowfish-based encryption and decryption adopted in this work.

## 5.8 | Analysis of PSNR

The PSNR is a metrics used to evaluate the image quality assessment (i.e., quality of the image) between the original secret image and the reconstructed secret image. The PSNR can be calculated as per Equation (20), where $L$ denotes the maximum value of the samples and MES represent the mean square error.

$$\text{PSNR} = 10Log\frac{L^2}{\text{MES}} \tag{20}$$

Figure 13 illustrates the analysis of PSNR (in dB) of the suggested SDT using DW-based Steganography and improved BF Cryptography model using improved Blowfish over other encryption models. On noticing Figure 13, it is observed that the improved BF model attains a high PSNR of 38 dB, which is higher than the existing models like Blowfish, RSA [1], ECC [40], 3-layer security [41], Fernet, and Elgammal. Thus, the image quality of the

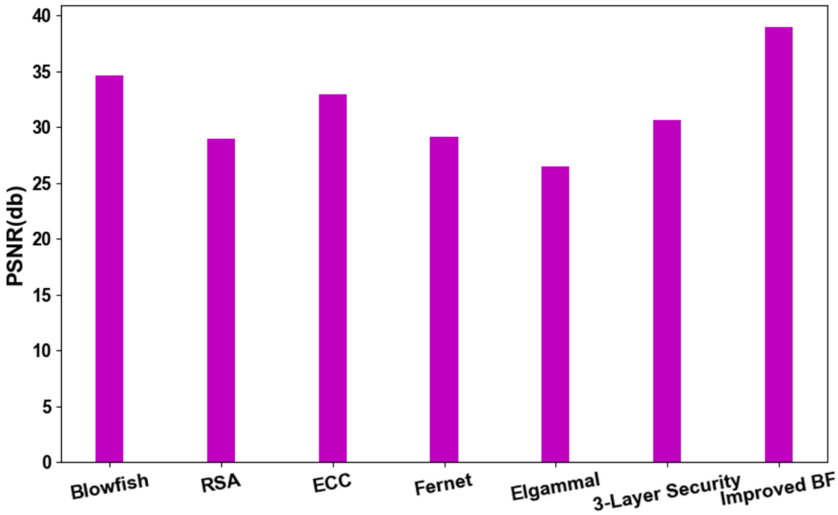


**FIGURE 13** | PSNR (dB) analysis for SDT using DW-based steganography and improved BF cryptography model using improved blowfish over other schemes.

reconstructed secret image is good for the suggested SDT using DW-based Steganography and improved Blowfish.

### 5.9 | Analysis on SSIM

The term SSIM denotes the Standard Schedules Information Manual which is a metric used to measure the similarity between the original secret image and the reconstructed secret image. Normally, the metrics measure the difference between the properties like luminance, contrast and structure of the pixels. The SSIM metric is evaluated as per Equation (21), where $\mu_p$ represent the pixel sample mean of $p$, $\mu_q$ represent the pixel sample mean of $q$, $\sigma_p$ denotes the sample variance of $p$, $\sigma_q$ represent the sample variance of $q$, $\sigma_{pq}$ denotes the sample covariance of $p$ and $q$, $c_1$ and $c_2$ are the two variables to stabilize the division with weak denominator, $c_1 = (k_1 L)^2$, $c_2 = (k_2 L)^2$, here the value of $k_1 = 0.01$ and $k_2 = 0.03$ and $L$ indicates the dynamic range of the pixel values.

$$\mathrm{SSIM}(p,q) = \frac{(2\mu_p\mu_q + c_1)(2\sigma_{pq} + c_2)}{(\mu_p^2 + \mu_q^2 + c_1)(\sigma_p^2\sigma_q^2 + c_2)} \tag{21}$$

Figure 14 encapsulates the SSIM of the suggested SDT using DW-based Steganography and an improved BF Cryptography model using improved Blowfish over other encryption schemes. Particularly, on observing Figure 14, it is observed that the developed model attains a high SSIM of (˜0.89) than the existing models like Blowfish, RSA, ECC, Fernet, 3-layer security [41] and Elgammal respectively. Thus, the suggested SDT using DW-based Steganography and an improved BF Cryptography model using improved Blowfish attains a perfect match of the reconstructed image with the original image.

### 5.10 | Analysis on RMSE

RMSE metric analysis illustrates the error from the Steganography image. In simple terms, it illustrates the various sizes or shapes of the image as a secret image is embedded in a cover image with a similarity value that is very close to the original image. The mathematical expression of the RMSE is shown in Equation (22).

$$\mathrm{RMSE} = \frac{1}{\sqrt{qp}} \sum_{j=1}^{M-1} \sum_{n=1}^{N} \left\| \left(C_k(i,j) - D_k(i,j)\right) \right\|^2 \tag{22}$$

The obtained RMSE values of the suggested model, Blowfish, RSA, ECC, Fernet, and Elgammal are depicted in Figure 15. From the depicted figure, it is clearly defined that the suggested SDT using DW based Steganography and improved BF Cryptography model using improved Blowfish attains a less RMSE value. Thus, it is stated that the suggested model attains a reconstructed secret image which is very close to the original image.

### 5.11 | Analysis on MSE

Mean Square Error (MSE) is the common quality measurements which is used to measure the difference between the cover image and the reconstructed image and, it is the average pixel by pixel squared difference between the cover image and the reconstructed image. The MSE measure is evaluated as per Equation (23), where $n$ indicates the number of samples, $Y_i$ represent the actual value and $\hat{Y}_i$ indicates the predicted value.

$$\mathrm{MSE} = \frac{1}{n} \sum_{i=1}^{n} \left(Y_i - \hat{Y}_i\right)^2 \tag{23}$$

The obtained MSE for the suggested model over the existing models is illustrated in Figure 16 respectively. And, noticing the observed graphs, the suggested SDT using DW-based Steganography and improved BF Cryptography model attains a very low error. Thus, it is stated that the reconstructed image quality is accurate to the original image for the suggested model.

### 5.12 | Analysis on Unified Average Changing Intensity (UACI)

UACI is deployed for assessing the strength of the encryption method. The UACI is designed to evaluate the number of mean

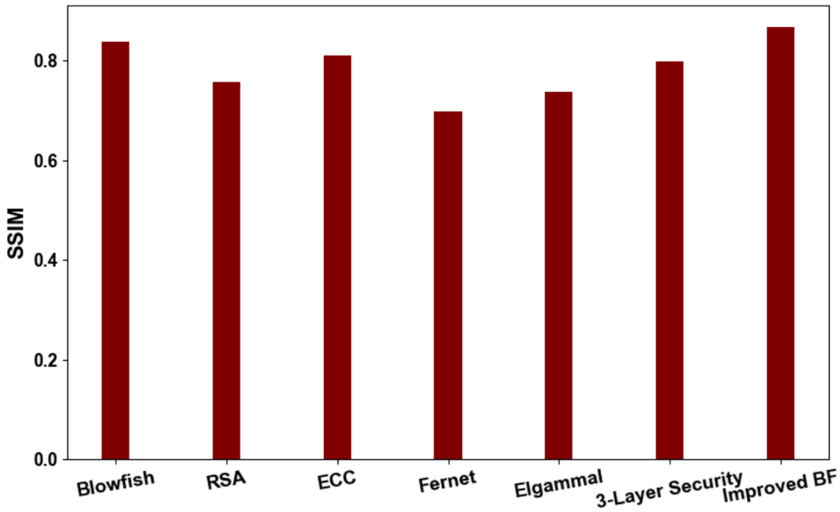


**FIGURE 14** | SSIM analysis for SDT using DW-based steganography and improved BF cryptography model using improved blowfish over other schemes.

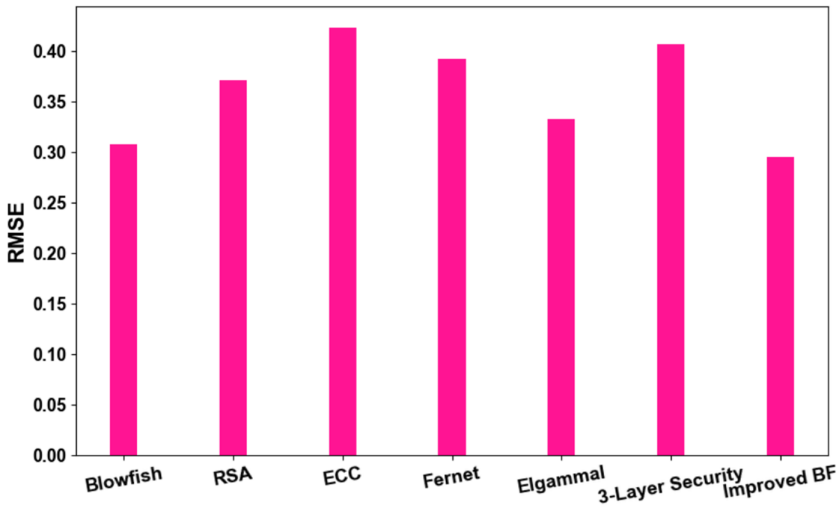


**FIGURE 15** | RMSE analysis for SDT using DW-based steganography and improved BF cryptography model using improved blowfish over other schemes.

intensities varied between two encrypted images. The UACI is computed as per Equation (24).

$$\text{UACI} = \frac{1}{M \times N}\left[\frac{\sum_{i=1}^{M}\sum_{j=1}^{N} C_k(i,j) - D_k(i,j)}{255}\right]100\% \quad (24)$$

The obtained UACI for the suggested model over the existing models is illustrated in Figure 17. On noticing Figure 17, the suggested SDT using DW based Steganography and improved BF Cryptography model attains a high value of 0.30, while Blowfish, RSA, ECC, Fernet, 3-layer security [41] and Elgammal score less UACI values. Thus, the strength of the encryption method is proved from UACI analysis.

## 5.13 | Analysis on Correlation

The correlation between original and secured data should be high for better performance of the proposed model. The correlation is computed as per Equation (25), where $x_p$ and $y_p$ are intensity values of $p-$ th pixel in the original image and the secured image respectively and $x_m$ and $y_m$ are the mean intensity values of the original image and the secured image respectively.

$$\text{correlation} - \frac{\sum_i \left(x_p - x_m\right)\left(y_p - y_m\right)}{\sqrt{\sum_i \left(x_p - x_m\right)^2}\sqrt{\sum_i \left(y_p - y_m\right)^2}} \quad (25)$$

The obtained correlation for the suggested model over the existing models is illustrated in Figure 18. In Figure 18, the suggested SDT using DW based Steganography and improved BF Cryptography model attains a higher value of 0.93, while Blowfish, RSA, ECC, Fernet, and Elgammal score lower correlation values. Thus, the correlation between original and secured data is high for developed work.

## 5.14 | Statistical Analysis

Table 5 describes the statistical analysis for the suggested SDT model using improved Blowfish over other encryption schemes.

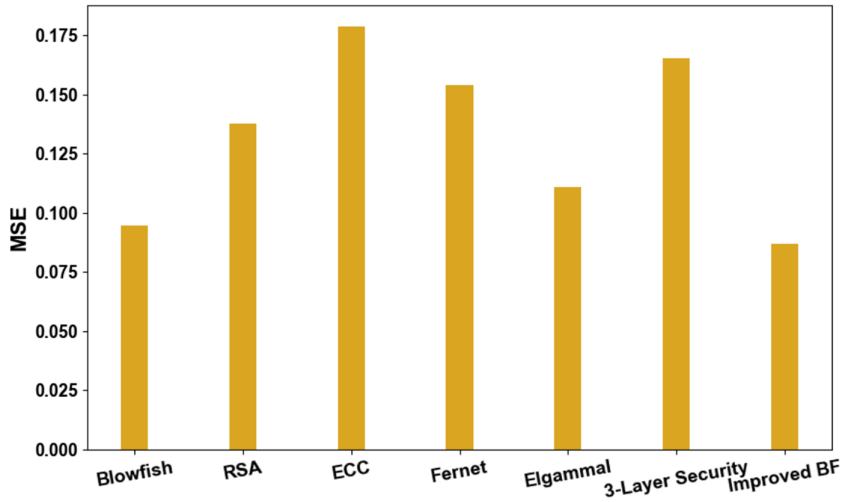


**FIGURE 16** | MSE analysis for SDT using DW-based steganography and improved BF cryptography model using improved blowfish over other schemes.

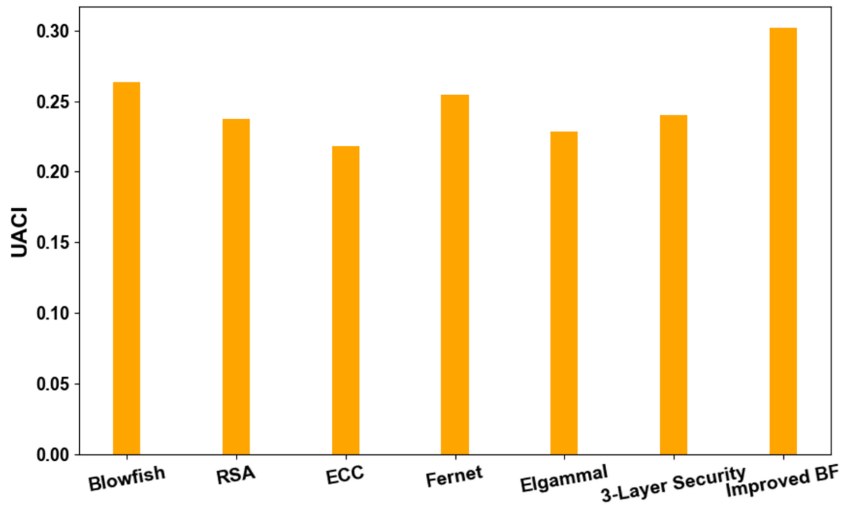


**FIGURE 17** | UACI analysis for SDT using DW-based steganography and improved BF cryptography model using improved blowfish over other schemes.

The analysis is done based on PSNR. The PSNR score should be higher for better encryption. Accordingly, the improved Blowfish-based encryption attained high PSNR values for all scenarios. Particularly, for the Max case, a high PSNR of 28.605 is obtained for the proposed work when compared to Blowfish, RSA [1], ECC [40], 3-layer security [41], Fernet, and Elgammal scores. PSNR value of 33 db. The error measure, RMSE, is less around 0.442 for the proposed modified Bi-LSTM for 40% of the testing data. The SSIM using modified Bi-LSTM is high around 0.85, and likewise UAI using modified Bi-LSTM is high around 0.259. Thus, the performance of the developed modified Bi-LSTM is proven from the analysis.

## 5.15 | Analysis of Classifier Performance

The analysis on the modified Bi-LSTM-based classifier over existing classifiers for metrics like correlation, MSE, PSNR, RMSE, SSIM, and UACI is shown in Figure 19. The correlation between original and secured data is high at initial stages and lessens with an increase in % of testing data. However, the modified Bi-LSTM attained better performance with high correlation. On the other hand, the error measure, MSE, is less for the proposed modified Bi-LSTM. In Figure 19, the modified Bi-LSTM attained a high

## 5.16 | Steganalysis

The process of studying encrypted data is called steganalysis. Steganalysis often involves a number of steps, including image scaling, noise reduction, cropping, blurring, and compression. A variety of steganalysis techniques are available to determine whether the stego image contains hidden information. Here, we consider attacks like Gaussian blur, salt and pepper noise, and rotation processes in our analysis to examine the betterment of the proposed work over existing ones.

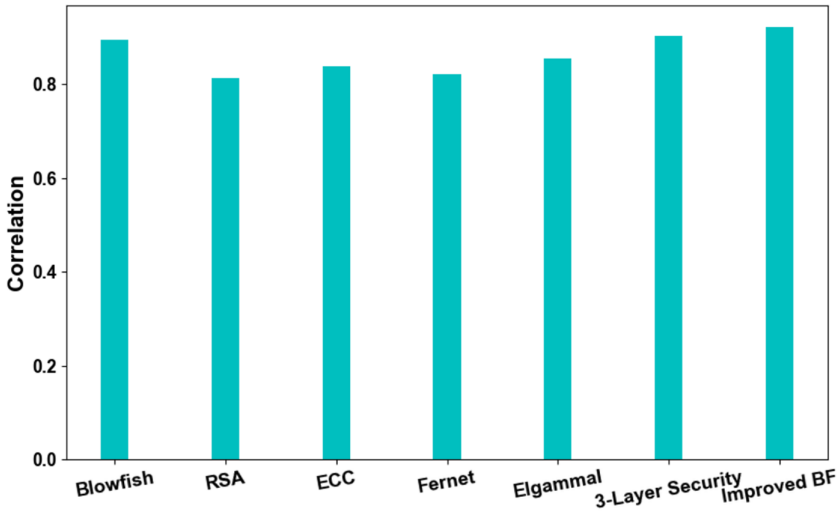


**FIGURE 18** | Correlation analysis for SDT using DW-based steganography and improved BF cryptography model using improved blowfish over other schemes.

**TABLE 5** | Statistical analysis using DW-based steganography and improved BF cryptography model using improved blowfish over other schemes.

| | Blowfish | RSA | ECC | Fernet | Elgammal | 3-layer security | Improved blowfish |
|---|---|---|---|---|---|---|---|
| Mean | 22.470 | 20.596 | 19.176 | 19.356 | 18.392 | 19.780 | 25.321 |
| Median | 23.160 | 21.002 | 18.913 | 19.526 | 18.546 | 19.572 | 25.089 |
| SD | 2.080 | 1.311 | 0.901 | 1.365 | 1.172 | 1.160 | 2.190 |
| Min | 19.090 | 18.498 | 18.301 | 17.480 | 16.899 | 18.387 | 22.499 |
| Max | 24.468 | 21.879 | 20.577 | 20.894 | 19.576 | 21.590 | 28.605 |

#### 5.16.1 | Impact of Image Blur

The impact of image blurring on improved Blowfish algorithm is evaluated against existing Blowfish, RSA, ECC, Fernet, and Elgammal methods based on metrics like correlation, MSE, PSNR measured in dB, RMSE, SSIM and UACI is shown in Table 6. In this paper, Gaussian blur function is employed to assess the impact of image blur. Table 7 shows the impact of Gaussian Blur on the modified Bi-LSTM over existing CNN, LinkNet, polyNet, LeNet, LSTM, and GRU for metrics like correlation, MSE, PSNR, RMSE, SSIM, and UACI. A high correlation, UACI, PSNR and SSIM values are obtained using improved Blowfish when compared to existing Blowfish, RSA, ECC, Fernet, 3-layer security [41] and Elgammal regarding Gaussian Blur. Likewise, a high correlation, UACI, PSNR and SSIM values are obtained using a modified Bi-LSTM over existing CNN, LinkNet, polyNet, LeNet, LSTM and GRU. On the other hand, fewer MSE and RMSE values are obtained using the modified Bi-LSTM in Table 7. Likewise, improved Blowfish obtained lower MSE and RMSE values than existing cryptographic methods.

#### 5.16.2 | Impact of Noise

The impact of noise on improved Blowfish over existing techniques based on varied metrics like correlation, MSE, PSNR (dB), RMSE, SSIM, and UACI is exposed in Table 8. Table 9 displays the impact of noise on modified Bi-LSTM over existing CNN, LinkNet, polyNet, LeNet, LSTM, and GRU for varied metrics. The salt and pepper noise is used to study the impact of noise in this research. A high correlation of 0.907676, UACI of 0.270187, PSNR of 38.94899 dB and SSIM of 0.861029 are obtained using improved Blowfish when compared to existing Blowfish, RSA, ECC, Fernet, 3-layer security [41] and Elgammal. Likewise, the modified Bi-LSTM obtained high correlation, UACI, PSNR and SSIM values over existing methods. While less MSE and RMSE values are obtained using modified Bi-LSTM and improved Blowfish as shown in Tables 8 and 9.

#### 5.16.3 | Effect of Image Rotation

The effect of image rotation on improved Blowfish over existing encryption models for varied metrics is shown in Table 10, while Table 11 shows the effect of image rotation on modified Bi-LSTM over existing classifier models for metrics like correlation, MSE, PSNR (dB), RMSE, SSIM, and UACI. In this research, the effect of image rotation is analyzed by rotating the image at 90°. On examining the Table, the improved Blowfish obtained high correlation, UACI, PSNR and SSIM values with less MSE and RMSE values when compared to existing Blowfish, RSA, ECC, Fernet, 3-layer security [41] and Elgammal. Similarly, better values are obtained for correlation, UACI, PSNR and SSIM using modified Bi-LSTM over existing CNN, LinkNet, polyNet, LeNet, LSTM, and GRU.

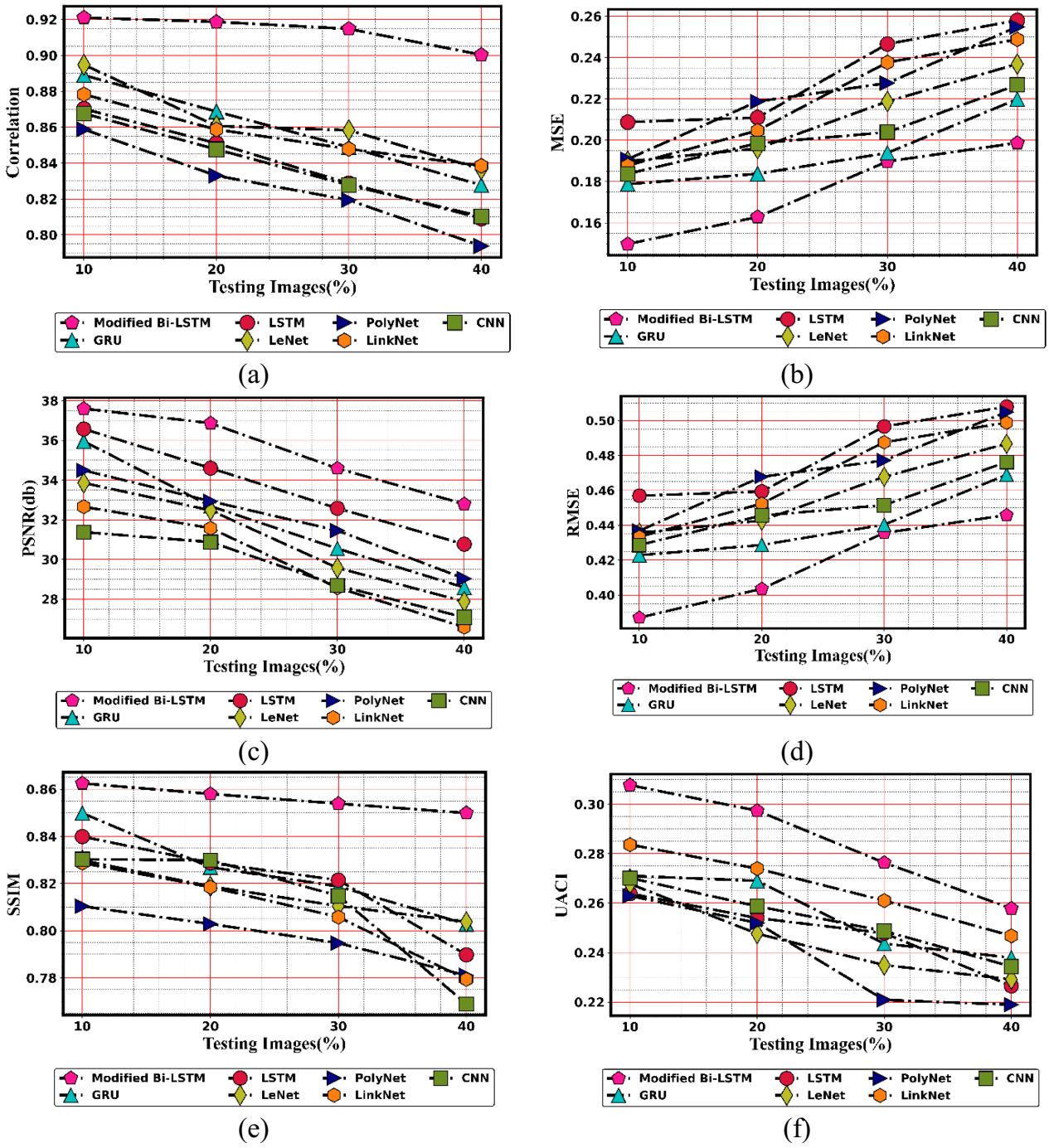


**FIGURE 19** | Analysis on modified Bi-LSTM-based classifier over existing classifiers for metrics like (a) correlation (b) MSE (c) PSNR (d) RMSE (e) SSIM and (f) UACI.

**TABLE 6** | Impact of Gaussian blur on improved blowfish over other schemes for varied metrics.

| Methods | PSNR (dB) | SSIM | MSE | RMSE | UACI | Correlation |
|---|---|---|---|---|---|---|
| Blowfish | 31.390 | 0.818 | 0.130 | 0.360 | 0.262 | 0.854 |
| RSA | 24.588 | 0.752 | 0.154 | 0.392 | 0.221 | 0.804 |
| ECC | 31.294 | 0.803 | 0.147 | 0.383 | 0.205 | 0.822 |
| Fernet | 27.899 | 0.664 | 0.174 | 0.417 | 0.246 | 0.817 |
| Elgammal | 25.939 | 0.719 | 0.152 | 0.390 | 0.210 | 0.854 |
| 3-layer security | 29.439 | 0.736 | 0.140 | 0.368 | 0.218 | 0.866 |
| Improved BF | 36.599 | 0.861 | 0.104 | 0.322 | 0.285 | 0.919 |

**TABLE 7** | Impact of Gaussian Blur on modified Bi-LSTM over other schemes for varied metrics.

| Methods | PSNR (dB) | SSIM | MSE | RMSE | UACI | Correlation |
|---|---|---|---|---|---|---|
| CNN | 32.488 | 0.839 | 0.209 | 0.457 | 0.275 | 0.836 |
| LinkNet | 32.194 | 0.844 | 0.215 | 0.463 | 0.258 | 0.845 |
| PolyNet | 32.658 | 0.852 | 0.190 | 0.435 | 0.269 | 0.836 |
| LeNet | 31.379 | 0.843 | 0.179 | 0.423 | 0.271 | 0.872 |
| LSTM | 34.279 | 0.831 | 0.204 | 0.452 | 0.264 | 0.852 |
| GRU | 35.477 | 0.826 | 0.173 | 0.416 | 0.255 | 0.863 |
| Modified Bi-LSTM | 36.599 | 0.861 | 0.104 | 0.322 | 0.285 | 0.919 |

**TABLE 8** | Impact of noise on improved Blowfish over other schemes for varied metrics.

| Methods | PSNR (dB) | SSIM | MSE | RMSE | UACI | Correlation |
|---|---|---|---|---|---|---|
| Blowfish | 33.109 | 0.819 | 0.120 | 0.346 | 0.251 | 0.863 |
| RSA | 24.598 | 0.750 | 0.157 | 0.397 | 0.223 | 0.808 |
| ECC | 29.409 | 0.803 | 0.138 | 0.371 | 0.202 | 0.811 |
| Fernet | 27.161 | 0.668 | 0.154 | 0.392 | 0.236 | 0.810 |
| Elgammal | 24.240 | 0.735 | 0.148 | 0.385 | 0.208 | 0.853 |
| 3-layer security | 31.377 | 0.759 | 0.132 | 0.353 | 0.219 | 0.873 |
| Improved BF | 38.949 | 0.861 | 0.098 | 0.313 | 0.270 | 0.908 |

**TABLE 9** | Impact of noise on modified Bi-LSTM over other schemes for varied metrics.

| Methods | PSNR (dB) | SSIM | MSE | RMSE | UACI | Correlation |
|---|---|---|---|---|---|---|
| CNN | 29.469 | 0.839 | 0.109 | 0.330 | 0.249 | 0.863 |
| LinkNet | 30.895 | 0.835 | 0.168 | 0.410 | 0.195 | 0.829 |
| PolyNet | 32.688 | 0.852 | 0.119 | 0.345 | 0.219 | 0.801 |
| LeNet | 31.399 | 0.837 | 0.198 | 0.445 | 0.204 | 0.835 |
| LSTM | 32.599 | 0.840 | 0.122 | 0.349 | 0.228 | 0.843 |
| GRU | 34.399 | 0.826 | 0.194 | 0.440 | 0.238 | 0.828 |
| Modified Bi-LSTM | 38.949 | 0.861 | 0.098 | 0.313 | 0.270 | 0.908 |

**TABLE 10** | Effect of image rotation on improved Blowfish over other schemes for varied metrics.

| Methods | PSNR (dB) | SSIM | MSE | RMSE | UACI | Correlation |
|---|---|---|---|---|---|---|
| Blowfish | 32.498 | 0.850 | 0.139 | 0.373 | 0.254 | 0.866 |
| RSA | 25.984 | 0.808 | 0.174 | 0.417 | 0.210 | 0.794 |
| ECC | 30.299 | 0.829 | 0.156 | 0.395 | 0.193 | 0.820 |
| Fernet | 27.398 | 0.788 | 0.164 | 0.405 | 0.242 | 0.807 |
| Elgammal | 25.399 | 0.811 | 0.146 | 0.383 | 0.204 | 0.849 |
| 3-layer security | 28.440 | 0.847 | 0.158 | 0.378 | 0.219 | 0.856 |
| Improved BF | 37.298 | 0.888 | 0.102 | 0.319 | 0.274 | 0.910 |

**TABLE 11** | Effect of image rotation on modified Bi-LSTM over other schemes for varied metrics.

| Methods | PSNR (dB) | SSIM | MSE | RMSE | UACI | Correlation |
|---|---|---|---|---|---|---|
| CNN | 30.488 | 0.840 | 0.126 | 0.355 | 0.257 | 0.858 |
| LinkNet | 31.588 | 0.839 | 0.159 | 0.398 | 0.210 | 0.871 |
| PolyNet | 33.266 | 0.857 | 0.199 | 0.446 | 0.190 | 0.852 |
| LeNet | 32.477 | 0.849 | 0.160 | 0.400 | 0.229 | 0.888 |
| LSTM | 35.894 | 0.847 | 0.188 | 0.433 | 0.238 | 0.863 |
| GRU | 35.188 | 0.820 | 0.189 | 0.435 | 0.222 | 0.879 |
| Modified Bi-LSTM | 37.298 | 0.888 | 0.102 | 0.319 | 0.274 | 0.910 |

**TABLE 12** | Ablation analysis.

| Metrics | Proposed model | Model using modified Bi-LSTM only | Model using Improved Arnold Map only | Model using Improved Blowfish only | Model with conventional Bi-LSTM | Model with conventional Arnold Map |
|---|---|---|---|---|---|---|
| PSNR (dB) | 35.499 | 34.298 | 34.576 | 33.465 | 32.758 | 32.689 |
| SSIM | 0.868 | 0.848 | 0.835 | 0.819 | 0.805 | 0.810 |
| MSE | 0.087 | 0.117 | 0.109 | 0.125 | 0.149 | 0.135 |
| RMSE | 0.295 | 0.341 | 0.330 | 0.353 | 0.386 | 0.368 |
| Correlation | 0.922 | 0.910 | 0.895 | 0.897 | 0.865 | 0.849 |
| UACI | 0.302 | 0.281 | 0.274 | 0.269 | 0.237 | 0.252 |

### 5.17 | Ablation Analysis

The ablation study evaluated the performance of the proposed model in comparison with the model using modified Bi-LSTM only, model using Improved Arnold Map only, model using Improved Blowfish only, model with Conventional Bi-LSTM and model with Conventional Arnold Map is shown in Table 12. The improved Blowfish-based encryption attains better correlation, UACI, PSNR (dB) and SSIM values when compared with other variants. The proposed model, which integrates the modified Bi-LSTM, improved Arnold Map, and improved Blowfish encryption, outperforms all other configurations across multiple performance indicators. Specifically, it achieves the highest PSNR of 35.499 dB, indicating superior image quality after embedding, as well as the highest SSIM value (0.868), reflecting excellent structural similarity between the original and reconstructed images. Furthermore, the lowest MSE (0.087) and RMSE (0.295) values confirm minimal reconstruction error. Comparatively, models using only modified Bi-LSTM, using only improved Arnold Map, using conventional Bi-LSTM and using conventional Arnold Map result in reduced PSNR of about 34.298, 34.576, 33.465, 32.758 and 32.689, respectively, illustrating that no single enhancement alone can achieve the full benefit of the hybrid approach. Specifically, the model using the modified Bi-LSTM only achieves a SSIM of 0.848, which is notably higher than that of the conventional Bi-LSTM (0.805) and is comparable to the model using only Improved Arnold Map (0.835). Similarly, the correlation and error metrics (MSE and RMSE), indicating that the modified Bi-LSTM plays a meaningful role in optimizing embedding localization and feature-driven region selection. Since the Bi-LSTM is responsible for learning spatial–feature dependencies that guide optimal embedding regions, the model using only improved Blowfish records even higher MSE and RMSE, reinforcing the necessity of advanced feature learning and spatial transformation methods. Overall, the results highlight that the integration of all three components in the proposed model leads to a well-balanced system, achieving high visual fidelity, low distortion, strong statistical consistency, and enhanced security, making it a robust solution for secure image embedding and transmission.

### 5.18 | Impact of Gaussian Noise on the Model's Performance: A Comparative Analysis

The performance comparison in the provided Table 13 clearly demonstrates the superiority of the proposed method over Gaussian noise-infused variants at different noise levels (10%, 50%, and 75%). The proposed method without Gaussian noise achieves the highest PSNR (35.499 dB), indicating better image fidelity, and the lowest MSE (0.087) and RMSE (0.295), reflecting minimal reconstruction error. Similarly, it maintains the highest SSIM value (0.868), showing strong structural similarity with the original image, and the highest correlation coefficient (0.922), highlighting strong statistical similarity. Furthermore, the proposed approach exhibits the highest UACI value (0.302), suggesting improved resistance against differential attacks and better security through more significant pixel intensity changes. In contrast, the performance metrics consistently degrade as the Gaussian noise level increases, with PSNR dropping to 27.288 and SSIM falling to 0.769 at 75% noise. As Gaussian noise levels increase, all performance indicators degrade significantly, reinforcing the resilience of the proposed system in maintaining data quality and security even in noisy environments. These results validate the effectiveness of the proposed approach in preserving both imperceptibility and robustness in real-world scenarios.

**TABLE 13** | Comparative analysis of the model under different rates of Gaussian noise.

| Metrics | Proposed without Gaussian noise | Gaussian noise = 10% | Gaussian noise = 50% | Gaussian noise = 75% |
|---|---|---|---|---|
| PSNR | 35.499 | 31.899 | 29.869 | 27.288 |
| SSIM | 0.868 | 0.833 | 0.804 | 0.769 |
| MSE | 0.087 | 0.128 | 0.154 | 0.193 |
| RMSE | 0.295 | 0.357 | 0.393 | 0.439 |
| Correlation | 0.922 | 0.894 | 0.869 | 0.845 |
| UACI | 0.302 | 0.273 | 0.256 | 0.214 |

## 5.19 | Statistical Test Analysis

Table 14 presents a comparative statistical evaluation of the suggested Modified Bi-LSTM approach over various conventional techniques like CNN, LinkNet, PolyNet, LeNet, LSTM, and GRU. A $p < 0.1$ indicates a statistically significant difference in performance between the models. Based on the statistical results presented in Table 14, the proposed Modified Bi-LSTM model demonstrates competitive and, in several cases, significantly superior performance compared to conventional models such as CNN, LinkNet, PolyNet, LeNet, LSTM, and GRU. Notably, the comparison with CNN yields statistically significant differences across all three tests, with the *t*-test ($p = 0.007$) and Friedman test ($p = 0.009$) showing strong evidence that Modified Bi-LSTM outperforms CNN. Similarly, in the case of LeNet, the Wilcoxon test ($p = 0.008$) indicates a significant improvement, further confirming the effectiveness of the proposed model in capturing relevant features and learning long-range dependencies. Although the comparison with GRU also reveals statistically significant differences in both the Wilcoxon ($p = 0.065$) and Friedman ($p = 0.045$) tests, the *p*-values are marginally below the 0.1 threshold, suggesting moderate but consistent improvements. On the other hand, the results for LinkNet and LSTM are mixed. While the *t*-test for LSTM ($p = 0.021$) indicates a significant difference, the Friedman test ($p = 0.929$) suggests no notable variance across the group, possibly due to variations in sample distributions. The comparison with LinkNet shows no significant differences across all tests, with all *p*-values above 0.1, suggesting that the performance of Modified Bi-LSTM is comparable to that of LinkNet in this context. Overall, the statistical evaluation confirms that the Modified Bi-LSTM offers improved performance over several traditional models, especially in terms of feature representation and learning capability. By integrating 3-level DWT, a modified Arnold-Bernoulli encryption scheme, and a structurally enhanced Bi-LSTM network, the proposed method ensures not only high data security and embedding efficiency but also adaptability to various cover image characteristics.

## 5.20 | Analysis on PSNR Based on Error Bars

The PSNR score of the proposed improved BF algorithm was comprehensively evaluated and compared against several traditional and state-of-the-art models, including Blowfish, RSA, ECC, Fernet, Elgammal, and 3-layer scheme. The comparative result is illustrated in Figure 20. The improved BF model achieved a superior performance with a higher PSNR of 2.1904. In contrast, the established methods yielded lower PSNR values with values ranging from 0.900 to 2.079. Furthermore, error bars represent the standard deviation across multiple runs, offering insights into the stability and consistency of each model. These results underscore the advantage of integrating 3-level DWT and a modified Arnold-Bernoulli encryption scheme. The proposed method ensures not only high data security and embedding efficiency.

**TABLE 14** | Statistical test comparison in terms of Wilcoxon, Friedman, and *t*-test.

| Modified Bi-LSTM Vs | Wilcoxon *p*-value | Friedman *p*-value | *t*-test |
|---|---|---|---|
| CNN | 0.078 | 0.009 | 0.007 |
| LinkNet | 0.138 | 0.108 | 0.079 |
| PolyNet | 0.066 | 0.148 | 0.125 |
| Lenet | 0.008 | 0.078 | 0.114 |
| LSTM | 0.130 | 0.929 | 0.021 |
| GRU | 0.065 | 0.045 | 0.065 |

## 5.21 | Assessment on Computational Time

Table 15 presents a comparative analysis of the computational time required by various models, highlighting the efficiency of the proposed Modified Bi-LSTM. Among all the evaluated models, the Modified Bi-LSTM achieves the lowest computational time of 56.288 s, demonstrating its superior execution efficiency. In contrast, conventional models such as PolyNet (168.579 s), LeNet (134.389 s), and LinkNet (124.770 s) exhibit significantly higher computation times, suggesting higher processing overhead. Even compared to LSTM (89.918 s) and GRU (98.817 s), the Modified Bi-LSTM shows a clear advantage, likely due to its optimized architecture and integration with lightweight encryption mechanisms like the modified Arnold-Bernoulli map. The CNN model, although relatively faster than some others at 102.879 s, still lags behind the Modified Bi-LSTM in terms of speed. This considerable reduction in computational time, without compromising performance, positions the Modified Bi-LSTM as a highly efficient solution for secure image embedding tasks, particularly in scenarios where both speed and security are critical.

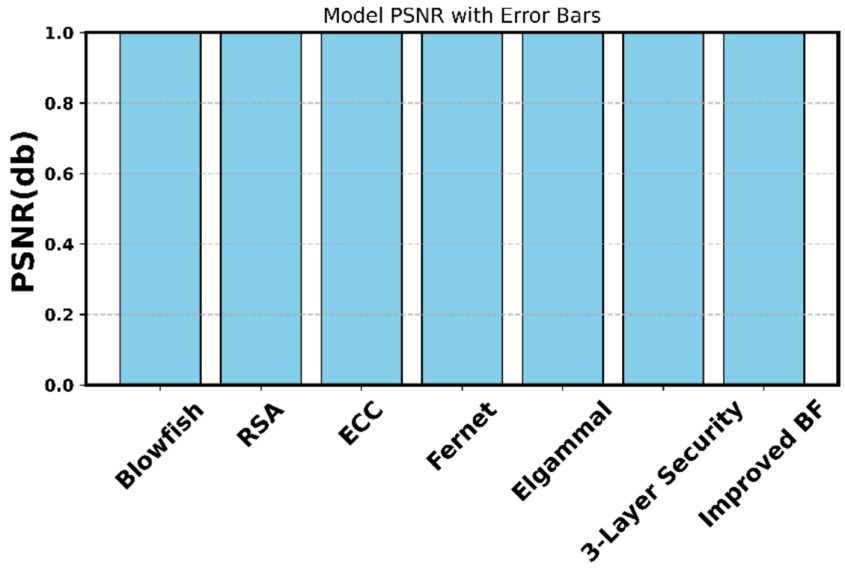


**FIGURE 20** | PSNR analysis based on error bars.

**TABLE 15** | Analysis on computational time.

| Models | Time (s) |
|---|---|
| CNN | 102.879 |
| LinkNet | 124.770 |
| PolyNet | 168.579 |
| LeNet | 134.389 |
| LSTM | 89.918 |
| GRU | 98.817 |
| Modified Bi-LSTM | 56.288 |

## 5.22 | Analysis Using Learned Perceptual Image Patch Similarity and Fréchet Inception Distance

Learned perceptual image patch similarity (LPIPS) is used to assess perceptual similarity based on visual features learned by neural networks, approximating human perception. Fréchet Inception Distance (FID) measures the distance of feature distributions between stego-images and cover images [66]. The model having lower values indicates higher perceptual similarity and reduced visual distortion, along with lower FID values reflecting better preservation of image consistency. Table 16 shows the comparison of the proposed improved Bi-LSTM against the existing methods such as GRU, LSTM, Lenet, Polynet, Linknet and CNN based on LPIPS value and FID value for NWPU VHR-10 Dataset. The results demonstrate that the Modified Bi-LSTM model achieves the lowest LPIPS value (0.163) and FID value (15.384) among all evaluated models, indicating superior perceptual fidelity and minimal distributional deviation. In contrast, GRU and LSTM exhibit higher LPIPS and FID values. Table 17 presents the results for medical images, where maintaining perceptual integrity is critical. The Modified Bi-LSTM again outperforms all comparative models, achieving the lowest LPIPS (0.144) and FID (13.595). The higher LPIPS and FID values observed in GRU, Polynet, and LSTM-based models indicate poorer preservation of structural and textural characteristics. Additionally, the results in Table 18 demonstrate that Modified Bi-LSTM records the lowest LPIPS (0.158) and FID (17.388) across natural images, demonstrating strong perceptual similarity and realistic image reconstruction. Across all three datasets, the Modified Bi-LSTM consistently achieves the best LPIPS and FID scores, indicating superior perceptual quality and distributional alignment with original images.

**TABLE 16** | Performance analysis on NWPU VHR-10 Dataset based on LPIPS and FID values.

| Models | LPIPS | FID |
|---|---|---|
| Modified Bi-LSTM | 0.163 | 15.384 |
| GRU | 0.768 | 78.238 |
| LSTM | 0.827 | 98.393 |
| Lenet | 0.637 | 67.690 |
| Polynet | 0.469 | 37.498 |
| Linknet | 0.395 | 29.948 |
| CNN | 0.589 | 48.385 |

**TABLE 17** | Performance analysis on MIAS mammography dataset based on LPIPS and FID values.

| Models | LPIPS | FID |
|---|---|---|
| Modified Bi-LSTM | 0.144 | 13.595 |
| GRU | 0.829 | 89.377 |
| LSTM | 0.654 | 72.385 |
| Lenet | 0.578 | 69.083 |
| Polynet | 0.719 | 83.766 |
| Linknet | 0.295 | 31.499 |
| CNN | 0.383 | 45.398 |

**TABLE 18** | Performance analysis on GPR1200 dataset based on LPIPS and FID values.

| Models | LPIPS | FID |
|---|---|---|
| Modified Bi-LSTM | 0.158 | 17.388 |
| GRU | 0.563 | 67.297 |
| LSTM | 0.397 | 28.379 |
| Lenet | 0.510 | 61.376 |
| Polynet | 0.436 | 55.486 |
| Linknet | 0.476 | 42.874 |
| CNN | 0.289 | 26.390 |

## 6 | Discussion

The suggested SDT using DW-based Steganography incorporates an improved BF Cryptography model, which was compared over other schemes such as Blowfish, RSA [1], ECC [40], 3-layer security scheme [41], Fernet and Elgammal models in terms of CCA, CPA, KCA and KPA. In terms of evaluating various attacks, the suggested improved BF algorithm showed better resistance to KPA and KCA attacks with minimal values of 0.140 and 0.162, respectively. Also, compared to the conventional Blowfish algorithm, which was critiqued for vulnerabilities to certain types of attacks, such as KPA and KCA, the improved Blowfish algorithm in this study incorporates additional mechanisms within the F function and outperforms traditional Blowfish in these respects by showing significantly lower vulnerability to KPA and KCA, having 0.140 and 0.162, respectively. Also, for assessing the decryption and encryption time, the existing models like Blowfish, RSA [1], ECC [40], 3-layer security scheme [41], Fernet and Elgammal models showed a higher period in the range of 3.197 s – 5.788 s; unlike these baseline models, the improved BF algorithm achieved lower decryption and encryption times of 2.488 and 2.679, respectively. While RSA [1] and 3-layer security [41] are known to cause higher distortions in the image quality due to their higher computational overhead, the improved Blowfish version achieves higher PSNR (37.431) and SSIM (0.870), indicating that the reconstructed secret image quality is significantly better than the baseline methods.

To measure the difference between the cover image and the reconstructed image in terms of error measures, the suggested improved BF model achieved comparably lower scores on MSE and RMSE, in contrast to the traditional methods. The findings of the study highlight that the improvements made in the F function, particularly through the addition and XOR operations on the outputs of the S-boxes, improve the diffusion and non-linearity of the algorithm, thus making it more secure without sacrificing performance. This demonstrates a significant advancement over prior models, which often lacked robust sequential feature processing capabilities. As a result, the modified Bi-LSTM ensures better reconstruction quality of the secret image. The combination of stronger security, faster processing times, and higher image quality sets this approach apart from earlier schemes, providing a more robust framework for secure communication and data hiding in a variety of applications. However, a notable limitation of the proposed work is the absence of a secret sharing mechanism that integrates both steganography and encryption. This gap limits its applicability in scenarios requiring collaborative access to sensitive data. As part of future work, the study aims to incorporate a counting-based secret sharing technique [67, 68] to enhance data security, particularly in environments where controlled, multi-user access is critical. Though the complexity increases because of the combination of both cryptography and steganography, the level of security also further increases [41], which is the growing need of the anticipated application.

## 7 | Conclusion

There were two stages to the suggested work: the extraction phase and the embedding phase. Both the cover image and the hidden image were subjected to the 3-level DWT approach during the embedding phase. After applying 3-level DWT to the cover image, region selection was carried out by extracting features like deep features, color features, shape features, and LGTrP features. These features were then subjected to a modified Bi-LSTM for selecting the region from a 3-level DWT image. After that, the secret picture applied by DWT was given a modified Arnold map. The incorporation of Bernoulli's map allowed Arnold's map to be modified. Subsequently, encryption was performed, whereby the modified Arnold function was calculated before the modified Blowfish algorithm. The input for the encryption procedure was the result of the altered Arnold function. The embedding step was completed after the encryption process. Following encryption, modified Blowfish decryption was used to determine the decryption procedure. Afterwards, the inverse Arnold map was applied, with its output serving as the input, and the inverse Bernoulli map as its output. The last retrieved secret image was obtained by using inverted 3-level IDWT. Analysis revealed that compared to Blowfish, RSA, ECC, Fernet, and Elgammal schemes, improved Blowfish required less time for encryption. Next to improved Blowfish, conventional Blowfish has shown less encryption time of 3.19797 s, and then ECC has occupied less time for encryption of around 3.698906 s. The encryption time for improved Blowfish was less around 2.48794 s. Additionally, the upgraded Blowfish's KPA was lower than that of the Blowfish, RSA, ECC, Fernet, and Elgammal. The KPA values for improved Blowfish are low, around 0.12. Despite the promising improvement in the proposed approach, it has some limitations, in which there are many image quality assessment metrics, but during the evaluation, various limitations in each quality assessment scheme that might impact the accuracy. Additionally, the proposed method remains susceptible to various attacks such as decoration, scaling, and clamor attack.

### Nomenclature

| | |
|---|---|
| 2D-DWT-2 L | 2D-discrete wavelet transform |
| AES | advanced encryption standard |
| AGA-OPAP | adaptive genetic algorithm-based optimal pixel adjustment |
| AT&CE | Arnold transform and chaotic encryption |
| ATS | Arabic text steganography |
| BF | blowfish |
| BMOGA | bit mask oriented genetic algorithm |
| CBA-128 | cross-breed algorithm |

| | |
|---|---|
| CCA | chosen cipher attack |
| CPA | cipher plaintext attack |
| DHKE | Diffie-Hellman key exchange |
| DW | discrete wavelet |
| DWT | discrete wavelet transform |
| ECC | elliptic curve cryptographic |
| FC | fully connected |
| IDWT | inverse DWT |
| KCA | known cipher attack |
| KPA | known plaintext attack |
| LGTrP | local Gabor transitional pattern |
| LSB | least significant bit |
| LWC | lightweight cryptography |
| MHM | modified Hénon map |
| PSNR | Peak signal-to-noise ratio |
| QRM | quick response method |
| RGB | red green blue |
| RSA | Rivest-Shamir-Adleman |
| SBE | steganography based encryption |
| SDT | secured data transfer |
| SIA-DTS | secure identity access and data transmission scheme |
| UACI | Unified average changing intensity |
| VIHCS | visually imperceptible hybrid crypto steganography |
| VMIE | visually meaningful image encryption |

## Data Availability Statement

The data that support the findings of this study are available from the corresponding author upon reasonable request.

## References


1. H. T. S. Alrikabi and H. T. Hazim, "Enhanced Data Security of Communication System Using Combined Encryption and Steganography," *International Journal of Interactive Mobile Technologies (iJIM)* 15, no. 16 (2021): 145.

2. N. F. Soliman, M. I. Khalil, A. D. Algarni, S. Ismail, R. Marzouk, and W. El-Shafai, "Efficient HEVC Steganography Approach Based on Audio Compression and Encryption in QFFT Domain for Secure Multimedia Communication," *Multimedia Tools and Applications* 80, no. 3 (2021): 4789–4823.

3. S. Rahman, F. Masood, W. U. Khan, et al., "A Novel Approach of Image Steganography for Secure Communication Based on LSB Substitution Technique," *Computers, Materials & Continua* 64, no. 1 (2020): 31–61.

4. U. K. Mondal, S. Pal, A. Dutta, and J. K. Mandal, "A New Approach to Enhance Security of Visual Cryptography Using Steganography (VisUS)," preprint arXiv, 2103.09477, 2021.

5. S. Zaware, "Crypto-Steganography Approach for Secure Data Transmission Using Image and Audio Files," *Vidyabharati International Interdisciplinary Research Journal* 12, no. 1 (2021): 409–415.

6. S. Farrag and W. Alexan, "Secure 2D Image Steganography Using Recamán's Sequence," paper presented 2019 International Conference on Advanced Communication Technologies and Networking (Commnet), IEEE, 2019, 1–6.

7. D. Pandey, S. Wairya, R. S. Al Mahdawi, et al., "Secret Data Transmission Using Advanced Steganography and Image Compression," *International Journal of Nonlinear Analysis and Applications* 12, no. Special Issue (2021): 1243–1257.

8. O. F. A. Wahab, A. A. Khalaf, A. I. Hussein, and H. F. Hamed, "Hiding Data Using Efficient Combination of RSA Cryptography, and Compression Steganography Techniques," *IEEE Access* 9 (2021): 31805–31815.

9. A. Malaghan, M. Aditya, B. Ajith, S. Anjana, and G. P. N. Karthik, "Combined Steganography and Image Cryptography System for Secure Data Transfer," *ACS Journal for Science and Engineering* 2, no. 1 (2022): 63–72.

10. S. Alkhliwi, "Encryption-Based Image Steganography Technique for Secure Medical Image Transmission During the COVID-19 Pandemic," *International Journal of Computer Science & Network Security* 21, no. 3 (2021): 83–93.

11. W. A. Awadh, A. S. Hashim, and A. K. Hamoud, "Efficiently Secure Data Communications Based on Cbc-rc6 and the Overflow Field of Timestamp Option in an ipv4 Packet," *Informatica* 46, no. 6 (2022): 125–133.

12. N. S. Lingamallu and V. Veeramani, "Secure and Covert Communication Using Steganography by Wavelet Transform," *Optik* 242 (2021): 167167.

13. P. Rakshit, S. Ganguly, S. Pal, and A. A. Aly, "Securing Technique Using Pattern-Based LSB Audio Steganography and Intensity-Based Visual Cryptography," *Computers, Materials & Continua* 67, no. 1 (2021): 1207–1224.

14. K. Gurunathan and S. P. Rajagopalan, "A Stegano-Visual Cryptography Technique for Multimedia Security," *Multimedia Tools and Applications* 79, no. 5 (2020): 3893–3911.

15. P. Geetha, V. S. Jayanthi, and A. N. Jayanthi, "Multiple Share Creation Based Visual Cryptographic Scheme Using Diffusion Method With a Combination of Chaotic Maps for Multimedia Applications," *Multimedia Tools and Applications* 78, no. 13 (2019): 18503–18530.

16. R. Sangeetha, G. Koteeswari, and M. Phil, "Securing Data in IOT Using Cryptography & Steganography Techniques," *International Journal of Research in Engineering and Science (IJRES)* 9 (2021): 1–5.

17. S. N. Bal, M. R. Nayak, and S. K. Sarkar, "On the Implementation of a Secured Watermarking Mechanism Based on Cryptography and Bit Pairs Matching," *Journal of King Saud University* 33, no. 5 (2021): 552–561.

18. P. Li, C. N. Yang, and Q. Kong, "A Novel Two-In-One Image Secret Sharing Scheme Based on Perfect Black Visual Cryptography," *Journal of Real-Time Image Processing* 14, no. 1 (2018): 41–50.

19. G. Selva Mary and S. Manoj Kumar, "Secure Grayscale Image Communication Using Significant Visual Cryptography Scheme in Real Time Applications," *Multimedia Tools and Applications* 79, no. 15 (2020): 10363–10382.

20. S. Sridhar, R. Sathishkumar, and G. F. Sudha, "Adaptive Halftoned Visual Cryptography With Improved Quality and Security," *Multimedia Tools and Applications* 76, no. 1 (2017): 815–834.

21. G. V. K. Murugan and R. Uthandipalayam Subramaniyam, "Performance Analysis of Image Steganography Using Wavelet Transform for Safe and Secured Transaction," *Multimedia Tools and Applications* 79, no. 13 (2020): 9101–9115.

22. V. Kumar, V. Pathak, N. Badal, P. S. Pandey, R. Mishra, and S. K. Gupta, "Complex Entropy Based Encryption and Decryption Technique for Securing Medical Images," *Multimedia Tools and Applications* 81, no. 26 (2022): 37441–37459.

23. B. Prasanalakshmi, K. Murugan, K. Srinivasan, S. Shridevi, S. Shamsudheen, and Y. C. Hu, "Improved Authentication and Computation of Medical Data Transmission in the Secure IoT Using Hyperelliptic

Curve Cryptography," *Journal of Supercomputing* 78, no. 1 (2022): 361–378.

24. S. Ahmad, M. F. Hayat, M. A. Qureshi, S. Asef, and Y. Saleem, "Enhanced Halftone-Based Secure and Improved Visual Cryptography Scheme for Colour/Binary Images," *Multimedia Tools and Applications* 80, no. 21 (2021): 32071–32090.

25. F. Varghese and P. Sasikala, "Secure Data Transmission Using Optimized Cryptography and Steganography Using Syndrome-Trellis Coding," *Wireless Personal Communications* 130, no. 1 (2023): 551–578.

26. B. M. Kumar, C. G. Sailesh, and R. K. Cv, "Secure Data Communication With Cryptography and Steganography," *International Journal of Electrical Engineering and Technology* 11, no. 3 (2020): 164–172.

27. M. Jana and B. Jana, "A New DCT Based Robust Image Watermarking Scheme Using Cellular Automata," *Information Security Journal: A Global Perspective* 31, no. 5 (2022): 527–543.

28. B. S. Ham, "Unconditionally Secured Classical Cryptography Using Quantum Superposition and Unitary Transformation," *Scientific Reports* 10, no. 1 (2020): 11687.

29. A. A. Ab, A. Gupta, and S. Ganapathy, "A New Security Mechanism for Secured Communications Using Steganography and Cba," *ECTI Transactions on Computer and Information Technology (ECTI-CIT)* 16, no. 4 (2022): 460–468.

30. W. Alexan, E. Mamdouh, A. Aboshousha, Y. S. Alsahafi, M. Gabr, and K. M. Hosny, "Stegocrypt: A Robust Tri-Stage Spatial Steganography Algorithm Using TLM Encryption and DNA Coding for Securing Digital Images," *IET Image Processing* 18, no. 13 (2024): 4189–4206.

31. K. Datta, B. Jana, and M. D. Chakraborty, "Two-Layers Robust Data Hiding Scheme for Highly Compressed Image Exploiting AMBTC With Difference Expansion," *Journal of King Saud University, Computer and Information Sciences* 34, no. 8 (2022): 5240–5260.

32. B. O. Al-Roithy and A. Gutub, "Remodeling Randomness Prioritization to Boost-Up Security of RGB Image Encryption," *Multimedia Tools and Applications* 80, no. 18 (2021): 28521–28581.

33. B. P. Valluri and N. Sharma, "Exceptional Key Based Node Validation for Secure Data Transmission Using Asymmetric Cryptography in Wireless Sensor Networks," *Measurement: Sensors* 33 (2024): 101150.

34. D. Singh, S. Kumar, C. Verma, Z. Illes, and N. Kumar, "Visually Meaningful Image Encryption for Secure and Authenticated Data Transmission Using Chaotic Maps," *Journal of King Saud University* 36, no. 10 (2024): 102235.

35. M. Alkhudaydi and A. Gutub, "Securing Data via Cryptography and Arabic Text Steganography," *SN Computer Science* 2, no. 1 (2021): 46.

36. L. Jiang and C. Mu, "Secure Identity Access and Data Transmission Scheme of Cloud-Assisted Intelligent Gymnasium," *Alexandria Engineering Journal* 115 (2025): 469–478.

37. G. Peter, A. Sherine, Y. Teekaraman, R. Kuppusamy, and A. Radhakrishnan, "Histogram Shifting-Based Quick Response Steganography Method for Secure Communication," *Wireless Communications and Mobile Computing* 2022, no. 1 (2022): 1505133.

38. L. N. Srinivasu and V. Veeramani, "Steganography Using Wavelet Transform for Secured Data Transmission," *Journal of Ambient Intelligence and Humanized Computing* 14, no. 7 (2023): 9509–9527.

39. A. Ngom, S. Djimnaibeye, N. F. Ngom, S. Sidibé, and O. Niang, "A New Wavelet Based Steganography Method for Securing Medical Data," in *International Conference on Innovations and Interdisciplinary Solutions for Underserved Areas* (Springer Nature Switzerland, 2022), 132–143.

40. E. S. B. Hureib and A. A. Gutub, "Enhancing Medical Data Security via Combining Elliptic Curve Cryptography With 1-LSB and 2-LSB Image Steganography," *International J Comp Sci Network Security (IJCSNS)* 20, no. 12 (2020): 232–241.

41. H. Samkari and A. Gutub, "Protecting Medical Records Against Cybercrimes Within Hajj Period by 3-Layer Security," *Recent Trends Inf Technol Appl* 2, no. 3 (2019): 1–21.

42. Z. Saeidi, A. Yazdi, S. Mashhadi, M. Hadian, and A. Gutub, "High Performance Image Steganography Integrating IWT and Hamming Code Within Secret Sharing," *IET Image Processing* 18, no. 1 (2024): 129–139.

43. R. K. Sogam, "Secure Data Transmission Using Cryptography, Image Processing and Steganography" (Doctoral dissertation, Dublin Business School), 2023.

44. A. Setyono, "Stegocrypt Method Using Wavelet Transform and One-Time Pad for Secret Image Delivery," in *2017 4th International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE)* (IEEE, 2017), 203–207.

45. M. T. Parvez and A. A. A. Gutub, "Vibrant Color Image Steganography Using Channel Differences and Secret Data Distribution," *Kuwait Journal of Science & Engineering* 38, no. 1B (2011): 127–142.

46. F. S. Hassan and A. Gutub, "Improving Data Hiding Within Colour Images Using Hue Component of HSV Colour Space," *CAAI Transactions on Intelligence Technology* 7, no. 1 (2022): 56–68.

47. A. K. Yadav, R. Roy, A. P. Kumar, C. S. Kumar, and S. K. Dhakad, "De-Noising of Ultrasound Image Using Discrete Wavelet Transform by Symlet Wavelet and Filters," in *2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI)* (IEEE, 2015), 1204–1208.

48. B. G. Banik and S. K. Bandyopadhyay, "Secret Sharing Using 3 Level DWT Method of Image Steganography Based on Lorenz Chaotic Encryption and Visual Cryptography," in *2015 International Conference on Computational Intelligence and Communication Networks (CICN)* (IEEE, 2015), 1147–1152.

49. S. Rustad, P. N. Andono, and G. F. Shidik, "Digital Image Steganography Survey and Investigation (Goal, Assessment, Method, Development, and Dataset)," *Signal Processing* 206 (2023): 108908.

50. J. Liang, "Image Classification Based on RESNET," *Journal of Physics: Conference Series* 1634, no. 1 (2020): 12110.

51. M. N. Abdullah, M. A. M. Shukran, M. R. M. Isa, et al., "Colour Features Extraction Techniques and Approaches for Content-Based Image Retrieval (CBIR) System," *Journal of Materials Science and Chemical Engineering* 9, no. 7 (2021): 29–34.

52. M. Koklu and I. A. Ozkan, "Multiclass Classification of Dry Beans Using Computer Vision and Machine Learning Techniques," *Computers and Electronics in Agriculture* 174 (2020): 105507.

53. T. Ahsan, T. Jabid, and U. P. Chong, "Facial Expression Recognition Using Local Transitional Pattern on Gabor Filtered Facial Images," *IETE Technical Review* 30, no. 1 (2013): 47–52.

54. Y. K. Goel and D. Samantaray, "Multi-Label News Classification Using bi-LSTM," *International Journal of Creative Research Thoughts (IJCRT)* 9 (2021): 1–8.

55. R. K. Sinha, N. San, B. Asha, S. Prasad, and S. S. Sahu, "Chaotic Image Encryption Scheme Based on Modified Arnold Cat Map and Henon Map," in *2018 International Conference on Current Trends Towards Converging Technologies (ICCTCT)* (IEEE, 2018), 1–5.

56. M. Agrawal and P. Mishra, "A Modified Approach for Symmetric Key Cryptography Based on Blowfish Algorithm," *International Journal of Engineering and Advanced Technology (IJEAT)* 1, no. 6 (2012): 79–83.

57. K. Gn, D. V. Ramaswamy, and M. G. Leela, "Performance Enhancement of Blowfish Algorithm by Modifying Its Function: Modified Blowfish," in *Innovative Algorithms and Techniques in Automation, Industrial Electronics and Telecommunications* (Springer Netherlands, 2007), 241–244.

58. Y. Fernando, D. Darwis, A. R. Mehta, W. Wamiliana, and A. Wantoro, "A New Approach of Steganography on Image Metadata," *JOIV: International Journal on Informatics Visualization* 8, no. 2 (2024): 968–976.

59. D. Kumbhakar, K. Sanyal, and S. Karforma, "An Optimal and Efficient Data Security Technique Through Crypto-Stegano for E-Commerce," *Multimedia Tools and Applications* 82, no. 14 (2023): 21005–21018.

60. T. S. Barhoom and S. M. A. Mousa, "A Steganography Lsb Technique for Hiding Image Within Image Using Blowfish Encryption Algorithm," *International Journal of Research in Engineering and Science (IJRES)* 3, no. 3 (2015): 61–66.

61. E. L. Kadhem and S. S. Baawi, "A Secure and High Capacity Image Steganography Approach Using Huffman Coding and RSA Encryption," *Journal of Al-Qadisiyah for Computer Science and Mathematics* 15, no. 2 (2023): 35.

62. K. Sethi, B. Sahoo, B. P. Kumar, K. Dhal, W. Cho, and G. P. Joshi, "Lightweight DWT Steganography With ECC-ChaCha20 for Secure Medical IoT Systems," *IEEE Access* 13 (2025): 142948–142960.

63. https://drive.google.com/file/d/1-foZ3dV5OCsqXQXT84UeKtrAqc5CkAE/view.

64. https://www.kaggle.com/datasets/kmader/mias-mammography.

65. https://www.kaggle.com/datasets/mathurinache/gpr1200-dataset.

66. S. K. Ghosal and A. K. Sahu, "AI-Powered Steganography: Advances in Image, Linguistic, and 3D Mesh Data Hiding–A Survey," *Journal of Future Artificial Intelligence and Technologies* 2, no. 1 (2025): 1–23.

67. F. Al-Shaarani and A. Gutub, "Securing Matrix Counting-Based Secret-Sharing Involving Crypto Steganography," *Journal of King Saud University* 34, no. 9 (2022): 6909–6924.

68. T. AlKhodaidi and A. Gutub, "Refining Image Steganography Distribution for Higher Security Multimedia Counting-Based Secret-Sharing," *Multimedia Tools and Applications* 80, no. 1 (2021): 1143–1173.