AN ENHANCED SECURED IRIS TEMPLATE USING STEGANOGRAPHY AND CRYPTOGRAPHY

Supported by tetfund
TERTIARY EDUCATION TRUST FUND

Agu Edward Onyebueke[1] and Danbeki Mercy[2]
[1,2]Department of computer science, Faculty of Computing and Information System
*Corresponding Author: aguedward@fuwukari.edu.ng

Received: September 14, 2024 Accepted: November 28, 2024

Abstract: The issue of exploiting or hacking a biometric template for harmful purposes can be resolved by integrating steganography and cryptography into the biometric system. It is no longer safe enough to identify someone using a password or personal identification number (PIN). Iris recognition is considered to be one of the best and accurate form of biometric measurements compared to voice, palm print, ear and hand geometry because iris of every person is unique, it never changes during human life, time and highly protected against damage. In this work, a cipher text is embedded into a cover image by the steganography (LSB) algorithm, creating a stego image. The two-level security techniques provide high embedded capacity and eminence stego images that are resistant to attackers. An iris template was generated from the MMU dataset and encrypted using the hybridize cryptography (Blowfish and AES) algorithm. Only a PNG image was used as the master or cover file. The dataset for this study was obtained from CASIA iris-V4 Dataset.

Keyword: Iris template; BLOW FISH; Advance encryption standard; LSB; Biometric system

Introduction:

The problem of information integrity and confidentiality is growing at an alarming rate due to the recent advancements in digital technology. Secure data transfer over communication channels has been a major problem since the dawn of the digital (Agu et. al., 2019). The majority of information is stored electronically thanks to advances in ICT. As a result, information security has faced a significant problem (Islam et al., 2015). To prevent any unauthorized access to Personal identification of information, a robust security technique is required. For the biometric system to be more robust, any technology that can both safeguard the template and improve performance must be used (Biu et al., 2018). Because they include distinctive features that make each person unique, biometric signatures such as fingerprints, iris, hand geometry, palm print, and gestures have all shown to be effective methods for determining an individual's identification. (Das et al., 2020) Cryptography and steganography are common methods for encrypting or hiding data by manipulating it. (Revenkar et al., 2010) The essential components of information security cannot be guaranteed by cryptography alone; as a result, additional techniques like steganography which is the second method for secure data transfer in a computer system are required to protect against threats like denial of service attacks and total information system failures (Abikoye et al., 2020) Steganography is similar although it adds a different measurement to cryptography. The purpose of steganography is to create a stego object by enclosing a crucial message in a typical cover item (text, image, audio, video, etc.) and transmitting it to the intended recipient therefore the recipient who is not the actual owner will not be able to see it, because the secret data is not visible to the human eye. (Alabdulrazzaq & Alenezi, 2022) The art and science of message concealing is what gives information security its secrecy, it protects a confidential communication's contents from nefarious individuals. The resulting stego-image can be transmitted without revealing that secret information is being exchanged. (Sharma, 2013) When cryptography and steganography are combined, the security of iris template protection is strengthened against significant damage to picture appearance in steganography that is relatively easy to detect, even if a third party only uses one of these techniques to compromise the security of the protection. In order to enhance and complement one another, the algorithms were integrated. (Islam et al., 2015) This study only addresses the iris template security issue, which raises the possibility of iris template assaults. To secure an iris template maintained in a database, a hybridized system utilizing cryptography (Advanced Encryption Standard, or AES) and steganography (Least Significant Bits, or LSB) techniques was presented. The subsequent sections of the paper include section 2, which reviews related literature; section 3, which outlines the methodology and describes performance metrics; section 4, which presents results and discussions; and section 5, which concludes the paper.

Review of related works:

Numerous techniques have been proposed to protect the biometric (iris) templates from any unauthorized or accidental alteration. The following are a few of the suggested methods:

(Das et al., 2020) proposed a more secure data communication with cryptography and steganography: An overview of the methods used to preserve the biometric data found in fingerprints is provided by this study. The fingerprint was deemed to be a practical biometric recognition method among those now in use. Because the frequency-domain approach is more resilient to attacks than the spatial domain technique, it is generally perceived as being superior. On the other hand, the frequency domain sees a higher utilization of spatial domain techniques due to their greater data capacity and ease of use. This article presented our review, which addressed the majority of traditional biometric systems, their corresponding performances, security and privacy issues, and will serve as a reference for likely biometric concealment systems. An important problem in telemedicine is the safe transfer of medical data across unprotected networks.

(Ogundokun & Abikoye, 2021) conducted research on a Safe and Secured Medical Textual Information Using an Improved LSB Image Steganography. In order to address the critical authentication issue, this also offered a modified least significant bit (LSB) technique capable of safeguarding and disguising medical data. The application was developed and run using MATLAB 2018, and it employed a logical bit shift operation. The results of the experiment demonstrated that the suggested method could ingrain medical data without producing a discernible stego picture fabrication. The study's main objective was to safeguard patient data in the digital health system. A modified least significant bit picture steganography technique was proposed in this study. PSNR and MSE are two performance metrics that were used to assess the suggested system after it was developed using MATLAB. There was an addition to the number of shifts. Comparing the suggested protected medical information system to other popular methods, it was shown to be effective in concealing medical information and producing undetectable stego pictures with mild entrenching falsifications. When compared to earlier research, the modified LSB picture steganography performed better, exhibiting a lower MSE value and a higher PSNR value than the traditional LSB approach

(Jassim et al., 2022) Biometric iris templates security based on secret image sharing and chaotic maps: the proposed system used a technique for safely storing the iris template in the database that combined secret image hiding and sharing to improve security and preserve privacy by splitting the template into two separate host (public) iris images. Only when both host images are reachable is it feasible to reconstruct the original template. Either the identity of the original biometric image is hidden by the host image. Biometrics-based authentication systems were able to improve security and privacy by storing the data as shadows across multiple sites instead of storing the whole set at one. Iris segmentation methods, feature extraction algorithms, a (2, 2) secret sharing and concealment are all included in the suggested biometric identification system. The standard color UBIRIS v1 data set is used to run the experiment and obtain results. The findings show that the techniques for protecting biometric templates from vulnerabilities can provide a countermeasure for those threats. Robust data encryption method based on a chaotic map preserves the security of iris templates kept in a central database. By employing the (2, 2) secret sharing technique, the template is split into two shares. One is stored in the database, while the other is on the user's ID card. The iris template is made secure by the fact that it can be kept in the database with just one share, which is concealed in a meaningful image. For the enrolled eye image, no data could be obtained. In this instance, unauthorised user access is prevented. In applications where security is crucial, this system will be more dependable and secure. The suggested secret sharing approach does not impair the performance of iris identification because it enables the restoration of the original iris template as soon as shadows become available.

(D et al., 2022) explore the concept of an Enhance Facial Biometric Template Security using Advance Encryption Standard with Least Significant Bit. Steganography and cryptography are the two most often utilized techniques for data protection and concealment. They integrated the two in their study to strengthen the security of biometric templates. The advanced encryption standard (AES) and the least significant bit (LSB) technique were employed to encrypt the templates and safeguard them from hackers. The effectiveness of combining stenography and encryption approaches to increase the security of biometric templates is the main focus of this work. Individuals' live facial data were gathered from four separate face samples. The steganography algorithm that has been created offers a facial template that is very secure against unauthorized access. According to the results, the training face biometric's recognition accuracy was 75%. Following assessment, more than 80% of the facial picture classifications were done correctly, with error rates, accuracy values, sensitivity, and specificity coming in at18%,95%,83%, and 75% overall. This demonstrates how effectively the system operated.

(Bagane et al., 2024) carried out a research on securing data in Images using cryptography and steganography algorithms. This study advocated the use of the Vigenère cipher technique in conjunction with a hash least significant bit (H-LSB) to add further security to data. The system proposed in this research employs steganography and cryptography in a multi-layer security technique to improve data security and make it safer and more secure to transfer via open channels or other networks. Techniques like steganography and cryptography have been suggested to increase data security. The suggested solution allows data to be transported over open channels or other networks while maintaining multi-layer security. The development of a system with improved security features to conceal covert communications from adversaries is the primary goal of this effort, being able to protect communications in our system application by encrypting data utilizing a combination of least significant bit steganography and Vigenère cipher algorithms. Information is encrypted so that only the sender and intended recipient can read it. The recipient is given a special key to decrypt the encrypted communication. This prevents data exchanged between the sender and the recipient in an insecure network environment from being compromised by an outsider. Following steganography, we obtain a fresh image in our system with no discernible changes to the image quality after the secret data is inserted in the image. It is a useful technique for hiding ciphered data inside of an image. We evaluated several photos with varying data sizes to be hidden using the suggested techniques in order to assess the system. The results of the test indicate that the system can offer enhanced security and a straightforward method for encrypting, embedding, and decrypting confidential messages with essentially no loss in image quality. As a result, this system offers increased protection with great efficiency. Considering the above, it is possible to enhance information/data security by combining cryptography and steganography techniques, as each by itself proves to be secure but is subject to attack. The research project addresses these problems by creating a novel technique that boosts the security of private images while also enhancing the quality of stego images.

Proposed methodology:

To consolidate the complexity of brute force and other means of attacks on encrypted data, this study proposes the utilization of steganography and cryptography techniques to develop an enhanced security for biometric template in the database. The idea behind the adaptation of the steganography approach is to falsify secret data transmission while eradicating data suspiciousness via the utilization of the least significant bits of data scrambling techniques. This study proposed the incorporation of the cryptography techniques to scramble the transmittable data adding some level of data protection via the use of two data encryption and decryption techniques namely the Blowfish and AES cryptography techniques. Having identified the need for information security, it becomes important to devise a methodology for the implementation of a secure system, while taking into cognizance the cost, efficiency, and effectiveness of the proposed system. This study proposed a three-step methodological approach. The first step entails using Blowfish to encrypt the original data first and Take the Blowfish encrypted data and encrypt it again using AES cryptography algorithm. The blowfish algorithm is proposed to harness the viability of the asymmetric cryptosystem in terms of digital signature repudiation authentication and its two cryptographic key (private and public) techniques that ensure secure public key transportation. By encrypting the data twice, an additional layer of security is added and increases computational overhead. Even if one layer is compromised, the data remains protected by the other. The AES proposed was targeted at providing additional data encryption standard approach to tighten information security as a symmetric cryptographic system. In the second step, as a means to integrate the steganography techniques, the LSB substitution is proposed to be performed based on four bits. The LSB-based image steganography methods embed secret data in the least significant bits of the biometric template (i.e., the image) pixel value. An embedding approach with a bigger embedding capacity is also designed in the second step, which focuses on reducing the amount of bit alterations per pixel during the embedding process. The amount of hidden data within a cover image is referred to as its embedding capacity. The third phase of the methodology encompasses the conductance of performance evaluation based on time metrics, and throughput evaluation metrics. The methodology described can be visualized in figure 1.

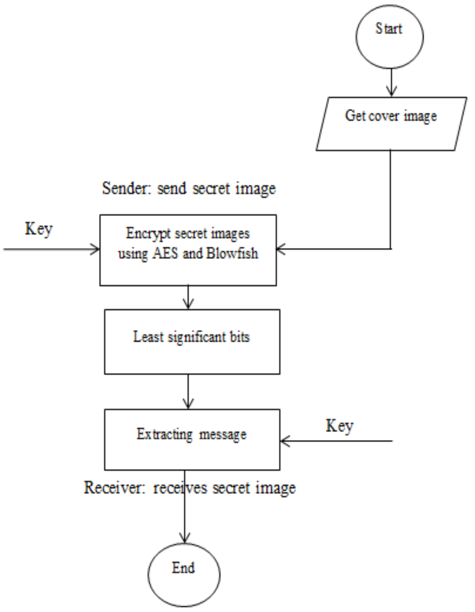

Start
Get cover image
Sender: send secret image
Key
Encrypt secret images using AES and Blowfish
Least significant bits
Extracting message
Key
Receiver: receives secret image
End

Figure 1: Proposed steganography and cryptographic methodology

Cryptography Techniques

AES is a popular technique that is perfect for encryption and decryption (Seth et al., 2021) Blowfish was conceived in 1993 by Bruce Schneier as a fast, free alternative to existing encryption algorithms. (Alabdulrazzaq & Alenezi, 2022) Since then, blowfish has undergone much analysis, and its reputation as a potent encryption method is gradually growing. Essentially, blowfish uses a variable-length key in a 64-bit block cipher. It's crucial to remember that the blowfish algorithm heavily relies on sub-keys, which are created prior to any data encryption or decryption. For this reason, the method is divided into two sections: data encryption and key expansion. A key with up to 448 bits can be expanded into many sub-key arrays, each containing 4168 bytes. It uses a straightforward procedure that is repeated sixteen times to encrypt data. A key-dependent permutation and a key-and data-dependent substitution make up each round. On 32-bit words, all operations are additions and XORs. Four indexed array data lookups are the only extra steps done per round. Moreover, blowfish make extensive use of sub-keys. Before any data is encrypted or decrypted, these keys need to be precomputed. The key length of the symmetric block cipher Blowfish can vary from 32 bits to 448 bits.

1. A predetermined string of pi's hexadecimal digits is used to populate the P-array and S-boxes.
2. Once all of the P-array's elements have been XORed with the key bits, the first element (P1) is now XORed with the key's first 32 bits, followed by P2 XORing with the second 32 bits, and so on.
3. The technique as outlined in the previous steps encrypts all strings that include zeros.
4. The output from the previous step 3 is used to replace the P1 and P2 arrays.
5. Using altered subkeys, Blowfish encrypts this output.
6. As a result of step 5, P3 and P4 in the P-array are altered. Until all four S-boxes and all P-arrays are changed, this process is repeated.

In total, Blowfish runs 521 times to generate all the subkeys and processes about 4 kilobytes (KB) of data.
The P-array consists of 18 32-bit subkeys: $P1, P2, \ldots P18$
Four 32-bit S-boxes have 256 entries each:

The P-array consists of 18 32-bit subkeys: $P_1, P_2, \ldots . P_{18}$
Four 32-bit S-boxes have 256 entries each:

$$S_{1,0}, S_{1,1}, \ldots . S_{1,255}$$
$$S_{2,0}, S_{2,1}, \ldots . S_{2,255}$$
$$S_{3,0}, S_{3,1}, \ldots . S_{3,255}$$
$$S_{4,0}, S_{4,1}, \ldots . S_{4,255}$$

The proposed blowfish algorithm uses a Feistel Structure Algorithm and its working is explained below.

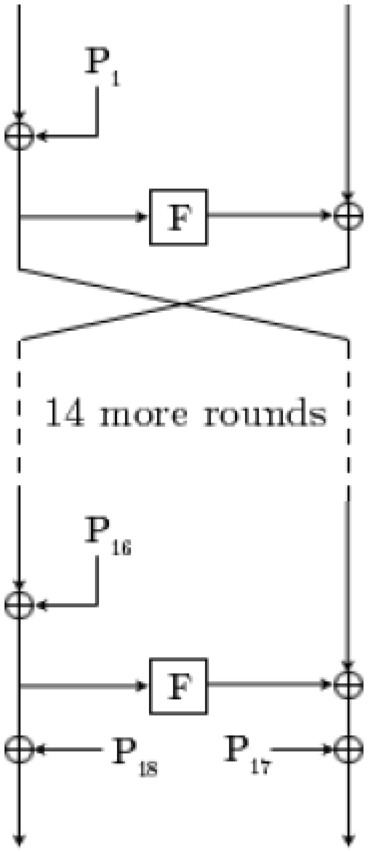


Figure 2: Feistel Structure of Blowfish

Blowfish is a Feistel network consisting of 16 rounds. The input is a 64-bit data element, x. To encrypt, the algorithm below is proposed

Algorithm 1: Blow-Fish

```
Let dataset be X
Divide x into two 32-bit halves: XL and XR
For i = 1 to 16:
    $X_l = X_l \oplus P^i$
    $X_r = F(X_l) \oplus X_R$
    $Swap\ X_l\ and\ X_r$
  $Swap\ X_l\ and\ X_r\ (undo\ the\ last\ swap)$
  $X_r = X_r \oplus P_{17}$
  $X_l = X_l \oplus P_{18}$
  $Recombine\ X_l\ and\ X_r$
```

F(XL) is the function from algorithm 1, and XL is the 16-bit input for the function in each round. The function divides the 16-bit input XL into four equal halves of 4 bits each. Each 4-bit half is then handed to an S-Box, and each S-Box produces a 4-Bit output. This suggests that four 4-bit outputs are produced by the four S-Boxes. The function's ultimate result, a 16-bit output, is obtained by adding the four 4-bit outputs modulo and XORing them. In summary both decryption and encryption are exactly the same, except that $P1,2,\ldots.P18$ are used in the reverse order.

S-Box (Substitution box) Operation

Having identified that the proposed blowfish consists of four S-Boxes, the proposed s-box operation proposed the usage of the XOR operation as s-box generation operation includes addition, multiplication and lookup tables. Hence, every S-Box proposed will be using a 4-bit input and thus generates a 4-bit output. The approach of blowfish adapted by this study in regards to s-boxes includes creating a 4-bit random number and XORing it with the input that is sent to each S-Box in order to produce 4-bit output from each S-Box.

For instance, assuming an output of XL is:
0010 0100 0010 1100 ………….. (3.1)
Dividing this 16-bit into four equal parts –
Part 1 Part2 Part3 Part4
0010 0100 0010 1100
Each part is given as input to S-Box
After generating the random number
Suppose
1111 1001 0111 1010…………… (3.2)
Dividing it into four equal parts—
RaNum1 RaNum2 RaNum3 RanNum4
1111 1001 0111 1010

XOR (1) and (2) using the s-boxes operations after that, to get the final 16-bit output, the outputs are added modulo and then XORed. This offers increased security since it generates the subkeys at random rather than using a set of predetermined permutations.

The working of the least significant bit

Considering that by using 7 bits to represent 5 volts of amplitude, we generate a relatively small division between values (0.04V). All datums can only have their reproduced value changed by the same amount (0.04V) if their least significant bit (LSB) is changed. As a result of this subtle alteration, data can be embedded into the bit sequence by making deliberate changes to the LSB of each sample without anyone noticing. We can inject a 25,000 bit message into the LSB for each second of recorded data by using successive data points to convey our message. When looking at the waveform after change, the unaided eye cannot discern the difference in voltage at any one datum.

Take a look at this example bit stream, for example:
01001010, 01001011, 01001100, 01001101,
01001110, 01001111, 01010000, 01010001 …

In the event we wished to inject the 8 bit message (11110000) into the data, we would modify the corresponding LSBs of the above bit stream to match our message. The resulting steganographic data stream would become
01001011, 01001011, 01001101, 01001101,
01001110, 01001111, 01010000, 01010000 … where the modified bits are in bold typeset.

Result and Discussion:

Table 1: Execution time comparison

File Size	BLOWFISH		AES		HYBRID	
(KB)	EN*	DE*	EN*	DE*	EN*	DE*
75	0.21	25.55	0.23	26.21	0.16	22.21
79	0.25	26.82	0.26	27.01	0.17	22.24
80	0.30	27.91	0.32	28.00	0.17	22.27
83	0.31	28.05	0.33	29.12	0.17	22.30
85	0.32	28.83	0.37	30.21	0.23	22.31
87	0.34	30.01	0.39	31.00	0.23	22.55
90	0.35	30.92	0.41	32.12	0.25	23.32
91	0.35	31.05	0.42	32.98	0.27	23.37

Table 1 provides a comprehensive overview of the empirical outcomes derived from the application of three distinct cryptographic algorithms: BlowFish, Advanced Encryption Standard (AES), and their hybrid configuration, within the context of image steganography and crypto analysis. The focus of the analysis lies in the meticulous measurement of encryption (EN) and decryption (DE) times, quantified in milliseconds, across varying file sizes represented in kilobytes.

Blow-Fish emerges as a stalwart in terms of consistent efficiency in both encryption and decryption processes across diverse file sizes. The encryption times, spanning a range from 0.21 to 0.35 milliseconds, coupled with decryption times oscillating between 25.55 and 32.98 milliseconds, underscore the algorithm's swift and dependable performance in facilitating image steganography. These findings position Blow-Fish as an adept solution for practitioners seeking expedited cryptographic operations.

Similarly, AES, the widely acknowledged encryption standard, exhibits commendable performance metrics across the specified file sizes. Encryption times, varying between 0.23 and 0.42 milliseconds, coupled with decryption times ranging from 26.21 to 32.98 milliseconds, affirm the algorithm's consistent and reliable efficiency. The steadfast nature of these timings reinforces AES as a robust and dependable choice for applications in image steganography and cryptoanalysis.

The hybrid approach, a strategic amalgamation of AES and Blow-Fish, aimed at synergizing the inherent strengths of both algorithms, attain competitive encryption and decryption times. Notably, encryption times ranging from 0.16 to 0.27 milliseconds and decryption times spanning 22.21 to 23.37 milliseconds underscore the hybrid model's efficacy in enhancing overall cryptographic efficiency. This amalgamated configuration serves as a promising avenue, leveraging the optimal attributes of each constituent algorithm to achieve a balanced compromise between speed and security. The graphical result for the encryption and decryption time for each algorithm with their respective file size can be visualized from Figure 3 and 4.

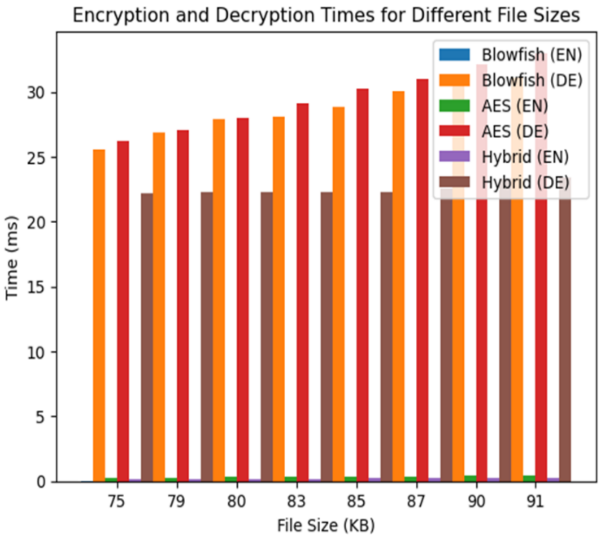


Figure 3: Encryption and Decryption Time Bar chart

Figure 3 depict the barchart of the excusion time comparism for different file sizes of the blowfish, AES (advance encryption standard) and their hybridization for both encryption and decryption with their colour representation. The result shows that the encryption and decryption of the hybrid is more efficient compare to the Blowfish and AES.

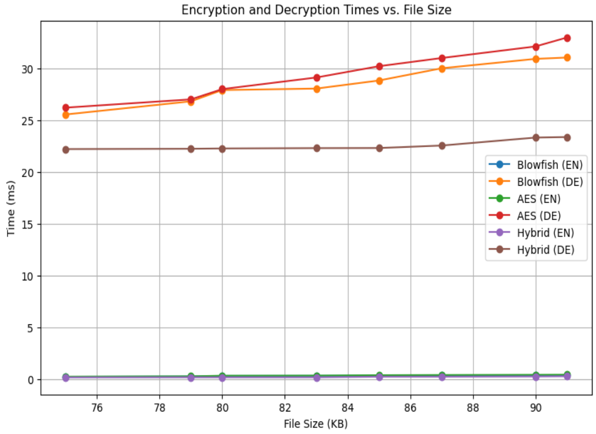


Figure 4: Encryption and Decryption Time Line chart

Figure 4 represent the encryption and decryption time line chart of blowfish, AES and their hybrid. The graph above shows that the AES encryption and their hybrid are most optimal compare to the others.

Steganography Embedding and False Positive Rate Accuracy

To assess the efficacy of the steganography embedding process, evaluation metrics, including Embedding Accuracy (EA) and False Positive Rate Accuracy (FPR), were investigated.

Table 2: Embedding and False Positive Rate Accuracy

File Size	Blow Fish		AES		Hybrid	
(KB)	EA	FPR	EA	FPR	EA	FPR
75	95.21	4.2	92.33	6.2	99.99	0.3
79	97.01	2.4	94.11	5.1	99.89	0.5
80	90.99	7.9	89.01	10.2	99.88	0.6
83	92.34	6.22	90.13	8.2	98.97	1.3
85	97.44	2.55	96.21	5.1	99.97	0.3
87	99.11	1.8	99.47	1.8	99.87	0.4
90	99.99	0.5	99.92	0.3	99.99	0.3
91	99.78	1.01	99.88	0.8	99.92	1.6

The table above shows the result of Blowfish, AES and their hybrid of embedding and false positive rate accuracy for both encryption and decryption, where the result of the hybrid for encryption and decryption are more optimal compared to Blowfish and AES encryption and decryption.

Throughput

This measures the volume of data or information that passes through a network in a given period. The module compares the results of the observed algorithms against each other concerning their throughput. The metrics throughput is a measure of the file's sizes per unit execution time of the algorithms for both encryption and decryption of the stego files. The file size and the encryption and decryption time for the stego files are captured from the result of Table 3. the metric for evaluation is defined as:

$$\mathbf{throughput} = \mathbf{t_p/e_t}$$

Where t_p is the file size (KB) and e_t is the encryption time.

Table 3: Throughput

	Throughput (MB)		
File (KB)	SizeBF	AES	HYBRID
75	357.14	326.09	468.75
79	316.00	303.85	464.71
80	266.67	250.00	470.59
83	267.74	251.52	488.24
85	265.63	229.73	369.57
87	255.88	223.08	378.26
90	257.14	219.51	360.00
91	260.00	216.67	337.04

Table 3 presents the throughput of the image cryptography and steganography embedding, which is a metric representing the efficiency of file size processing per unit execution time during both encryption and decryption phases in the context of crypto-steganography. The pertinent data, encapsulating file sizes and corresponding encryption and decryption times, is extracted from Table 1. The evaluation metric for throughput is defined as the ratio of file size (in kilobytes) to execution time.

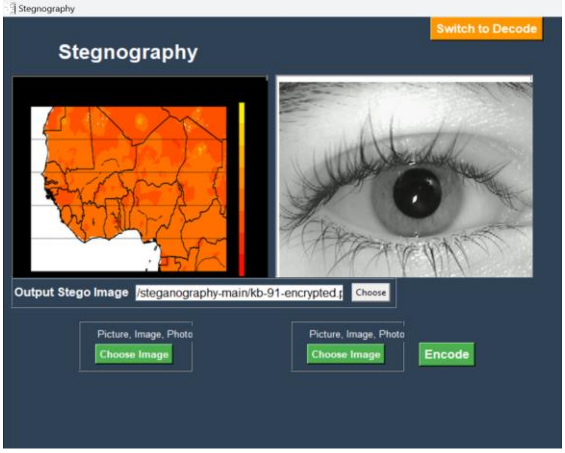
Graphical Result Presentation

To enhance the user experience and ensure the practical applicability of the developed system, a graphical user interface (GUI) was meticulously designed and implemented. Figure 2 illustrates the encryption and embedding procedures applied to secret images sourced from the iris dataset. The left-hand side of Figure 4.1 depicts the chosen cover image, while the right-hand side showcases the iris secret image slated for embedding within the cover image. Initiating the encoding operation, denoted by the "encode" button, yields the integration of the secret image into the cover image, subsequently instigating the extraction and decoding processes.

Figure 4.4 provides a representative illustration of the system's functionality, showcasing the extraction process of a concealed image from the cover image. The visual representation comprises two images: the left-hand side exhibits the steganographic image, concealing the embedded secret image, while the right-hand side displays the successfully extracted secret image. The interface incorporates a prompt box, furnishing detailed information on the extraction and decryption time required for the secret image.

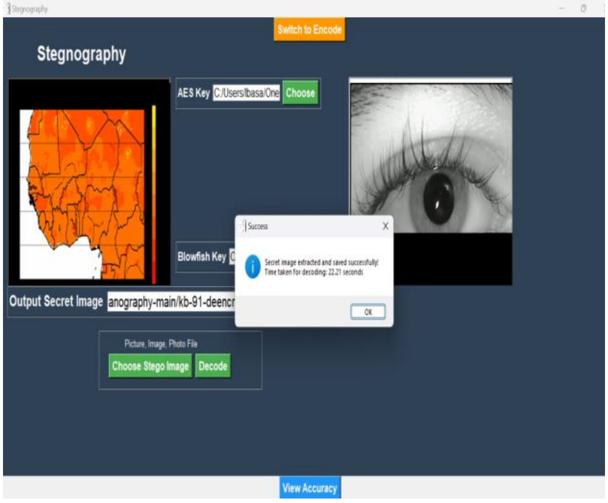
Additionally, the figure features an input key field, specifically designated for entering the encryption keys associated with the Advanced Encryption Standard

(AES) and Blowfish algorithms. These keys are instrumental in decrypting the embedded image within the cover image. The utilization of a graphical user interface not only facilitates user interaction but also provides a seamless platform for initiating and monitoring the extraction process, contributing to the overall usability and accessibility of the system.



Output Stego Image /steganography-main/kb-91-encrypted.p

Figure 4.3: Steganography and Cryptography encryption and embedding



AES Key C:/Users/Ibasa/One

Blowfish Key C

Output Secret Image anography-main/kb-91-deencr

Secret image extracted and saved successfully!
Time taken for decoding: 22.21 seconds

Figure 4.4: Cryptography and Steganography extraction and decryption

Conclusion:

One of the most reliable biometrics on the market now is iris detection. It is used in many fields, including live passwords and forensics. Governments utilize the codes as a special way to identify people. Iris templates are vulnerable to both direct and indirect attacks, among other sorts of attacks. Template security has consequently emerged as a key concern in biometric identification. Each of these procedures takes two inputs: a stego picture and a cover image for retrieval, and an iris template and image for security. At the conclusion of each successful operation, there is only one output: an iris template for the retrieving operation and a stego picture for the securing operation. The hidden text message or stego file is embedded into the master file, but the tiny alterations that result are invisible to the human eye. In conclusion, it is shown that the system's strength lies in the steganography technique in place, which ensures a highly guarded iris template against unwanted access. In conclusion, it is shown that the steganography algorithm, which produces an iris template that is incredibly secure against unwanted access, is the system's strongest point. The issue of panicking about information that is in transit or saved in a database will be reduced, if not completely removed, in an information communication technology environment thanks to the system's security level. A stronger security platform is created when steganography and cryptography are used in iris recognition.

Comparism

This section compares the implemented hybrid cryptographic and steganography algorithms against some of the state of the art algorithms implemented by other authors. During the computational analysis, the computational time of the state-of-the-art cryptographic and steganography algorithm is also classified as the encryption/decryption time of the stego files and cover files.

Table 4: Result comparism

S/N	Authors	Image size and type	Encryption time	Decryption time	throughput	GAR,FAR,TAR
1	(Biu et al., 2018) Husain & Magaji (2018)	JPEG Image	10	0.5	-	FAR = 1
3	Mahmoud & Elshoush (2022)	128bit	12.5% or 0.125 bytes	-	-	-
4	(Ammour et al., 2018) et el., (2018)	-	-	-	0.326	FAR = 0.12%, GAR = 98.75%.

Author Contributions: "Conceptualization: Agu Edward Onyebueke and Danbeki Mercy; methodology, Danbeki Mercy; validation: Agu Edward Onyebueke.; formal analysis: Agu Edward Onyebueke.; investigation: Danbeki Mercy.; resources: Agu Edward Onyebueke; data curation: Danbeki Mercy.; writing—original draft preparation: Danbeki Mercy; writing—review and editing: Agu Edward Onyebueke; visualization: Agu

Edward Onyebueke; supervision: Agu Edward Onyebueke; project administration: Danbeki Mercy.

Funding: "This research received no external funding"

Data Accessibility Statement:
The data we utilized is accessible to the public and may be found at **www.kaggle.com/datasets/naureenmohammad/mmu-iris-dataset**.

Conflicts of Interest: "The authors declare no conflict of interest."

Reference

Abikoye, O. C., Ojo, U. A., Awotunde, J. B., & Ogundokun, R. O. (2020). *A safe and secured iris template using steganography.pdf*.

Alabdulrazzaq, H., & Alenezi, M. N. (2022). Performance Evaluation of Cryptographic Algorithms: DES, 3DES, Blowfish, Twofish, and Threefish. *International Journal of Communication Networks and Information Security*, *14*(1), 51–61. https://doi.org/10.54039/ijcnis.v14i1.5262

Ammour, B., Bouden, T., & Boubchir, L. (2018). Face–iris multi-modal biometric system using multi-resolution Log-Gabor filter with spectral regression kernel discriminant analysis. *IET Biometrics*, *7*(5), 482–489. https://doi.org/10.1049/iet-bmt.2017.0251

Bagane, P., Venkatesh, S., Guttikonda, J. B., Badhoutiya, A., Pratap Srivastava, A., Khan, A. K., Deepak, A., & Shrivastava, A. (2024). Securing Data in Images Using Cryptography and Steganography Algorithms. *International Journal of Intelligent Systems and Applications in Engineering*, *12*(15s), 17–25.

Biu, H. A., Husain, R., & Magaji, A. S. (2018). an Enhanced Iris Recognition and Authentication System Using Energy Measure. *Science World Journal*, *13*(1), 11–17. www.scienceworldjournal.org

D, G. M., Hambali, M. A., Abdulganiyu, O. H., & Lawrence, E. (2022). Enhance Facial Biometric Template Security using Advance Encryption Standard with Least Significant Bit. *Journal of Computer Science and Engineering (JCSE)*, *3*(2), 60–70. https://doi.org/10.36596/jcse.v3i2.527

Das, S. B., Mishra, S. K., & Sahu, A. K. (2020). Cryptography Algorithm. *A New Modified Version of Standard RSA Cryptography Algorithm*, *767*(January), 281–287.

Islam, M. N., Islam, M. F., & Shahrabi, K. (2015). Robust information security system using steganography, orthogonal code and joint transform correlation. *Optik*, *126*(23), 4026–4031. https://doi.org/10.1016/j.ijleo.2015.07.161

Edward O. Agu, Michael O. Ogar, Anthony O. Okwori (2019), Formation of an improved RC6 (IRC6) cryptographic algorithm, *International Journal of Advanced Research in Computer Science*, *Volume 10, issue 4*.

Jassim, M. F., Hamzah, W. M. S., & Shimal, A. F. (2022). Biometric iris templates security based on secret image sharing and chaotic maps. *International Journal of Electrical and Computer Engineering*, *12*(1), 339–348. https://doi.org/10.11591/ijece.v12i1.pp339-348

Ogundokun, R. O., & Abikoye, O. C. (2021). A safe and secured medical textual information using an improved LSB image steganography. *International Journal of Digital Multimedia Broadcasting*, *2021*. https://doi.org/10.1155/2021/8827055

Revenkar, P. S., Anjum, A., & Gandhare, W. Z. (2010). Secure Iris Authentication Using Visual Cryptography. *International Journal of Computer Science and Information Security(Ijcsis)*, *7*(3), 218–221.

Seth, B., Dalal, S., Le, D. N., Jaglan, V., Dahiya, N., Agrawal, A., Sharma, M. M., Prakash, D., & Verma, K. D. (2021). Secure cloud data storage system using hybrid paillier⇓blowfish algorithm. *Computers, Materials and Continua*, *67*(1), 779–798. https://doi.org/10.32604/cmc.2021.014466

Sharma, H. (2013). Secure Image Hiding Algorithm using Cryptography and Steganography. *IOSR Journal of Computer Engineering*, *13*(5), 01–06. https://doi.org/10.9790/0661-1350106