International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 08, August-2022

A Stegano-Cryptography Framework for Securing Cloud Data with Enhanced Monarch Butterfly Optimization

V. Mahavaishnavi
Research Scholar
Department of Computer Science and Engineering,
Annamalai University,
Annamalai Nagar – 608 002

Dr. R. Saminathan
Associate Professor
Department of Computer Science and Engineering,
Annamalai University,
Annamalai Nagar – 608 002

Dr. P. Anbalagan
Assistant Professor
Department of Computer Science and Engineering,
Annamalai University,
Annamalai Nagar – 608 002

Abstract:- In today's environment, transmitting content on the web, such as health data and other classified information is not safe. It is encoded as a picture, audio, or word document to secure this confidential material that can only be decoded using a particular key. In this research, systems for medical steganoanalysis is framed with the Enhanced Monarch Butterfly Optimization (EMBO) model for successful screening of pixels and for embedundisclosed notification (i.e. transcriptremedial claim information) in the main picture to facilitate protection to surveillance interactions and preserving information for attempting to secure health information to prevent healthcare science cyber-attacks. Firstly, the image is transformed to frequencies domain using multilevel Discrete Wavelet Transform (DWT) and the pixel choosing is optimized using the EMBO method in the spectral analysis. For measuring cost metric, the EMBO-based pixel selection technique employs an optimization technique that is dependent on the objective functions, which evaluates the entropy, edge and intensity of the image. The suggested Stegano-cryptography technique strategy is compared to other current schemes in provisions of Mean Square Error (MSE) andPeak-Signal-to-Noise-Ratio (PSNR) to verify the applicability of the projected methodology, which was accomplished on the MATLAB working tool.

Keywords:- Steganography, Object,Covert, Segmentation, Entropy, Intensity,Enhanced Monarch, Edge,MSE and PSNR.

I.INTRODUCTION

The safeguarding of data in addition to processing against illegal monitoring, alteration or intervention is referred to as information security. Cloud technology necessitates stringent safeguards based on several characteristics of a large, loosely coupled system. Multiple aspects relating to data service, administration and privacy among others must be addressed[1]. Security and privacy issues are important considerations, which may be accomplished through the use of cryptographic, asymmetric encryption and advanced detection techniques. Cryptography is the art of transferring data in a manner that the data's presence is obscured. It assures that the signals injected cannot be recovered by anybody else. When it comes to exchanging confidential information, digital watermarking adds another degree of security by embedding the media. Steganoanalysis makes use of three characteristics: virtually every aspect of life, endurance and sturdiness. This technique has a wide range of commercial uses, including copyrighted works for digital products such as films and photos.

Cryptography is used by Cloud Service Providers to offer a high level of data protection. Cryptography is a means of jumbling information and communicating data in a specific format that can only be read and operated by those who want to read and operate it[2]. There seem to be two forms of cryptography: symmetric key cryptographic protocols, where the transmitter and recipient use the same key and asymmetrical or public key cryptography, where the transmitter and recipient use separate keys. Many different cryptographic systems have been suggested by scientists. A safe and adaptive encryption techniques approach can be used to preserve the security or obscurity of essential information.

Many Cloud Provider supply cloud service memory, in which they store customer vital information in the cloud data storage, this helps to mitigate cloud infrastructure vulnerability[3]. Because data must be routinely exchanged in multi-tenanted systems like a clouds, matrix and so on.Maintaining critical and sensitive information in the cloud computing becomes a tough topic. As a result, in order to store crucial information on social data storage, safe and dependable cryptography procedures are required.

Because it will give two-way data confidentiality being transferred on the system, a mixed technique of steganogrpahy may be implemented [4]. When hidden message and encryption are coupled, the information is encrypted and hidden behind the background picture, providing a degree of security.

The work's primary goal is to guarantee the secrecy of important files held on cloud environment. Cybersecurity with an encrypted message has now been utilized to secure the information for this study. Hidden message is presented in the following step, using Bi-orthogonal Wavelet Transforms (BWT) and the Encoding and Decoding approach. The optimal solution is then calculated using three optimization techniques: Enhanced Monarch Butterfly Optimization (EMBO), Spider Swarm Optimization (SSO) and Cuckoo Search (CS).

II.RELATED WORKS

Steganography may be accomplished in a variety of methods, including integrating data into images, videos and other formats. [5] Conducts the conjunction of any item with Media.For image steganography, a DWT-DCT methodology is utilized. Steganography is safer since it can combine both speech and picture secret information. To split a picture into peak, medium and intermediate component, DWT and DCT convert that from the spatial and frequency arena. CT is used to shrink the body. Choosing the non-key image data for anchoring and extracting of actual text followed by DWT-DCT modification of messaging and videos.

Cryptography is the art of any secret message via the use of writing or code. And their obfuscation techniques is correct, steganography is the art and technology of composing in such a manner which nobody save the transmitter and intended recipient questions the statement's presence. The plain text of 58-bit chunks was utilized to create a ciphertext of the 8-bit brick using a 10-bit password, with the 8-bit blocks being IP, FK, SW, Fg, IP-1. The encrypted message will indeed be created from these 8-bit blocks. During the first method, an array for a bit and a maximal byte is constructed. The array items will be separated and evaluated using the key, as well as the least major and most substantial bits[6].The second solution uses encryption pixels and unencrypted pixels to use the S-DES algorithm to construct each byte (pixel) of all three vectors (R, G, B matrix of content). The encryption used it to encryption each pixel is 10-bit in length and is derived from the picture pixel. After running it via MATLAB, this is the outcome. After that, we use the S-DES to retrieve the picture pixels, which we then transform to the test. On the other hand, the S-DES encryption picture may be obtained from the segmented image. The AES technique is also used by Internet Key Exchange (IKE) to send the secret key to the receiver for message processing. The image will be protected with the AES method in this [7]. If it's taken, it'll be in the middle of the procedure. The picture will then be decreased via RGB transformation, after which encrypting will be conducted. In this case, we'll use Encryption technology using a signature bit with a value of 1 frame and a matrix value of 4. After ten rounds of AES encryption, a cypher product is formed, which can only be viewed by someone with a secret key. By simply reciprocating the cryptographic algorithms, the cryptographic algorithm is the same as the encryption process. The video picture is incoherent after encryption signature bits of all DCT coefficients of the lone Integration node.This is the encrypting level in the middle. No regardless what sort of frame is utilized, this technique secures at most 128 bits. This significantly decreases the number of encryption calculations required to get good encryption solutions.

To conduct integrated encryption decryption, [8] adopted a combination technique of cryptography and steganography. At the same time, the LSD approach based on hashes was utilized. In its system architecture, cryptographic and steganography will operate concurrently, with one side visual input being accepted and all frames being transformed to binary, as well as the other side information being provided in a concealed version and Encryption algorithm executed. These two parts will be inserted afterwards. Then it'll be turned into a stegano covering. Then, utilizing MATLAB this stegano cover will be removed.The RSA technique will then be used to transform that from cypher text to text format. As a result of this technology, encryption and steganography may be used to convey data in a safe manner. Where cryptographic is used to protect concealed info via text and data encryption is used to withhold information in images.

In [9], a novel security mechanism is introduced that combines cryptographic primitives with cryptographic. The author has utilized AES for cryptographic protocols, which has since been employed in this research; the author has also described the aim of utilizing this technique.

The author of [10] provides a definition of steganography for safe data transfer. These ideas have now been examined in order to understand how our technique works. The ECC technique was used to increase the security of a mixture of encryption techniques. This technique has been used to generate a shared key for plain text encrypting. A hidden graphic is sometimes used as a covering for an encrypted message, typically 40% of the value combined with the background image.

According to [11] the user must be able to however many bits in the picture should be changed depending on the scenario. In addition, the random bit generating will assign a randomized embedded site. This two - pronged approach improved security. The process's reliability and distinctiveness have both been improved.

III.DESIGN AND IMPLEMENTATION OF PROPOSED METHODOLOGY

Content is safeguarded utilizing three tiers of cloud computing security in this method.Theinitial level is customer id and code word, the stage 2 is cryptographic using sign- crypto and the third level is asymmetric encryption with various optimization approaches. People are usually authorized using their user id and password. Unfortunately, there is a risk that the id and passwords will be compromised by hackers. The sign-crypto technique is used to protect the message, which is the second floor, to guarantee that the data is secure.Data encryption is employed at the next stage; in which encoded data is inserted in the image using Bi-orthogonal Wavelet Transformations (BWT) and used for band decompose. Following wavelet transform, three separate techniques, including Social Spider Optimization (SSO), Cuckoo Search (CS) and Enhanced Monarch Butterfly Optimization (EMBO) are used to incorporate those pictures. EMBO outperformed the competition consisting of three techniques.

Stegano-cryptography

Figure 1 illustrates the proposed stegano-cryptography infrastructure for this project, which includes several features such as userid and password, information, cryptography and steganography.The sign-crypto technique is used in this cryptographic to secure the data. Necessarily a legal is a public-key encryption system that serves as both a numerical identifier and an encryption technique at the same time.

Sign-crypto algorithm

The key distribution technique is a probabilistic process that accepts any two important integers (p,q) as input and outputs publicly (n,e), privatized (n,d) and symmetrical (C k) keys (p,q) mechanism for creating keys →(P_k,S_k,C_k).

Data encryption mechanism (DEM)

The probabilistic algorithm (AES) uses an original comment M and a symmetrical key C k to generate a cypherpassage CM. (M,C k) method for generating keys (CM).

Key derivation key

The probability procedure that takes an numeraln and an numeral duration n Len as inputs and produces (z,Z), where z is a spontaneous integer between 0 and n-1 and Z is n Len a sequence charge inside the type of the leading necessary bit initial that is converted from z. (n,nLen) the secret to key extraction (z,Z).

Encryption

The probabilistic approach that receive arbitrary key numeral z and recipient public key $P_k(n, e)$ it outputs (c,C), for which c is the cypher content and C is a nLenstring charge inside the type of its first crucial small piece, which is altered $(P_k, (n, e))$ Encryption→ (c, C).

Key derivation function

The probability (hashing method (MD5)) that generates the output Key Encrypting Key (KEK) from a random input numeral Z and the height of the encrypt techniques key kek Len produce from Z. (kekLen, Z) is the main extraction function (KEK).

Wrapping function

Wrap is a probabilistic procedure that takes a symmetric encryption C, k and a Key Encrypting Key (KEK) as inputs and produces wrapped Key WK as a result. (C_k,KEK) WK is the tightly wrapped function.

Concatenation

The stochastic method that accepts a Wrapped Key (WK) as input, ciphertext C as outputs and returns an Encapsulating Key (EK).

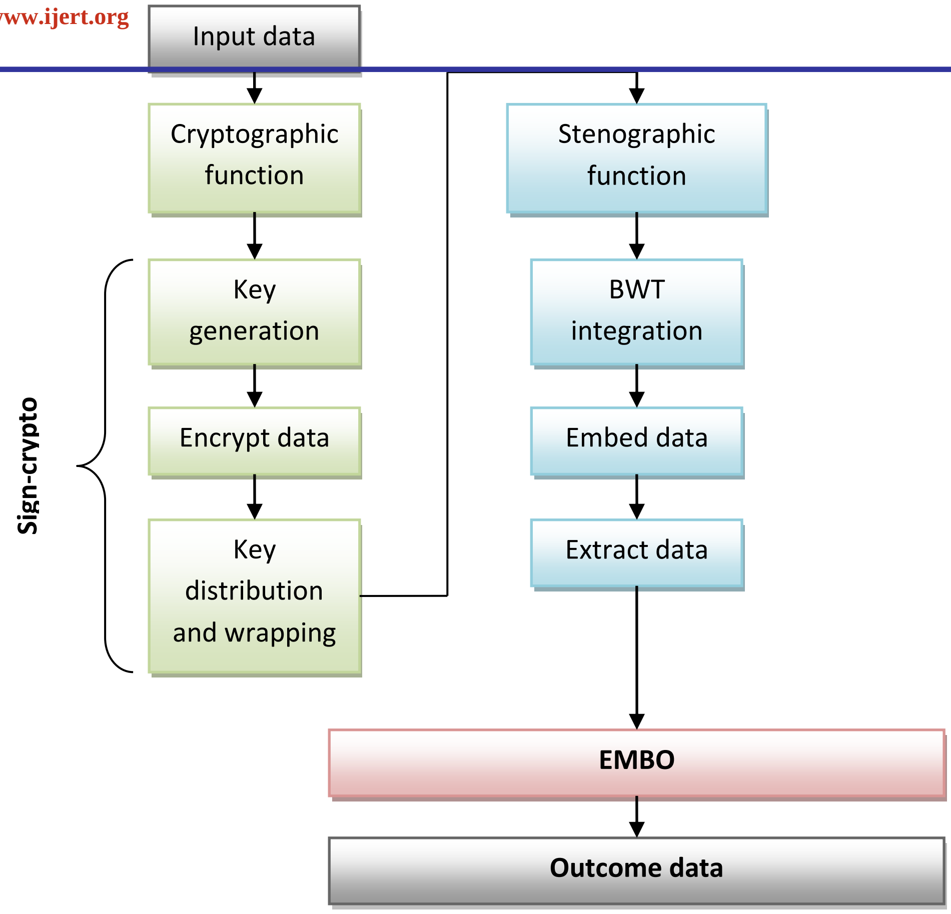


Figure 1: Flow of the Stegano-cryptography framework

Sign-crypto

The probabilistic algorithm that takes input ciphertextCM, sender's private key $S_k(n,d)$, Encapsulated Key (EK) and outputted the signcrypted data (δD). $(CM, S_k, (n,d), EK)$Sign-crypto→ (δD) by means of this sign-crypo algorithm in Figure 2, the information has encrypted resolutely and for the next stage of safetysteganography is done.

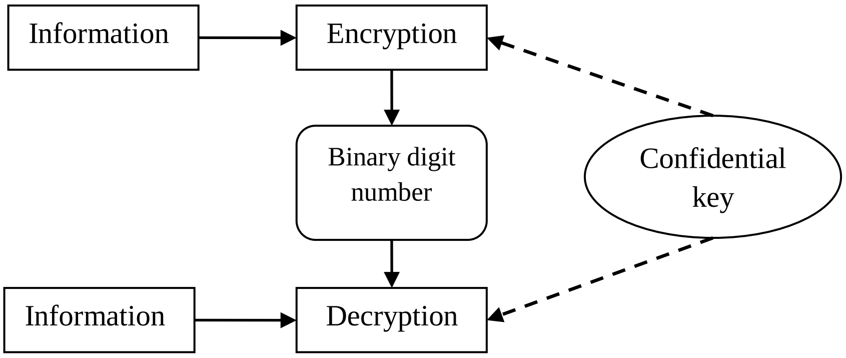


Figure 2: Sign-crypto procedural blocks

Steganography technique

Different procedures such as Bi-orthogonal Wavelet Transform (BWT), Integrating and Extracting approaches are employed inthe optimization strategy.

Bi-orthogonal Wavelet Transforms (BWT)

A bi-orthogonal waveform is defined as a wavelet with an invertible but non-orthogonal wavelet transform. Bi-orthogonal wavelets provide for a greater number of degrees of freedom in designing than conventional wavelets. The possibility of delivering symmetric wavelet functions provides an extra degree of possibilities. This collection of wavelets demonstrates the linear phase property, which is essential for picture reconstructing. The qualities deduced by using two wavelet transformation, one for degradation and the other for reconstructions, instead of a singular wavelet are fascinating.

Steganography: EmbeddingProcess

Input: Information$I_a[x,y]$,image$M_g[x,y]$

Output:Steganographyimage$S_g[x,y]$

Procedure:

Utilizeattemptseparationmethod, the input contentionorder$I_e[x,y]$, has separated by a quantity for non-overlapping shot$D[x,y]$. Then, identify the number of frames $E[x,y]$ incorporated in every one separated shot $D[x,y]$ to embed. Exchange image $M_g[x,y]$ into vector form of arepresentation$W[x,y]$.

- We must discover those blue regions around each frame in a picture sequence using R, G, and B.
- Those blue lengths BE[x,y] for each distinct picture are focused for embedeach vector instance W[x,y] under one of those green sections of every screen.
- Disintegrate the blue section BE[x,y] around each split outlines E[x,y] into four sub-bands, for illustration so as to the changed T_f [x,y] framework is HH, HL, LH, and LL, using the Bi-orthogonal Wavelet decomposition.
- Choose the low-frequency sub - bands (HL, LH) commencing with the modified frame to incorporate the picture M_g [x,y].
- The HL and LH sub-bands used to embed the stegano picture are divided into 5 categories in the same way that the similitude grid is divided into three categories. Only the cosine similarity grid of the HL and LH bands has been chosen to incorporate those two comparable sections of the stated that the prevalence picture in the lower half C_p [x,y].
- Only the resemblance grid has been implemented in the top section U_p of the HL sub-band using the necessary stages: As described in equation 1, find the mean (C_p) and the highest amount max(C_p) of the chosen embedded component (C_p).

$$M(C_p) = \sum_{n=1}^{i} C_p(n) \qquad (1)$$

- Embed those watermark bits 0 or 1 in a zigzag way in the decided embedding part, since the steganography may be that image. Two situations with admiration to the steno image develop.

Case 1: With respect to embedding the watermark bit '1'.

The values in the embedding part $C_p[x,y]$ are compared against the maximum value $\max(C_p)$ and changed as follows: If the value in the chosen embedding, component might be larger than 1, take the absolute value and embed the same. Otherwise, if the amount within the incorporating an element is less than 1, use the comparing pixel to estimate the optimum possibilities and then embed the modified quantity, as defined in equation 2.

$$\begin{gathered}\text{if} C_{p(m)} > 1 \\ \text{then} C_p[a,b] << xs \leq C_{p(m)}\rvert \\ \text{else} C_p[a,b] \lll< C_{p(m)} + \max(C_F) \\ \text{end if} \qquad (2)\end{gathered}$$

Case 2: When it comes to inserting the watermark, pixel'0'is the best option.
Make the absolute number and incorporate them self-same if the value of the integrating component C_p [x,y] is less than 0. However, if the quality of the immersing is better than 1, the comparative image is subtracted from the larger values max ((c_p)) and the revised quantity is embedded as stated in equation 3.

$$\begin{gathered}\text{if} C_{p(m)} < 0 \text{ then} \\ C_p[a,b] << xs\lfloor C_{p(m)}\rfloor \\ \text{else} \\ C_p[a,b] << C_{p(m)} - \max(C_p) \\ \text{end if} \qquad (3)\end{gathered}$$

- The bottom elements of that similarity matrix, L_e are similarly buried beneath the LH sub-band. In addition, each image shows a frame for each shot inserted beneath it.
- To improve the image's quality, segregate each of the included pictures for the embedded attributes.
- To create the watermark information picture sequence S_g[x, y] map the modified sub-bands beneath their separate positions and use the Inverse Coefficient Wavelet Transform.

Steganography: Extraction Process

Input:textinsequence $I_o[x,y]$,imageextent.
Output:enhanced stenographic image $S_{rz}[x^i, y']$
Procedure:

- The input text material Io [x,y] is separated into a number of non-overlapping shots D' [x,y] using the shot divisions methodology. The no of frame E' [x,y] in every fragmentation attempt D' [x,y] that has to be retrieved is then determined. The blue segment BE' [x,y] of all the segmented pictures are taken to recover the underlying steganography components.
- The frames blue sections are decaying with the help of the Bi-orthogonal Wavelet. Compress using the HH, HL, LH, and LL subbands.
- The low-frequency subbands (HL, LH) from the converted pictures were picked to extract the factors associated picture.

- The stegano picture, commencing with those incorporating a component, is retrieved in a zigzag pattern, commencing by means of the HL and LH subbands and progressing through the stages below. The retrieved pixel value is one if the imbedded bit amount is bigger than the mean pixel value. If it's smaller, the retrieved pixel might be 0 at that moment, as indicated in equation 4.

$$\begin{cases} 1, & C_p(n) > mean\left(C_p\right), \text{ where } 0 < n < j \\ 0, & \text{otherwise} \end{cases} \quad (4)$$

- To obtain the stegano picture, generate the following with the size of the steganograph image and insert the obtained image in it.
- The stegano image Arz [x',y'] is created by using the reversal method of column seeking function.

Enhanced Monarch Butterfly Optimization

EMBO is a 2015 proposal for a new nature-inspired heuristic algorithm. It is based on the migratory behavior of the monarch butterfly. All Monarch Butterfly specimens in EMBO are idealized and therefore only comprised of two places, namely the northwestern United States Mexico (Land 2) and southern Canada (Land 1) [11]. The monarch butterfly, individual of the most well-known butterflies in North America, with a distinctive golden and black patterning. It's a Nymphalidae (milkweed butterfly) from the Nymphalidae family. Male and female monarchs have distinct wing patterns that would be second-hand to distinguish them. Every summer, the North American monarch butterfly migrates hundreds of kilometers from the United States and southern Canada to Mexico. It passes east of the rock-strewnheap on its way to California. They travel 100 or 1000 of miles to Mexico to overwinter. Migration southward begins in August and terminate when the originalcold arrives. In the spring, though, the reverse occurs. During one of these migrations, the females deposit ovaries in order to produce children. According to new research, certain butterflies conduct Levy flying when migrating or moving [12].To make EMBO queen butterfly movement behavior solve various computational difficulties, the migratory behavior of monarch butterflies may be idealisedkeen on the subsequent guidelines [13].

- Monarch butterflies are found in either ground 1 or ground2 that account for the majority of the monarch butterfly populations.
- A migration problem occurred each kid monarch moth individuality from a monarch butterfly in ground 1 or ground 2.
- An elderly monarch butterfly will die after a youngster is produced in order to maintain the butterfly species. This may be done using the EMBO approach by swapping its parents with freshly created ones if it has a higher fitness than its parent. The freshly created one, from the other hand, is likely to be eliminated if it does not outperform its parents in terms of strength. The parent is retained entire and undamaged in this circumstance.
- The monarch butterfly folks by means of the better strength pass on to the subsequently generations naturally and no one can modify them. This ensures that the monarch butterfly majority's quality or efficacy can never diminish with the passage of time. As a result, the migrations operation and the caterpillar adjustment operators are used to change the locations of monarch butterflies.

Fitness evaluation

The EMBO optimization approach was used to find the pixel location in this study. We developed a differential equation for evaluating the employability of each image pixel that was based on the edge, heterogeneity and intensity of the pixel points [14-15]. The population's optimal location was determined using the objective functions. The charge matrix, which carried elsewhere all the image locations of a picked at random particles in the swarm, determines the objective functions. The cost substring dimension is (i/2 * l/2). Let's call the community 'Pij' and the robustnesspurpose'Fij' as follows:

$$F_{ij} = \sum_{i=1}^{n} \sum_{j=1}^{n} P_{ij} * C_{ij} \quad (5)$$

Where, 'C_{ij}' is the population's integral gain. The populations 'Pij' is determined by three factors: edge, unpredictability and intensity. The computational complexity is as follows:

$$C_{ij} = 1/3[B_{ij} + E_{ij} + I_{ij}] \quad (6)$$

The edges, permeability and amplitude of the pixel points in the ith row and jth column of the data set are represented by 'B_{ij}', 'E_{ij}' and 'I_{ij},' accordingly.

Numerical Results

The material has been protected in a variety of methods, and assessment parameters have already been applied to a stegano picture and a normal image as a result of the previous explanation. The Normalized Correlation (NC) andPeak Signal-to-Noise Ratio (PSNR) values are calculated among the numerous assessment measures. In addition, the factors associated image and standard image have been subjected to Man-in-the-Middle Attacks (MMA), Denial-of-Service Attacks (DSA) and Brute-Force Attacks (BFA). The PSNR and NC parameters are derived using three optimization technique: the Cuckoo Search (CS) strategy, the Particle Swarm Optimization (SSO) method and the Social Spider Optimization (SSO) algorithm. MATLAB is used for the whole development.

T

able 1:Process of Stegano-crytography(Without attacks)

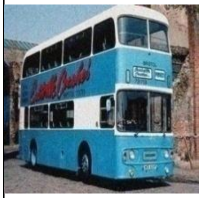
Data	Sign-crypto Encryption	Stegano image	SteganoEmbed	SteganoExtract	Sign-crypto- Decryption		
			PSNR	NC	DSA	MMA	BFA
Welcome	00101 00010 …	 Water.jpg	38.066	0.992	22.651	13.147	0.381
Hi I am fine	00101 00010 …	 Bus.jpg	35.562	0.996	33.378	24.621	0.591

Table 2: Process of Stegano-crytography(With attacks)

Images	Attacks	PSNR	NC	DSA	MMA	BFA
 Water.jpg	Noise	20.3696	0.8572	38.4213	46.1609	53.5414
	Blurring	19.7705	0.6695	40.7674	79.8567	59.2156
	Filter	37.0766	0.9733	35.1305	51.6446	63.3743
 Bus.jpg	Noise	20.0798	0.8182	34.8146	33.2023	55.2194
	Blurring	16.986	0.6693	27.3208	55.9793	68.0609
	Filter	32.0056	0.7976	33.4431	47.4002	50.7279

Efficiency analysis of EMBO

Figure 3 displays an analysis of multiple optimization algorithms and their efficiency in percentages.

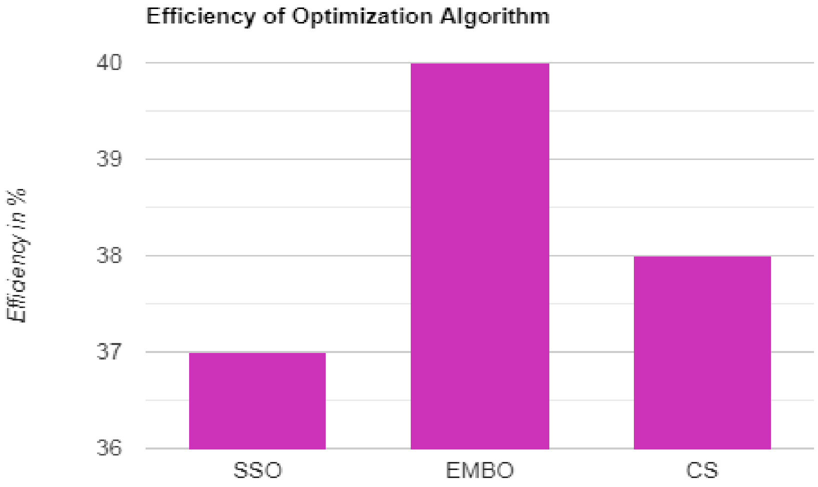


Figure 3: Efficiency computation

When comparing the EMBO algorithm to the Social Spider Optimization (SSO) technique and the Cuckoo Simulated (CS) annealing, it can be shown that the EMBO algorithm has an increased performance of 6.68 percent over the period. As a result, the suggested research crypto-stegano outperforms the competition.

Comparative analysis of PSNR

The overall performance of a picture when the content was inserted is determined by the peak signal to noise ratio. The greater the PSNR score, the better the high resolution.

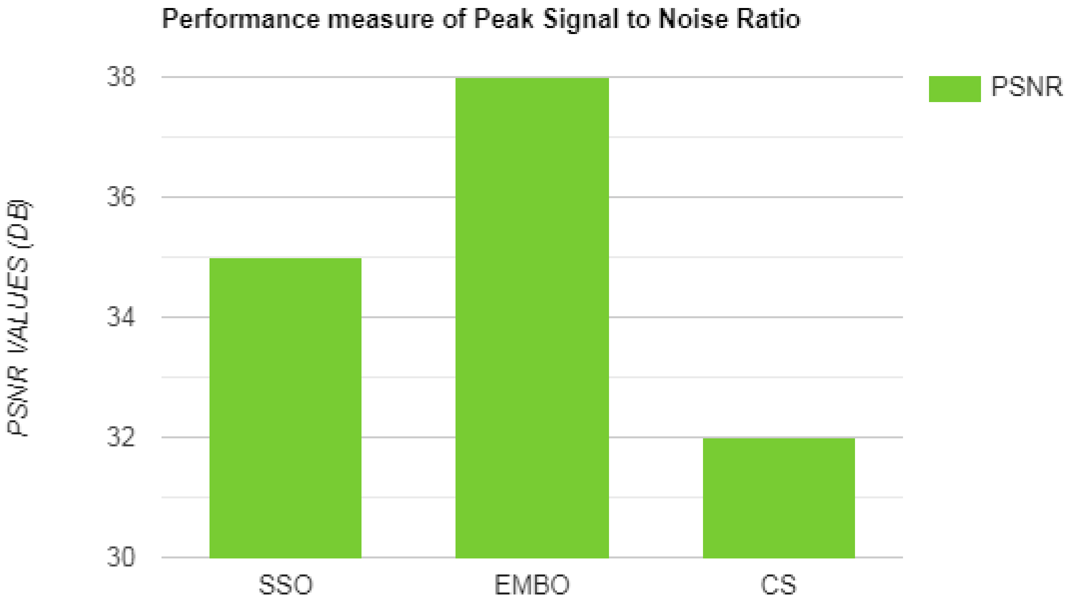


Figure 4: PSNR computation

The peak signal noise ratio of SSO is bigger than CS, and less than EMBO, per the numbers in Figure 4. It's because of the cryptographic technique that was utilized for encrypting and decrypting, as well as the unique increased social spider optimizations. In comparison to previous techniques that were available, the sign-crypto method delivers higher security and computational complexity. When comparing the EMBO technique to the Social Spider Optimization algorithm and the Cuckoo Simulated annealing, it can be shown that the expanded social spider optimization technique has a higher PSNR, which is 6 percent higher on average.

Comparative analysis of Normalized Correlation

The normalized cross-correlation of matrices is computed using normalized connectivity. The image's normalized data is converted with or without attacking, and the normalized association for the whole optimization problem is always smaller than that one, indicating that the improved social spider optimization algorithm is effective.

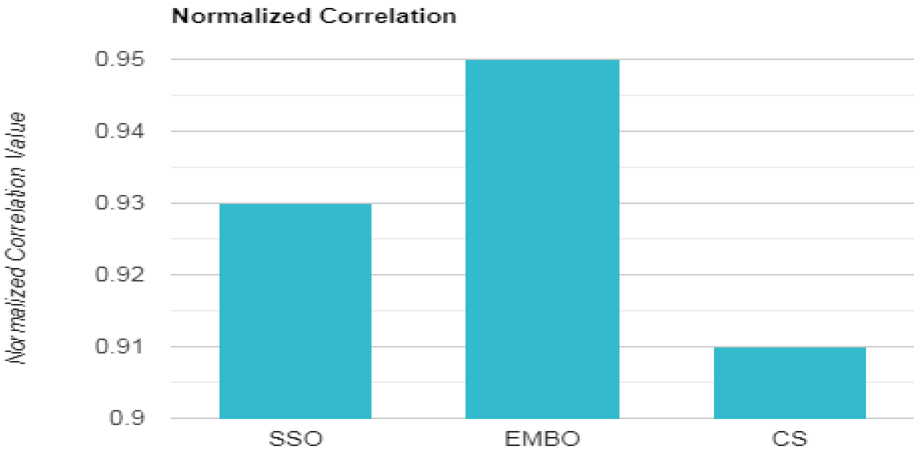


Figure 5: NC computation

When compared to a different scene, the normalized correlation of SSO is substantially greater than CS, as per the data in Figure 5. When comparing the EMBO approach to the Social Spider Optimization method and the Cuckoo Search method, it can be shown that the EMBO technique has a greater NC of 0.03 percentage points.

Comparative analysis of CryptographyAlgorithm

When compare to the present approach, the suggested method takes less time to execute. Figure 6 demonstrates the overall completion time for both the proposed and current methods, with the effectiveness of the blowfish, RSA and DES algorithms being evaluated. It demonstrates that the suggested crypto-stegano, in combination with the sign-crypto method, requires the least amount of time to execute.

Table 3:Execution time of Cryptography Algorithm

Method	Execution time(ms)
Sign-crypto	3539
Blowfish	34109
RSA	196451
DES	47541

Table 3 illustrates how long mathematical calculations take to run, and it's evident that the sign-crypto technique needs the least amount of time.

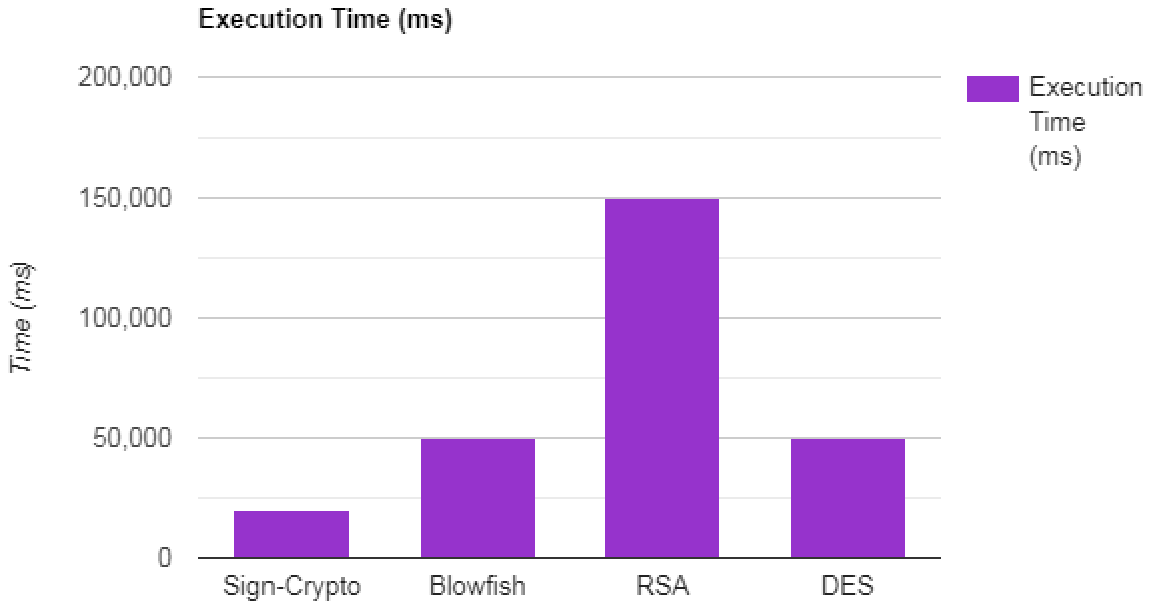


Figure 6: Execution time computation

Figure 6 illustrates how long sign-crypto, blowfish, RSA and DES take to execute. Figure 6 shows that when compared to other approaches, the sign-crypto technique requires less time. As a result, it can be stated that the sign-crypto method used in the crypto-stegano approach, together with the EMBO method, is effective in safeguarding information in the cloud.

IV.CONCLUSION

Several technologies were used to safeguard information in the cloud, including cryptography to encode material using the sign-crypto technique, and steganography with BWT for Embedding and Extraction. Normalized Correlation (NC) and Peak Signal-to-Noise Ratio (PSNR) are the parametersecond-hand to determine effectiveness. After using optimization method such as Cuckoo Search (CS), Enhanced Monarch Butterfly Optimization (EMBO) and Social Spider Optimization (SSO), the picture is subjected to multiple Denial-of-Service Attack (DSA), Brute-Force Attack (BFA)and Man-in-the-Middle Attack (MMA). In comparison to other algorithms, EMBO performed better, as evidenced by the results and analysis.The comparing diagrams for something without strikes and with strikes had appeared (Noise, Blurring and Filter). For water and bus pictures, the greatest peak signal to noise ratios are 38.06 and 35.56 respectively and for withoutattack and with attack 37.0765 and 32.0055. In comparison to previous algorithms, the improved social spider optimization algorithm has a high PSNR value. For the water and bus the normalized coefficient value are 0.9910 and 0.9947 without attack and 0.97921 and 0.8181 with assault. Our suggested hybrid crypto-stegano approach is clearly capable of retrieving the optimum result significantly more efficiently in the above-mentioned scenarios. In the future, a variety of processes and Machine Learning based approaches can be used to attain better trade off.

REFERENCES

[1] Al-Shaarani, F. &Gutub, A. (2021),“Securing matrix counting-based secret-sharing involving crypto steganography”, Journal of King Saud University-Computer and Information Sciences.

[2] Alkhudaydi, M.&Gutub, A. (2021),“Securing data via cryptography and Arabic text steganography”, SN Computer Science, 2(1), 1-18.

[3] Wahab, O. F. A., Khalaf, A. A., Hussein, A. I. & Hamed, H. F. (2021), “Hiding data using efficient combination of RSA cryptography, and compression steganography technique”, IEEE Access, 9, 31805-31815.

[4] Joshi, R., Trivedi, M. C., Gupta, A. K.&Tripathi, P. (2021), “Current Trends in Cryptography, Steganography and Metamorphic Cryptography: A Survey”, In Advances in Computational Intelligence and Communication Technology (pp. 237-247), Springer, Singapore.

[5] V. M. Wajgade& S. Kumar, “Enhancing Data Security UsingVideo Steganography,” Int. J. Emerg. Technol. Adv. Eng., vol. 3,no. 4, pp. 549–552, 2013.

[6] V.V. Korgaonkar& M. N. Gaonkar, “A DWT-DCT combinedapproach for video steganography,” RTEICT 2017 - 2nd IEEEInt. Conf.Recent Trends Electron. Inf. Commun. Technol. Proc.,vol. 2018-Janua, pp. 421–424, 2017.

[7] Keshav S. Kadam& AmarDeshmukh, “Video Frame Encryption Algorithm using AES”, Int. J. Eng. Res., vol. V5, no.06, pp. 588–591, 2016.

[8] N. A. Al-Juaid, A. A. Gutub, & E. A. Khan, “Enhancing PCData Security via Combining RSA Cryptography and Video-Based Steganography”, J. Inf. Secur. Cybercrimes Res., 2018.

[9] Taqa, Alaa, Zaidan, A., Bahaa& Bilal (2009),“NewFramework for High Secure Data Hidden in the MPEG UsingAES Encryption Algorithm”, International Journal of Computerand Electrical Engineering. 10.7763/IJCEE.2009.V1.87.

[10] Taha, Mustafa &Shafry, Mohd&Rahim, Mohd&Lafta, Sameer&Hashim, Mohammed &Alzuabidi, Hassanain (2019), “Combination of Steganography and Cryptography: A shortSurvey”, 10.1088/1757-899X/518/5/052003.

[11] Chen S, Chen R &Gao J, “A monarch butterfly optimization for thedynamic vehicle routing problem algorithms”, 2017, 10(3):107.

[12] FengY, Wang G. G, Deb S, Lu M & Zhao X J, “Solving 0–1 knapsackproblem by a novel binary monarch butterfly optimization”, NeuralComput&Applic. 2017, 28(7):1619–34.

[13] Wang G. G, Deb S, Zhao X & Cui Z,“A new monarch butterfly optimizationwith an improved crossover operator”, Oper Res.2016, 18(3):731–55.

[14] Preethi, P. &Asokan, R. (2019),“A high secure medical image storing and sharing in cloud environment using hex code cryptography method-secure genius”, Journal of Medical Imaging and Health Informatics, 9(7), 1337-1345.

[15] Preethi, P.&Asokan, R. (2019),“An attempt to design improved and fool proof safe distribution of personal healthcare records for cloud computing”, Mobile Networks and Applications, 24(6), 1755-1762.